Access Controls for IIOT Work Systems – Biometric Mechanisms

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Supervisors

Prof. Brian Cusack

Dr Raymond Lutui

July 2026

By

Francis Ebere Anyanka

School of Engineering, Computer, and Mathematical Sciences

Abstract

This research aims to address security challenges in the IIoT (Industrial Internet of Things) work environment. The increasing digitalisation of industrial workplaces through the Industrial Internet of Things (IIoT) has transformed the way organisations manage physical access to critical infrastructure, manufacturing plants, and hazardous operational environments. Despite these advances, existing access control mechanisms, including passwords, RFID cards, tokens, PINs, and unimodal biometric systems, remain vulnerable to credential theft, spoofing attacks, environmental interference, and operational constraints. Industrial environments further complicate authentication due to the use of personal protective equipment (PPE), variable lighting, dust, machinery noise, worker movement, and harsh working conditions, which significantly reduce biometric recognition accuracy. Existing authentication solutions, therefore, fail to provide the level of security, usability, and resilience required for reliable contactless physical access control in modern IIoT environments.

This research addresses these limitations by designing, developing, and evaluating a contactless multimodal biometric fusion framework for secure physical access to industrial work sites. The proposed framework integrates facial, iris, ear, gait, palmprint, fingerprint, and voice biometrics within a deep learning-based fusion architecture capable of improving authentication robustness under dynamic operational conditions. To strengthen biometric template security, the framework incorporates biometric watermarking to protect identities and ensure data integrity. The research delivers three complementary Design Science Research artefacts: Artefact 1, a conceptual framework derived from a systematic literature review that establishes the theoretical foundations of contactless multimodal biometric authentication; Artefact 2, an experimentally validated prototype implemented within the Second Life virtual environment to simulate realistic industrial access control scenarios; and Artefact 3, a refined adaptive authentication framework informed by industrial expert evaluation, integrating contextual intelligence and adaptive biometric fusion to improve authentication resilience in complex industrial environments.

The study adopted the Design Science Research Methodology (DSRM) to create three prototypes, to guide the iterative design, development, demonstration, and evaluation of the proposed solution. The research combined a systematic literature review, conceptual framework development, prototype implementation, controlled

experimentation, and expert evaluation. A virtual industrial environment developed within Second Life enabled safe, repeatable, and cost-effective simulation of industrial access control without disrupting operational facilities. The proposed artefacts were evaluated for authentication accuracy, precision, recall, computational performance, environmental robustness, and usability, in accordance with ISO 9241-11.

The findings demonstrate that multimodal biometric fusion substantially improves authentication performance compared with conventional unimodal biometric systems while reducing authentication errors and increasing resilience against spoofing and operational variability. Experimental results confirmed that environmental conditions, including PPE occlusion, worker movement, poor illumination, and industrial noise, remain major factors influencing biometric reliability, thereby validating the need for adaptive authentication mechanisms. Although multimodal fusion significantly enhanced recognition performance, the research further established that static fusion alone is insufficient under highly dynamic industrial conditions. Instead, adaptive contextual weighting and intelligent decision-making were shown to improve authentication robustness by responding to changing biometric quality and environmental constraints. Expert evaluation further confirmed the practical feasibility, scalability, and industrial relevance of the proposed framework for future IIoT deployments.

This research contributes a validated contactless biometric access control framework, a comprehensive experimental evaluation methodology, and three rigorously developed Design Science Research artefacts that collectively advance knowledge in secure IIoT authentication. The research demonstrates how contactless multimodal biometric fusion can provide secure, usable, and scalable physical access control for industrial work sites while addressing real-world operational challenges. Beyond its immediate contribution to industrial cybersecurity and access management, the research establishes a foundation for future investigations into explainable artificial intelligence, adaptive biometric fusion, continuous authentication, privacy-preserving biometric protection, federated learning, and deployment within real-world cyber-physical industrial systems. The proposed framework, therefore, offers both a significant academic contribution and a practical pathway towards next-generation secure contactless biometric authentication for Industry 4.0 and emerging Industry 5.0 environments.

Table of Contents

ABSTRACT ..... **I**

TABLE OF CONTENTS ..... **III**

ATTESTATION OF AUTHORSHIP ..... **XIII**

PUBLICATIONS ..... **XIV**

ARTIFICIAL INTELLIGENCE DECLARATION TEMPLATE ..... **XV**

ACKNOWLEDGEMENTS ..... **XVII**

ETHICS EXCEPTION ..... **XVIII**

LIST OF ABBREVIATIONS ..... **XIX**

CHAPTER 1: INTRODUCTION **1**

1.0 INTRODUCTION 1
1.1 WHY AUTHENTICATION IS NEEDED (E2 REQUIRED 1) 2
1.2 THE PROBLEM & CONTEXT 2
1.3 THE RESEARCH QUESTIONS & METHOD 5
1.4 THE FINDINGS 7
1.5 THE THESIS STRUCTURE 8
1.6 CONCLUSION 11

CHAPTER 2: LITERATURE REVIEW **12**

2.0 INTRODUCTION 12
2.1 LITERATURE SELECTION PROCESS 12
2.2 INDUSTRIAL INTERNET OF THINGS (IIOT) DEFINITION 14
2.2.1 Industrial Revolution – Historical Approach 15
2.2.2 Context – IIOT 16
2.2.3 Current Architecture 17
2.2.4 Types of IIoT Architectures 18
2.2.5 Risks Associated with IIoT. 20
2.2.6 Current Security Issues 21
2.3 ACCESS CONTROL ALGORITHMS 25
2.3.1 Types of Access Control Algorithm 25
2.3.2 Access Control- Authentication and Authorisation in IoT 27
2.3.3 Types Of Multi-Factor Algorithm 31
2.3.4 Multifactor Authentication (MFA) Token Access Control Used In Previous Works 31
2.4 BIOMETRIC TRAITS 34
2.4.1 Biometric System Pathway (Trait Sensor Interaction) 35
2.4.1.1 Pre-processing stage 35
2.4.1.2 Region of interest stage 36
2.4.1.3 Feature extraction stage 37
2.4.2 Biometric Factors Definition 39
2.5 BIOMETRIC TRAITS AND DEEP LEARNING 42
2.5.1 Face Recognition Paradigms 42
2.5.2 Fingerprint Recognition Paradigms 43

2.5.3 The Palm Print Recognition Paradigms 45
2.5.4 The Iris Recognition Paradigms 46
2.5.5 The Gait Recognition Paradigms 48
2.5.6 The Voice Recognition Paradigms 49
2.5.7 The Ear Recognition Paradigms 51
2.5.8 Contactless Weight Scaling 53
2.5.9 Performance Rating of These Biometric Traits 54
2.6 HUMAN-COMPUTER INTERFACE AND BIOMETRICS 57
2.6.1 Past Works on Different Human-Computer Interfaces 57
2.6.2 Advances In Human-Computer Interaction and Biometric Systems 58
2.7 VIRTUAL ENVIRONMENTS AND IIOT 60
2.7.1 Communication Modes and Social Behaviours in Social VR 60
2.7.2 VR Software Platforms and Selection Rationale 61
2.7.2.1 Evaluation of Virtual Environments 61
2.8 USEABILITY FUNCTIONALITY FACTORS IN IIOT 62
2.8.1 Operational Technology Security Standards 63
2.9 REVIEW OF ISSUES & PROBLEMS 64
2.9.1 Human-computer Interaction Problems 64
2.9.2 Issues With Biometric Access Controls 66
2.10 PROPOSED SOLUTION ARTEFACT 1 68
2.10.1 Biometric Access Control Fusion System (BACFS) Features 70
2.11 CONCLUSION 71

CHAPTER 3: RESEARCH METHODOLOGY 73

3.0 INTRODUCTION 73
3.1 ISSUES AND PROBLEMS FROM CHAPTER 2 74
3.1.1 Research Problems Selection 74
3.2 RESEARCH QUESTIONS AND HYPOTHESIS 77
3.2.1 RESEARCH QUESTIONS AND HYPOTHESES 77
3.3 SIMILAR STUDIES 78
3.4 SELECTING METHODOLOGY 84
3.4.1 Comparison Of Design Thinking and Design Science Methodology 84
3.4.2 Justification for Design Science Research Methodology for Biometric Fusion in IIoT 87
3.4.3 Design Science Research Methodology Implementation 89
3.4.3.1 Phase 1: Problem Identification and Definition 90
3.4.3.2 Phase 2: Solution Objectives Definition 91
3.4.3.3 Phase 3: Artefact 1, 2 and 3 proposed Design and Development 91
3.4.3.4 Phase 4: Artefact Application Demonstration 91
3.4.3.5 Phase 5: Demonstration Effectiveness Evaluation 92
3.4.3.6 Phase 6: Artefact Results Communication 92
3.5 ARTEFACT 1 95
3.5.1 Data Collection 95
3.5.2 Artefact 1 Data Analysis 96
3.5.3 Two-Level Authentication Systematic Overview 98
3.5.3.1 Proposed CNN-Based Multi-Factor Analysis Logic 98
3.5.3.2 Authentication at First Level 99
3.5.3.3 Authentication at Second Level 100
3.6 ARTEFACT 2 101
3.6.1 Data Collection Strategies for Second Life 101
3.6.2 Experimental Design 102
3.6.2.1 Introduction 102
3.6.2.2 Objectives & high-level design 103
3.6.2.3 Design summary (factors, cells, trials) 104

3.6.2.4 Constraint Combination Logic 104
3.6.2.5 Per-trial procedure (operator workflow) 105
3.6.2.6 Validation, metrics and analysis 105
3.6.2.7 Biometrics Replicated as Functional Proxies in the Second Life 106
3.6.3 Map To The 8 Biometrics (Reference to System Design) 108
3.6.3.1 Limitations & notes (transparent) 109
3.6.3.2 Deliverables from the experiment 109
3.6.4 Data Analysis 110
3.6.5 Mathematical summary/formulae (compact) 111
3.6.5.1 reliability score 111
3.6.5.2 Normalised weight 112
3.6.5.3 Fusion score 113
3.6.6 Artefact 2 Decision support system 113
3.7 ARTEFACT 3 114
3.7.1 Data Collection Processes 115
3.7.2 Data Analysis Process Steps for Expert Feedback. 116
3.8 EXPECTATIONS ON ARTEFACTS 118
3.8.1 Limitations 120
3.9 CONCLUSION 120

CHAPTER 4: ARTEFACT 2 123

4.0 INTRODUCTION 123
4.1 ARTEFACT 1 WITHIN THE EXPERIMENTAL FRAMEWORK 124
4.1.1 Recap of Artefact 1 from Literature (Chapter 2) 124
4.1.2 Artefact 1 (A1) Into Measurable Components 124
4.1.3 Implementation of Artefact 1 (A1) in the VR System 124
4.1.4 Data Collection: Realising Artefact 1 (A1) 125
4.1.5 Transitioning To Artefact 2 (A2) 125
4.2 EXPERIMENTAL RESULTS FROM ARTEFACT 2 (SECOND LIFE TEST SIMULATION) 125
4.2.1 Experimental Authentication Model 125
4.2.2 Dataset Overview 126
4.2.3 Trial Distribution by Constraint Count 127
4.2.4 Overall Authentication Outcomes 127
4.2.5 Authentication Efficiency by Constraint Level 128
4.2.6 Trait Degradation Analysis 128
4.2.7 Cross-Avatar Consistency 129
4.2.8 Constraint Focused Experimental Results (A1–A6) 129
4.2.9 Interpretation of Constraint Focused Behaviour 130
4.2.10 FRR and Authentication Performance Analysis for the Experiment 131
4.3 ANALYTICAL INTERPRETATION OF EXPERIMENTAL RESULTS 131
4.3.1 Analytical Framing 131
4.3.2 Constraint Accumulation and Efficiency Collapse 132
4.3.3 Trait Degradation Statistical Analysis 133
4.3.4 Cochran-Armitage Trend test 134
4.3.5 Cross-Avatar Variance Analysis 135
4.3.6 Behavioural Segmentation Model 135
4.3.7 False Rejection Rate (FRR) 136
4.3.8 Consolidated Statistical Summary 136
4.4 REDESIGN JUSTIFICATION TOWARD ARTEFACT 2 137
4.4.1 Required Architectural Properties for Artefact 2 137
4.4.2 Structural Enhancements for Upgrade Artefact 2 138
4.4.2.1 Mathematical Reformulation for Artefact 2 138
4.4.2.2 Expected Performance Improvements 138

4.5 IMPLEMENTATION OF THE ADAPTIVE WEIGHTED ARCHITECTURE (ARTEFACT 2) 139
4.5.1 Architectural Transition and Design Principles 140
4.5.2 Mathematical Implementation Model 140
4.5.3 Conclusion 142

CHAPTER 5: ARTEFACT 3 146

5.0 INTRODUCTION 146
5.1 HIGHLIGHTING ARTEFACT 2 146
5.1.1 Filtering Artefact 2 for Meaningful Findings 147
5.1.2 Linking Artefact 2 Back to Artefact 1 147
5.1.3 Informing Expert Review 147
5.1.4 Outcome and Future Direction 148
5.2 OVERVIEW OF EXPERT REVIEW PROCESS 148
5.2.1 Purpose of the Expert Review 150
5.2.2 Methods 151
5.3 EXPERT EVALUATIONS 152
5.3.1 Expert 1: Field Operator (Industrial/Construction Worker) 153
5.3.2 Expert 2: IT security (Adaptive Authentication Specialist) 153
5.3.3 Expert 3: IT Security (IAM Specialist) 154
5.3.4 Expert 4: Biometric Systems (Academic) 155
5.3.5 Expert 5: Applied IT Security 156
5.3.6 Expert 6: IoT Systems Engineer 157
5.3.7 Expert 7: Virtual Reality (VR) Specialist 157
5.3.8 Expert 8: Industrial IoT Architect 158
5.3.9 Expert 9: Site Security Officer (Construction) 159
5.4 THEMATIC ANALYSIS 160
5.4.1 Thematic Theme Reviews 165
5.4.1.1 Adaptive Weighting and Context Awareness 165
5.4.1.2 Anti-Spoofing and Attack Resistance 166
5.4.1.3 Edge versus Cloud Processing. 167
5.4.1.4 Environmental Robustness and performance under personal protective equipment (PPE) Constraints 169
5.4.1.5 Explainability and Confidence Transparency 170
5.4.1.6 Multimodal Integration 171
5.4.1.7 Policy and Compliance Integration 172
5.4.1.8 Real-Time Performance and Latency 173
5.4.1.9 Simulation versus Reality 174
5.4.2 General Conclusion of the Thematic Review 175
5.5 ARTEFACT 3 (A3) ARCHITECTURE SPECIFICATION 177
5.5.1 Sensor/Input layer 177
5.5.2 Adaptive Fusion Layer 178
5.5.3 Decision and policy layer 179
5.5.4 Data and management layer 179
5.5.5 Algorithms and Partitioning 180
5.5.6 Edge vs Cloud 180
5.5.7 Failure Modes & Mitigation: 181
5.5.8 Artefact 3 Architecture Diagram Plan 182
5.6 CONCLUSION 184

CHAPTER 6: DISCUSSION 185

6.0 INTRODUCTION 185
6.1 DISCUSSION OF THE MAIN RESEARCH QUESTION AND SUB-QUESTIONS 186
6.2 DISCUSSION OF RESEARCH QUESTION 1 TO 3 (RQ1–RQ3) 187

6.2.1 Research Question 1 187
6.2.2 Research Question 2 188
6.2.3 Research Question 3 189
6.3 HYPOTHESES TESTING 190
6.3.1 Hypothesis 1 (H1) 190
6.3.1.1 Positive Evidence for H1 191
6.3.1.2 Evidence Against H1 192
6.3.1.3 H1 Hypothesis Decision 193
6.3.2 Hypothesis 2 (H2) 193
6.3.2.1 Positive Evidence for H2 193
6.3.2.2 Evidence Against H2 194
6.3.2.3 Hypothesis 2 Decision 194
6.3.3 Hypothesis 3 (H3): 195
6.3.3.1 Positive Evidence for H3 195
6.3.3.2 Evidence Against H3 196
6.3.3.3 Hypothesis Decision 196
6.3.4 Overall Interpretation of the Hypothesis Testing 196
6.4 CONTRIBUTION OF THE STUDY 197
6.4.1 Practical Implications 198
6.5 ISO STANDARDS ALIGNMENT TO ARTEFACT 3 198
6.6 FUTURE RECOMMENDATIONS 199
6.7 CHAPTER CONCLUSION 200

CHAPTER 7: CONCLUSION 201

7.0 INTRODUCTION 201
7.1 SUMMARISED KEY FINDINGS 201
7.2 KEY RESULTS MAPPED TO RESEARCH QUESTIONS 203
7.3 THEORETICAL CONTRIBUTIONS 204
7.4 PRACTICAL AND INDUSTRIAL IMPLICATIONS 204
7.5 LIMITATIONS 205
7.6 RECOMMENDATIONS 206
7.7 ARTEFACT 2 VS ARTEFACT 3 COMPARISON 207
7.8 CONCLUSION 209

REFERENCES 210

APPENDIX ARTEFACT 1 –EXPERTS PARTICIPATION 238

APPENDIX A2 – EXPERT FEEDBACK 241

Expert 1 Feedback 241
Expert 2 Feedback 241
Expert 3 Feedback 242
Expert 4 Feedback 242
Expert 5 Feedback 242
Expert 6 Feedback 243
Expert 7 Feedback 243
Expert 8 Feedback 244
Expert 9 Feedback 244

APPENDIX B1- SECOND LIFE TEST RESULT TABLE 245

APPENDIX B2- SECOND LIFE IMPLEMENTATION CODE 252

Gate_Scanner.Lsl — Land Scanner 252

Avatar_Hud.Lsl — Wearable Hud (Per Avatar) 255
Logger 258
Gate Control 259

APPENDIX B3- SECOND LIFE AVATAR SNAPSHOT SCENARIO. 260

Avatar 1 Snapshots 261
Avatar 2 Snapshots 262
Avatar 3 Snapshots 262
Avatar 4 Snapshots 263
Avatar 5 Snapshots 263
Avatar 6 Snapshots 264
Avatar Industrial Face Mask 264
Avatar Industrial Face Mask & Heavy Load 265
Avatar Industrial Face Mask & Helmet 265
Avatar Lowlight, Fastmove & Heavy Load 266

TABLE OF FIGURES

FIGURE 1.1THESIS STRUCTURE 9
FIGURE 2.1 PRISMA FRAMEWORK FOR LITERATURE SELECTION.....14
FIGURE 2.2 TYPES OF BIOMETRIC TRAITS FOR AUTHENTICATION AND THEIR EXAMPLES (LIPPS ET AL., 2021, P.3) 35
FIGURE 2.3 ARTEFACT 1 69
FIGURE 3.1 DSRM (PEFFERS ET AL., 2007, P. 54) 90
FIGURE 3.2 ARCHITECTURE OF SCIENTIFIC RESEARCH (MAO ET AL., 2023, P.110) 90
FIGURE 3.3 DESIGN SCIENCE RESEARCH METHODOLOGY STEPS ARE PROPOSED FOR THIS RESEARCH. 93
FIGURE 3.4 COMPLETE THE DESIGN SCIENCE RESEARCH METHODOLOGY STEPS PROPOSED FOR THIS RESEARCH FLOWCHART 94
FIGURE 3.5 TOTAL FUSION LOGIC FLOW CHART.....97
FIGURE 3.6 FIRST LEVEL AUTHENTICATION IDEA 99
FIGURE 3.7 SECOND-LEVEL AUTHENTICATION IDEA 100
FIGURE 3.8 ARTEFACT 1 TESTED IN FOR THE IMPROVED ARTEFACT 2 103
FIGURE 3.9 DECISION SUPPORT SYSTEM FOR SECOND LIFE ARTEFACT2.....114
FIGURE 3.10 SUMMARISES THE MAIN STEPS INVOLVED IN DESIGNING AN EXPERT FEEDBACK PROCESS. 116
FIGURE 3.11 EXPERT DATA COLLECTION AND ANALYSIS PROCESS STEPS.....118
FIGURE 3.12 ARTEFACT ROAD MAP 122
FIGURE 4.1 PASS / FAIL DISTRIBUTION 127
FIGURE 4.2 AUTHENTICATION EFFICIENCY VS CONSTRAINT COUNT 128
FIGURE 4.3 TRAIT DEGRADATION UNDER CONSTRAINT ACCUMULATION.....129
FIGURE 4.4 ARTEFACT 1 EXPERIMENTAL RESULT STRUCTURE (STATIC FUSION ARCHITECTURE) 137
FIGURE 4.5 BEHAVIOURAL SHIFT (ARTEFACT 1 VS ARTEFACT 2) 139
FIGURE 4.6 ARTEFACT 2 (ADAPTIVE WEIGHTED ARCHITECTURE) 142
FIGURE 5.1 NVIVO CODING WORD FOCUS FOR EXPERT 1 153
FIGURE 5.2 NVIVO CODING WORD FOCUS FOR EXPERT 2 154
FIGURE 5.3 NVIVO CODING WORD FOCUS FOR EXPERT 3 155
FIGURE 5.4 NVIVO CODING WORD FOCUS FOR EXPERT 4 156
FIGURE 5.5 NVIVO CODING WORD FOCUS FOR EXPERT 5 156
FIGURE 5.6 NVIVO CODING WORD FOCUS FOR EXPERT 6 157
FIGURE 5.7 NVIVO CODING WORD FOCUS FOR EXPERT 7 158
FIGURE 5.8 NVIVO CODING WORD FOCUS FOR EXPERT 8 159
FIGURE 5.9 NVIVO CODING WORD FOCUS FOR EXPERT 9 160
FIGURE 5.10 NVIVO EXPERT REVIEW THEME CONTEXT CHART SHOWING MAJOR THEME FOCUS AS DIFFERENT SIZE AREA 164
FIGURE 5.11 ADAPTIVE WEIGHTING AND CONTEXT AWARENESS, NVIVO EXPERT CODING 166
FIGURE 5.12 ANTI-SPOOFING AND ATTACK RESISTANCE NVIVO EXPERT CODING 167
FIGURE 5.13 EDGE VERSUS CLOUD PROCESSING NVIVO EXPERT CODING 168
FIGURE 5.14 ENVIRONMENTAL ROBUSTNESS AND PPE CONSTRAINTS NVIVO EXPERT CODING 170
FIGURE 5.15 EXPLAINABILITY AND CONFIDENCE TRANSPARENCY NVIVO EXPERT CODING 171
FIGURE 5.16 MULTIMODAL INTEGRATION NVIVO EXPERT CODING 172
FIGURE 5.17 POLICY & COMPLIANCE NVIVO EXPERT CODING 173

FIGURE 5.18 REAL-TIME PERFORMANCE AND LATENCY NVIVO EXPERT CODING 174
FIGURE 5.19 SIMULATION VS REALITY FROM NVIVO EXPERT CODING 175
FIGURE 5.20 WORD FOCUS FOR THE THEMATIC ANALYSIS FROM NVIVO 176
FIGURE 5.21 THEMATIC ANALYSIS FROM NVIVO MATRIX CODING 177
FIGURE 5.22 ARTEFACT 3 FULL FRAMEWORK 183
FIGURE 7.1 INDUSTRIAL EXPERT STUDY. 238
FIGURE 7.2 SECOND LIFE EXPERIMENTAL SCENARIO 260
FIGURE 7.3 GATE AND OUTPUT TEST 260
FIGURE 7.4 BLENDER CURATED BIOMETRIC MACHINE 261
FIGURE 7.5 AVATAR 1 261
FIGURE 7.6 AVATAR 2 262
FIGURE 7.7 AVATAR 3 262
FIGURE 7.8 AVATAR 4 263
FIGURE 7.9 AVATAR 5 263
FIGURE 7.10 AVATAR 6 264
FIGURE 7.11 INDUSTRIAL FACE MASK 264
FIGURE 7.12 INDUSTRIAL FACE MASK & HEAVY LOAD 265
FIGURE 7.13 INDUSTRIAL FACE MASK & HELMET 265
FIGURE 7.14 LOWLIGHT, FASTMOVE & HEAVY LOAD 266

TABLES OF TABLES

TABLE 1.1 REASON TO AUTHENTICATE....2
TABLE 2.1 PRISMA METHOD IDENTIFYING QUESTIONS. 13
TABLE 2.2 SUMMARY OF DIFFERENT TYPES OF IIOT ARCHITECTURES 19
TABLE 2.3 SHOWS IIOT RISKS, THEIR SOURCES, AND THEIR TYPES. 20
TABLE 2.4 SUMMARY OF SECURITY CHALLENGES IN IIOT AND IOT.....21
TABLE 2.5 SUMMARY OF THE TYPES OF ATTACKS IN DIFFERENT LAYERS.....23
TABLE 2.6 ACCESS CONTROL TYPES AND DEFINITION. 26
TABLE 2.7 PREVIOUS AUTHENTICATION MECHANISM....27
TABLE 2.8 DIFFERENT TYPES OF MULTIFACTOR ALGORITHMS AND THEIR DEFINITION31
TABLE 2.9 PREVIOUS WORK SHOWED THE BIOMETRIC PRE-PROCESSING STAGE. 36
TABLE 2.10 TYPES OF THE REGION OF INTEREST. 36
TABLE 2.11 PREVIOUS WORK DONE USING FEATURE EXTRACTION. 38
TABLE 2.12 BIOMETRIC FACTORS AND THEIR EXPLANATIONS: ADAPTATION (KIRAN ET AL., 2018, P. 429). 39
TABLE 2.13 BIOMETRIC TRAITS PERFORMANCE COMPARISON (OLOYEDE ET AL., 2016, P. 7542) 40
TABLE 2.14 PREVIOUS BIOMETRIC WORKS: BIOMETRIC MECHANISM. 41
TABLE 2.15 SUMMARY OF CONTACTLESS SCALE WEIGHTING 54
TABLE 2.16 SUMMARY OF BIOMETRIC EVALUATION SCALE....54
TABLE 2.17 COMPARISON WITH VIRTUAL ENVIRONMENTS (ONDREJKA, 2008) 62
TABLE 2.18 SUMMARY OF THE PROBLEM FROM THE RESEARCH GATHERED FROM SECTION 2.4.2 AND SECTION 2.4.3. 65
TABLE 2.19 SUMMARIES OF BIOMETRIC TRAITS DRAWBACKS....66
TABLE 2.20 BIOMETRIC ACCESS CONTROL DRAWBACK....67
TABLE 3.1 HCI ISSUES AND PROBLEM FEASIBILITY TABLE FROM SECTION 2.9 76
TABLE 3.2 BIOMETRIC ACCESS CONTROLS ISSUES AND PROBLEM TABLE FROM SECTION 2.9 76
TABLE 3.3 SUMMARIES OF FOCUS SIMILAR STUDIES....78
TABLE 3.4 SOCIO-TECHNOLOGICAL SIMILAR STUDIES 80
TABLE 3.5 COMPARISON TABLE BETWEEN DESIGN SCIENCE AND DESIGN THINKING METHODOLOGY 84
TABLE 3.6 SHOWS THE ARTEFACT 1 TESTING OBJECTIVES.....101
TABLE 3.7 SHOWS THE TEST EXECUTION. 102
TABLE 3.8 SIMULATION CONSTRAINT COUNT 104
TABLE 3.9 SHOWING WHICH SL-MEASURABLE METRICS CORRESPOND TO WHICH BIOMETRIC TRAIT. 108
TABLE 3.10 RELIABILITY SCORE DEFINITION....112
TABLE 3.11 NORMALISED WEIGHT TERM DEFINITION 112
TABLE 3.12 EXAMPLE OF FUSION SCORE TABLE 113
TABLE 3.13 FUSION SCORE TERM DEFINITION....113
TABLE 3.14 ARTEFACT 2 EXPECTED OUTPUT....119
TABLE 4.1EXPERIMENTAL DATASET SUMMARY 126
TABLE 4.2DISTRIBUTION OF TRIALS 127
TABLE 4.3 PASS / FAIL DISTRIBUTION 127
TABLE 4.4 EFFICIENCY VS CONSTRAINT COUNT 128
TABLE 4.5 MEAN BIOMETRIC SCORES BY CONSTRAINT COUNT 128
TABLE 4.6 PASS RATES BY AVATAR 129
TABLE 4.7 AVATAR AUTHENTICATION SUMMARY 130
TABLE 4.8 ISO STANDARD ASSUMPTION TABLE 131

TABLE 4.9 EFFICIENCY BY CONSTRAINT LEVEL....132
TABLE 4.10 TRAIT SCORE DECAY WITH PERCENTAGE REDUCTION....133
TABLE 4.11 THE OVERALL OUTCOME DISTRIBUTION FROM THE SECOND LIFE EXPERIMENT 134
TABLE 4.12 CROSS-AVATAR ANALYSIS 135
TABLE 4.13 BEHAVIOURAL CLASSIFICATION....135
TABLE 4.14 DEFINITION OF TERMS FOR FRR....136
TABLE 5.1 LIST OF EXPERTS 151
TABLE 5.2 THEMATIC REVIEW/ANALYSIS OF THE 9 EXPERT REVIEWS USING NVIVO ..161
TABLE 5.3 ZONES AND SECURITY LEVELS....179
TABLE 5.4 EXPERT FEEDBACK IMPACTED ON ARTEFACT 3 DESIGN ELEMENTS 181
TABLE 6.1 EVIDENCE MATRIX....197
TABLE 6.2 ISO MAPPING TO ARTEFACT 3 199
TABLE 7.1 ARTEFACT 2 AND ARTEFACT 3 COMPARISON TABLE FROM SECTIONS 4.5 AND 5.5 208
TABLE 7.2 EXPERIMENTAL RESULT....245

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

This research was conducted in accordance with the principles of academic integrity and ethical research practices. I fully acknowledge any assistance received during the completion of this dissertation. Generative AI technology, specifically Chat GPT, Microsoft Copilot (provided by AUT) and Grammarly, is used only for the limited purposes of:

- Organising non-substantial content
- Editing and proofreading for clarity
- Supporting idea generation

All AI-generated content has been thoroughly analysed, critically reviewed, edited, and fact-checked by the author. The research design, data analysis, and formulation of the findings are entirely the original work of the author. Where applicable, AI-generated contributions have been appropriately cited.

I take full responsibility for the accuracy, originality, and integrity of this research report.

Francis Ebere Anyanka

Publications

Anyanka, F., Cusack, B. Lutui, R. (2027). “Contactless Biometric Access Control for IIoT Work Systems”, *Journal of Computers & Security* (Submitted).

Artificial Intelligence Declaration Template

Artificial Intelligence Guidelines:

Artificial Intelligence (AI) tools, including generative AI tools approved for use by AUT (AI Tool Register), can be used as learning tools when preparing to write your research proposal or research component. AI tools also have capability to assist with data modelling, data analysis and data visualisation. However, the research component you submit for examination must be substantively your own work. AI tools cannot solely be used to generate content when writing or creating an artwork/artefact, as this constitutes plagiarism. The formal guidelines for appropriate use of AI on the AI Hub must be followed. Also refer to the Using Artificial Intelligence in your Research: Self-Assessments, Checklists, and Sample Text, for examples and sample text.

If you do plan to use AI tools, this declaration should be submitted with the initial research proposal, Confirmation of Candidature, and when you submit your research component for examination. You must complete the template below for each AI output used detailing the following:

- **Chapters where AI was used in any way**
- **Purpose of AI Use**
- **AI Tool(s) Used**
- **Prompts Used**
- **Post-AI Processing Methods**

Specify the chapter number(s) in your research proposal/research component where AI was used.	
Chapter number(s):	**4 (Experiment second life testing for Artefact 1)**
Briefly explain why the AI tool was used (e.g., idea generation, summarization, data analysis, image creation, etc.).	
Purpose of AI Use:	Used to help with coding for the Lindel scripting language for Second Life VR software, as I am new to the scripting language.
Clearly state the AI tools used.	
AI Tool(s) Used:	**ChatGPT**
Prompts or queries entered into the AI tool (only the instructive portion of the prompt is required). Include all relevant variations.	
Prompts Used:	**Replicate biometric features as dummies one by one, testing avatars for them. Also, do I need to create these biometric features, or can I just add a code to the avatar's skin? Please give me step-by-step instructions and code for these one-by-one biometric features on Second Life A full Administrator HUD Buttons: Approve, Reject, List, Open Gate, Close Gate 2. A logging system exporting all events to a CSV file 4. A biometric "spoof detection" simulation layer. Also, I need codes for the Auth gate.**
A summary or description of the AI-generated output. (Optional: attach output in an appendix.)	
Output Received:	**Lines of code and my prompting a lot of refinement to the output till I got a working code to my specification**
Describe how the AI output was used, edited, or transformed.	
Post-AI Processing Methods:	**The code was examined and then run through Second life sandbox and simulated to give the actual result final result is in appendix**

You may use this free text box to explain the intent for the use of the AI generated content. *For example, rather than stating what prompt(s) were used, you may articulate the purpose for which the prompt was used (supported by examples) here:*
For coding purposes.

STUDENT DECLARATION

By signing you are confirming that the AI use stated in the table(s) above are accurate and follow AUT's recommended guidelines detailed in the AI Hub and Postgraduate Handbook.				
Student Name:	**Francis Ebere Anyanka**	**Signature:**	**Date:**	**17/06/2026**

Acknowledgements

Completing my Doctor of Philosophy (PhD) at the Faculty of Design and Creative Technologies at the Auckland University of Technology (AUT) is one of the greatest challenges I have had to overcome. I am very glad that this journey has come to an end, as it was a make-or-break one mentally, financially, and otherwise. During this research/studies, I have learnt new skills and knowledge, elevated my discipline, developed new ideas, and had to learn to use new tools. I would like to thank numerous people for dedicating their time, advice, and endless support towards the completion of my PhD study.

I am very grateful to my supervisor/father figure, Prof Brian Cusack, for his unmeasured commitment, his belief in me, his encouragement when I almost gave up, his continuous support, leadership, guidance and patience throughout the research. As a matter of first importance, I would like to express my gratitude to GOD for giving me the strength to finish this task effectively. I likewise need to value my youth pastor, Dr and Dr Mrs Ekundayo, Dr Esther, Dr Feggy, Sam, and many others for their help in helping me understand the fundamentals of the task. Ethically and monetarily, I might likewise want to thank my mom, Pastor Mrs F.D. Anyanka, for her love, kindness, and support throughout my life. At long last, I need to express my appreciation to my dad, Rtd Maj C.E Anyanka, my siblings (Sam Heavens, Henry Heavens, Victor Heavens, Janefrancess, Marietta, and all my beautiful Whanua), and my great companions who bailed me out and gave me encouragement and inspiration when I contemplated surrendering. God bless you all for your support, one way or the other, which you have rendered to me in times of adversity.

Ethics Exception

Exceptions to Activities requiring AUTEC approval (6)

The following activities do not require AUTEC approval: *"6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise".*

Reference:

http://www.aut.ac.nz/researchethics/guidelines-and-procedures/exceptions-to-activities requiring-autec-approval-6

LIST OF ABBREVIATIONS

Abbreviation	Full Term
ACs	Advisory Committees
AI	Artificial Intelligence
AI/ML	Artificial Intelligence / Machine Learning
APCERT	Asia Pacific Computer Emergency Response Team
APNIC	Asia-Pacific Network Information Centre
BAC	Biometric Access Control
CNN	Convolutional Neural Network
DCT	Discrete Cosine Transform
DDCT	Divergence-driven Consistency Training
DL	Deep Learning
DSRM	Design Science Research Methodology
DT	Design Thinking
DSS	Decision Support System
DWT	Discrete Wavelet Transform
ECG	Electrocardiography
EDI	Equity, Diversity, and Inclusion
EEG	Electroencephalography
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
FFT	Fast Fourier Transform
Ft	Features
GAN	Generative Adversarial Network
HCI	Human-Computer Interaction
HSV	Hue, Saturation, Value
IIoT	Industrial Internet of Things
IoT	Internet of Things
IVE	Immersive Virtual Environment
LSL	Linden Scripting Language
M.A.	Multi-Factor Analysis

MES	Manufacturing Execution System
MFA	Multi-Factor Authentication
ML	Machine Learning
Morphs	Avatar Morphological Features
MX	Matching Score Index (Fusion Metric)
P(success)	Probability of Successful Authentication
P(failure)	Probability of Failed Authentication
PLC	Programmable Logic Controller
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PRISMA-P	Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols
RE	Requirements Engineering
ROI	Region of Interest
RNN	Recurrent Neural Network
SL	Second Life
S/N	Serial Number
SVM	Support Vector Machine
TOTP	Time-Based One-Time Password
VR	Virtual Reality
XAI	Explainable Artificial Intelligence
ZEMFA	Zero-Effort Multi-Factor Authentication

Chapter 1: INTRODUCTION

1.0 INTRODUCTION

The use of the Industrial Internet of Things (IIoT) is just one instance where digitisation has created a new reliance on connected systems in the world of industry. These systems have revolutionised the way industries work, making them more automated, real-time monitored and intelligent industries. However, with all the advancements come a crucial question: how can secure, reliable authentication be achieved in dynamic, unpredictable environments? Industrial and virtual environments are more dynamic than controlled laboratory environments, where changes in lighting conditions, helmet or mask, carrying heavy loads, wearing industrial-grade gear, and users moving very fast, just to name a few factors, affect security system performance.

Conventional authentication methods, such as passwords and static biometric templates, do not cope with this variation. Biometric systems offer security improvements when using something unique to a human being, but many current systems assume the system will remain stable and not change when it does. As a result, effectiveness decreases in practical applications. This means there is a disconnect between theory and real-world applications, which is even greater in an immersive, distributed setting such as a virtual platform or an IIoT system.

In this study, the gap is addressed by proposing a context-aware, multi-modal and adaptive biometric authentication framework. It is not the traditional way of seeing authentication as a process that takes place once and for all, but as a (temporal) process that is influenced by the environment and is most apt to give preference to the most authentic input at any given time. The strategy is efficient and effective, with a strong focus on system-level design and performance, but it doesn't prioritise Human-Computer Interaction, and this is the first trade-off this research also seeks to address.

The research is conducted systematically. starting with laying a theoretical background (Artefact 1) based on the literature review of the current state of the art regarding both biometric systems and multimodal fusion and secure authentication. This is followed by the design and implementation of an experimental system (Artefact 22) intended for testing under different conditions. Based on the results, potential drawbacks are identified, and an improved adaptive model (Artefact 3) is proposed to

overcome these drawbacks and enhance the system's resilience. The methodology approach presents a systematic development of theory, implementation, and improvement, which can be used to develop an authentication system as a solution.

1.1 WHY AUTHENTICATION IS NEEDED (E2 REQUIRED 1)

Industrial sites depend on operational technology (OT)which is the control systems, machinery and safety systems that run physical processes (Stouffer et al., 2023). A wrong action by an unidentified or unauthorised person can damage equipment, stop production or injure people. IEC 62443 lists identification and authentication control as its first foundational requirement (IEC, 2013), and NIST SP 800-82 Rev. 3 gives access control and authentication a central place (Stouffer et al., 2023). Four consequences make authentication unavoidable, and these are; physical harm from unauthorised setpoint or logic changes; competence and permit rules for cranes, forklifts, confined spaces and high-voltage areas; protection of the last safety layer, since bypass must be restricted and recorded; and accountability after an incident.

Table 1.1 Reason to Authenticate

System or task	Why authentication is unavoidable
Site gate	Controls who are on site; rollcall, trespass
Hazardous area, permit-to-work entry	Only trained, permitted people enter; site must know who is inside
SCADA/HMI, PLC workstations	Unauthorised setpoint or logic change can cause harm
Safety systems, E-stop override or bypass	Bypass removes the final protective layer
Cranes, forklifts, heavy plant	Only certified operators may drive
Tool and equipment stores	Accountability for loss
Remote and vendor access	External access is an attack path
Post-incident traceability	Investigation, regulation, insurance

1.2 THE PROBLEM & CONTEXT

Biometric authentication systems have long been associated with asserted security benefits, leveraging unique physical and physiological features of the human body,

including facial recognition, iris recognition, and voice recognition (Li et al., 2014a; Lipps et al., 2021; Bao et al., 2023). When used under controlled conditions, they are accurate and reliable. Most of the literature available today, however, focuses on biometric systems in ideal or laboratory conditions in which numerous factors can be completely controlled, including (but not limited to) light, user position, noise around the user, and so on (Miller et al., 2020; Dave et al., 2021; Miller et al., 2021). This results in a gap between theory and practice, especially in Industrial Internet of Things (IIoT) applications operating in dynamic, unpredictable environments.

There is no authentication in the industry or the real world that occurs in isolation. It exists as part of a system or architecture that includes humans, machines, the environment, and tasks. In attempting to verify, workers are allowed to wear personal protective equipment (PPE), such as a helmet, gloves, and/or face covering. A high percentage of them experience low light, dust, noise, and/or time limitations, and they may move faster than normal in their mode of operation. These factors significantly affect the quality of biometric input data, which in turn impacts system performance (Sisinni et al., 2018; Jain et al., 2022; Saqib & Moon, 2023). For instance, facial recognition fails when a person is wearing a mask or protective wear, or voice recognition fails in noisy areas like a factory, construction site, or similar locations (Lipps et al., 2021; Ren et al., 2022; Osanaiye et al., 2016; Oloyede et al., 2016).

The current biometric authentication systems are not context-dependent, and the majority of such systems operate based on static thresholds and decision rules, and assume that all elements entering the system are equally reliable. However, as the literature on multimodal biometric fusion suggests, the performance of different biometric characteristics depends on the conditions (Oloyede et al., 2016; Minaee et al., 2019). For instance, facial recognition works well in well-lit conditions but is not accurate in occluded conditions, whereas voice recognition is accurate in occluded conditions but is not accurate in noisy conditions. However, several systems will treat them as a single identity and reach an incorrect or inefficient authentication conclusion.

Not only the technical performance, but also the socio-technical aspects regarding people's interaction and behaviour are in question in IIoT. In many IIoT environments, authentication is not the main task but is performed in parallel with the main tasks. Engineers do not care about optimising the capture of any biometric because they just want to get the job done quickly and safely. This is then combined with the human factor and any differences in positioning, rushed interactions, or

evolving usage patterns (Jain et al., 2022; Sadeghi et al., 2015; Saqib & Moon, 2023). Different research highlights that usability and efficiency, as defined in frameworks such as ISO 9241-11, are critical to system adoption, yet many biometric systems fail to account for these human factors.

Real-life examples further emphasise the problem. In combination with facial recognition technology, safety goggles can prevent workers wearing helmets from repeatedly entering construction zones, and cause delays and disgruntled workers. In manufacturing operations, humans operating heavy equipment may not be able to accurately interact with the authentication interface, thereby affecting the ability to successfully authenticate. Certain operations, such as coordination or warehouse operations, involve many people moving quickly and time-sensitive activities, which result in partial or poor-quality biometric capture. These problems not only hurt system efficiency but can also lead users to workarounds that entirely circumvent authentication mechanisms and compromise security.

Moreover, the increasing integration of IIoT systems means that authentication is no longer confined to a single point of access but is distributed across interconnected devices and platforms. This amplifies the impact of authentication failures, as they propagate across systems, affecting operational continuity and security.

Other important drawbacks noted in the literature were the use of only one biometric modality and/or static fusion techniques. Single-modal systems have the disadvantage that they are constrained by the environment regarding such a trait. The multimodal systems are more resilient, but in fact, many of them are statically fused, and in both types of systems, all the biometric inputs are treated as equally valuable. This is not a method that takes into account the changing environment in which real-world data is collected, and/or the different reliability of each of the inputs.

Therefore, even with sufficient and proper information, existing systems are subject to failure. In a static system, for instance, if one biometric factor is corrupted by environmental factors, the system may give equal weight to other, more reliable factors, leading to an incorrect decision. This impacts both accuracy and efficiency, as users are required to log in multiple times.

To conclude, a problem to be solved in this research is not only to enhance the accuracy of biometrics but also a socio-technical problem. The current authentication systems are not able to:

- Be flexible in changing or changing environmental conditions.

- Include consideration of the human operations and behaviours.
- Be capable of making decisions dynamically depending on the level of certainty of the data.

1.3 THE RESEARCH QUESTIONS & METHOD

To address the socio-technical challenges outlined in Section 1.1, this study is guided by a set of focused research questions that progressively examine both the system's technical performance and its behaviour under real-world conditions. These questions are designed not only to evaluate how well the system works, but also to understand why it behaves the way it does when exposed to environmental and human factors.

The baseline study is obtained by analysing the performance of a biometric fusion authentication system in ideal conditions, which is the first research question (RQ1). This is very important as it allows the system to mask the external noise and disturbances, to correctly evaluate the intrinsic functions of the model, and to enable the evaluation of other important system functions, such as the accuracy of the biometric feature extraction and fusion. It does this by mimicking conditions reported in the literature (Chapter 2), which, in turn, constitute a controlled environment.

The second research question (RQ2) brings in environmental/contextual constraints and shifts the focus from a theoretical to a practical approach to the study. This is where the system is tested under conditions most similar to those of typical IIoT devices, such as low light, occlusion, and motion. It is a key part of a gap analysis, particularly for efficiency and reliability. This step is critical in highlighting the gap between expected performance Artefact 1(A1) and observed performance Artefact 2(A2), particularly in terms of efficiency and reliability.

RQ3 aims to identify the constraints affecting system performance as a follow-up to this. The constraints differ across biometric systems, where occlusion is a severe problem for face recognition, whereas noise is a severe problem for voice recognition. These factors are isolated and studied, providing a better understanding of their interactions with the system across different environmental and human factors. This also aligns with the socio-technical viewpoint, which considers the limitations of technology and the human/environmental conditions.

The research aims to improve the performance of systems in constrained environments, and the questions address this aim. The questions go beyond enhancing each biometric modality to the possibility of improving the system's effectiveness,

particularly in decision-making. It is very similar to Artefact 3(A3), the artefact of building adaptive mechanisms (adaptive weighting) and context-aware decision logic.

The present study is based on the Design Science Research Methodology (DSRM) to systematically address the above questions. It is analytical and constructive research aimed at designing, implementing, and developing an artefact to solve a real-life problem. There are three interrelated stages of the methodological process:

- **Artefact 1 – Theoretical Framework Development (Figure 2.3)**
  After completing Chapter 2, the theoretical framework is developed as Artefact 1 (Artefact 1) (Theoretical framework development), where the literature on biometric authentication, multimodal fusion, and IIoT systems is synthesised. The Artefact 1 concept explains the behaviour of the system, i.e., the accuracy, robustness, and efficiency of the system, and stands as the theoretical foundation of the study.
- **Artefact 2 – System Design and Experimental Evaluation (Figure 4.6)**
  Design and development of an experimental system are carried out through the following steps (Artefact 1). This system is a mix of several biometric inputs, and the performance of the different biometric inputs under different conditional constraints. Importantly, this stage models ‘real-world' problems by imposing constraints on the system and assuming a different constraint scenario, so that the system is observed and analysed to create a new framework or architecture that is improved upon in the next phase or step.
- **Artefact 3 – Adaptive System Refinement (Figure 5.22)**
  Artefact 3 is based on the results of Artefact 2 Testing. The study does not view performance limitations as isolated problems but rather considers them part of a system design problem. In this context, Artefact 3 suggests an adaptive architecture that has knowledge of the environment and context and can change its shape and/or function. To overcome the major drawbacks mentioned above, Artefact 3 will propose a more suitable dynamic architecture that is sensitive to the environment and context, relying on expert knowledge in these domains. These inputs are then used to shape and iterate a new architectural /framework design or product with a view to solving the research problem or gaps.

The methodological design sufficiently solves the problem as described in section 1.1. In the study, various kinds of challenges (controlled (RQ1), constrained (RQ2), and

system improvement that can be addressed by a biometric authentication system are analysed (RQ3). What is more important it recognises that the problem should be solved not by making the algorithms better, but by making the systems change their behaviour in response to human behaviour and environmental change. This way, the research questions and methods are not isolated from the problem, ensuring the research is technically valid and relevant to it.

1.4 THE FINDINGS

The findings of this study relate to the socio-technical problem outlined in Section 1.1. that also considers the practical constraints, human interactions, and system limitations in IIoT. This has the technical advantage of producing relevant and meaningful results for potential implementation.

First, the study establishes that the biometric fusion system performs well under ideal conditions. Similar to the literature mentioned in Chapter 2, in controlled situations, high levels of accuracy are typically reported. In these cases, the biometric data are either identifiable or invulnerable to external influences. In context, this means that an essential concept is that there is no fundamental problem with the underlying technology. The system can be used to accurately and efficiently authenticate under minimal environmental and human influences. But when considered in the context of the research gaps or problem and the research question outlined in sections 1.1 and 1.2, this also raises a caveat. Industrial and Operational facilities do not typically have optimal conditions. The system is theoretically sound and will rely on its sensitivity to change.

Second, Impacted as the number of constraints increases from none to five. This directly relates to the issues as stated in the problem area. Several problems, including occlusion, inadequate lighting, and motion, reduce the quality of biometric inputs and result in higher authentication failures and lower accuracy. Very importantly, this is not just technically, but also socio-technically. The longer the task, the more re-authentications and delays will be faced, which may affect the workflow and lead to lower user confidence in the system. The system's inability to adapt to these conditions confirms the gap identified in existing approaches.

The third is that there are restrictions that result in the poorest performances, for instance, occlusion and lighting. This aligns with the problem analysis, which indicated that these factors directly affect the capture of the biometric feature. In

industrial applications, there are such restrictions that cannot be ignored. Workers should wear protective equipment, and the lighting requirements of the system can often be influenced by the operation. This confirms the socio-technical aspects of the problem and demonstrates that human practices (e.g., safety compliance) and the environment, such as weather, are more likely to impact the performance of a system than the algorithm itself.

The fourth finding highlights that while multi-modal biometric fusion improves reliability, its effectiveness is limited by static decision-making mechanisms. Even when multiple biometric inputs are available, the system does not adjust their importance based on context. As a result, degraded inputs still negatively influence the overall decision. Within the problem frame, this finding is particularly significant. It confirms that the limitation lies not only in data acquisition but in how the system interprets and prioritises information. This directly supports the argument that improving authentication requires a shift from static to adaptive system design.

Finally, the study shows that the adaptive strategies implemented in Artefact Artefact 3 provide a feasible way to improve context awareness, dynamic weighting, and flexible decision logic and to increase the system's ability to handle variability. Socio-technically, this would allow the system to be more responsive to real-world conditions, reduce inefficiencies, and maximise effectiveness. To sum up, the results overall support the problem statement in Section 1.2:

- The system works well in the controlled environment but fails in the natural environment.
- Environmental and human factors have a very great influence on performance.
- Non-dynamic system designs don't take into account variability.
- There needs to be adaptive mechanisms to improve efficiency/effectiveness.

The results show that improving biometric accuracy is not just about accuracy but also about making systems reliable and resilient in the interdependencies among humans, technology, and the environment.

1.5 THE THESIS STRUCTURE

This section explains the thesis structure and explains what to expect in each chapter.

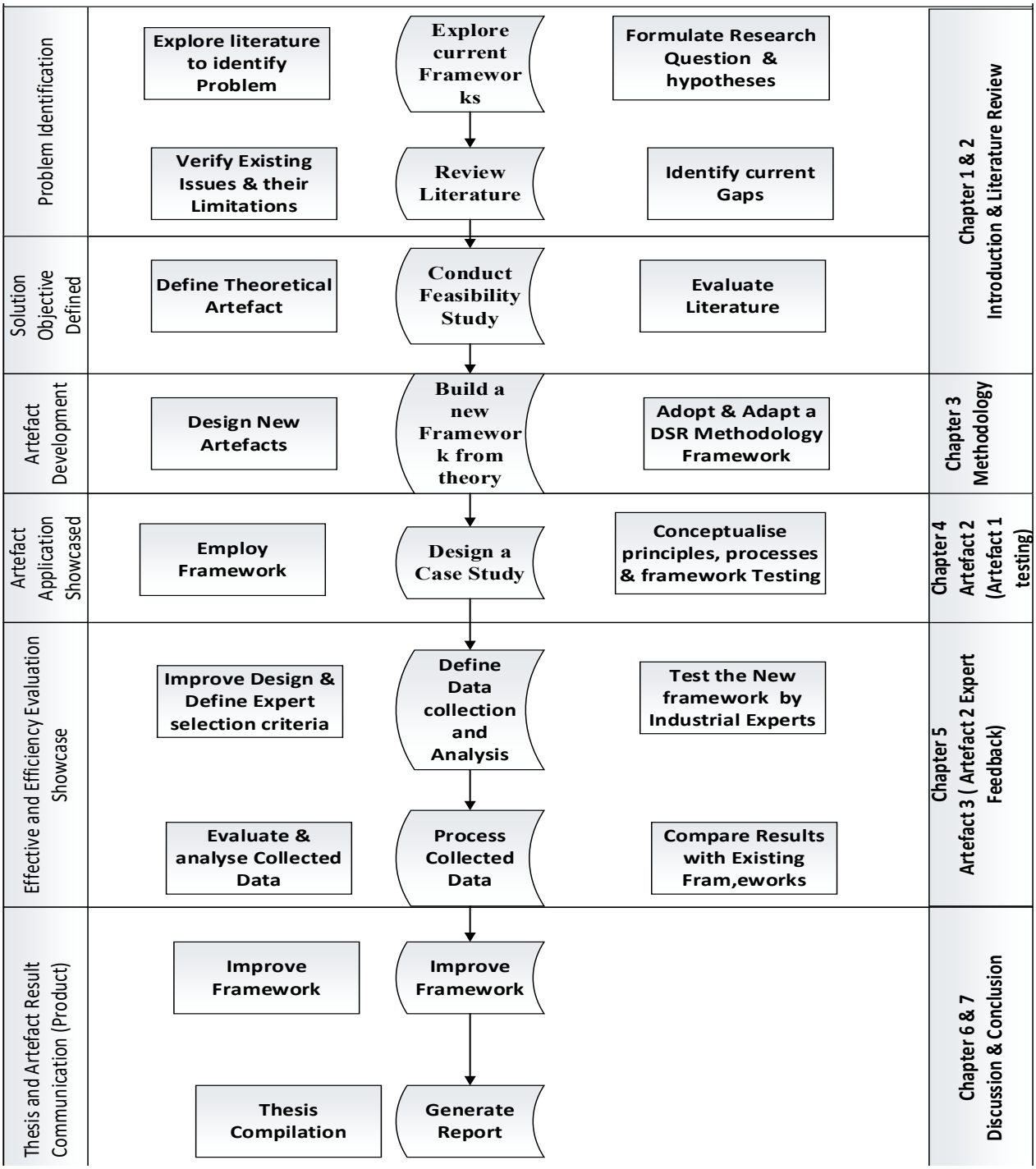


Figure 1.1Thesis structure

This thesis is organised to reflect a clear progression from problem identification to solution development, evaluation, and refinement. Each chapter builds logically on the previous one, ensuring that the research remains coherent and grounded in both theory and practice, as shown in Figure 1.1.

- **Chapter 1 – Introduction**

  This chapter provides a background to the study. It sets the research issue in a socio-technical context, presents the motivation and proposed solution,

introduces the research questions and methodology, summarises the key findings, and outlines the general structure of the thesis.

- **Chapter 2 – Literature Review (Artefact 1: Theoretical Foundation)**
  This chapter discusses in detail the latest research and analysis on biometric authentication, multi-modal fusion, IIoT systems, and virtual environments. It identifies existing solutions, explains why they are not suitable in real-world conditions, and develops the theoretical framework (Artefact 1) that should be followed when conducting the research.
- **Chapter 3 – Methodology and System Design**
  This chapter provides an introduction to the research approach, grounded in the selected research methodology. It provides a description of how Artefact 1 is divided into measurable parts, as well as the design and implementation of the experimental system. Some guidelines for assessing metrics that help determine system performance (efficiency and effectiveness) are also included.
- **Chapter 4 – Experimental Results (Artefact 2: System Evaluation)**
  The results of the implemented or experimental system are reported in this chapter, both in ideal and constrained conditions. It provides comprehensive feedback on system performance, enabling identification of the impact of system factors (environment & context) on authentication.
- **Chapter 5 – Artefact 3: Adaptive System Refinement**
  The design presented in this chapter is an improved version of that in Chapter 4. It describes the expert expectations and feedback used to address the limitations listed in Artefact 2, thereby driving an iteration and improvement to the final artefact.
- **Chapter 6 – Discussion and Research Contributions**
  This chapter summarises the results, answers the research questions, and evaluates the hypotheses. It situates the results in a socio-technical perspective whilst highlighting the theoretical and practical implications of the research.

The sequence of chapters provides a logical flow of the research from problem → theory → implementation → evaluation → refinement → contribution, allowing the reader to follow the research's development processes.

1.6 CONCLUSION

This chapter presents the main problem to be addressed for this research: “Current biometric authentication systems have limited capabilities for working effectively in dynamic real-world environments under constrained environments, especially in the context of IIoT.” The current systems have demonstrated good performance in the laboratory setting but fail when faced with environmental and people constraints. There is some degree of variability and occlusion, as well as unaccounted-for effects of activities or operational constraints.

The research has shown that this limitation is not merely technical but socio-technical, requiring a link between the system's design, environmental conditions, and people's behaviour. The study, in turn, suggests a biometric authentication framework that adapts to context, incorporates multimodal inputs, and employs flexible decision-making mechanisms. The research questions were introduced, and the research procedure was demonstrated from the theoretical foundations (Artefact 1) to the experimental evaluation (Artefact 2), followed by a discussion of the expert adaptable refinement (Artefact 3). The key findings were summarised, highlighting the importance of flexible authentication. This overall is meant to set the course and the relevance of the research in this chapter. A step back is needed to consider improvements in biometric accuracy and to discuss the authentication system design that will function in the socio-technical challenges of the real world. The literature survey in the next chapter serves as a basis for the proposed approach and provides an overview of the theories that will underpin it.

Chapter 2: LITERATURE REVIEW

2.0 INTRODUCTION

Chapter 2 analyses the existing literature on the Industrial Internet of Things (IIoT) and the security mechanisms that use biometric access controls. The research aims to use biometric access controls in remote (onsite and online) locations—for example, construction sites and shipping yards. The literature was identified, screened and selected following the PRISMA 2020 guideline (Page et al., 2021), which structures a systematic review into identification, screening, eligibility and inclusion. The aim of Chapter 2 is to analyse available documentation from other researchers, identify gaps in the body of knowledge, and identify issues and problems related to IIoT and Biometric access control.

Chapter 2 has nine sections to review IIoT using Biometrics as the access control mechanism. Section 2.1 is the Delphi literature selection method. It shows how and why the research materials and content used for this research were selected, and how search keywords, catchphrases, or sentences were used to find materials. Section 2.2 defines the IIoT sector and its flaws in existing security provisions. Section 2.3 lists the access control mechanisms, analyses current access controls, and identifies which are suitable for identification, authentication, and validation. Section 2.4 introduces the Biometrics trait and its authentication process. The deep learning capabilities of biometric features such as fingerprints, irises, faces, palmprints, gaits, voices, and ears are covered in Section 2.5. The usefulness of biometrics is reviewed in Section 2.6. The challenges and issues mentioned in previous parts are summed up in Section 2.7. The chapter's contribution is reviewed in Section 2.8, which also offers a link to Chapter 3.

2.1 LITERATURE SELECTION PROCESS

This section examines two approaches to selecting the right literature. To determine which literature selection method is most appropriate for this study, this section examines the Delphi method (Bibri et al., 2022) and the PRISMA (Page et al., 2021) framework. The PRISMA way is often used when writing about systematic reviews and meta-analyses. It entails a methodical procedure for finding, evaluating, and incorporating pertinent research into a systematic review (Moher, 2009). The Delphi Method is a recognised method frequently utilised in the technological field and is

well-liked by researchers for decision-making through the consensus process. The Delphi method is a structured way for experts to communicate their methods to obtain expert consensus (Holsapple et al., 2002). The RAND Corporation first introduced it and is now used across many areas and industries to predict, measure, and make decisions (Okoli & Pawlowski, 2004).

The Delphi Method and the PRISMA technique have been used in different domains of engineering, management, business, the humanities, physical science, and the Industrial Internet of Things (IIoT) (Saffie et al., 2016; Page et al., 2021). The following sections outline the differences between Delphi method and the PRISMA method. The Delphi method's effectiveness has given researchers confidence to use it across different study designs, as it demonstrates flexibility and adaptability. Although it offers many rewarding approaches, it also has some disadvantages.

According to Ji et al. (2013), operations or research using the PRISMA methodology are deemed expensive and time-consuming. Surveys and studies assessing PRISMA's impact have found that adherence to its guidelines improves the quality of reporting in systematic reviews.

Table 2.1 PRISMA method identifying questions.

Identifier	Question
PQ1	What is the IIoT, and what are its derivatives?
PQ2	What is the IIoT context being referred to in this literature?
PQ3	What are the challenges of Biometric access control implementations in IIoT?
PQ4	How can Biometric traits be practical and efficient for access control in the IIoT sector?

The iterative Round 1 identifies vital search words. These are IIoT, access control mechanisms, biometric access control mechanisms in IIoT, biometric mechanisms, and deep learning. A preliminary search is conducted across the selected digital libraries, including IEEE, Google Scholar, ScienceDirect, Elsevier, and Springer. The iterative Round 2 verifies the quality and relevance of the previous step's search results. The document abstract and conclusion are scanned for relevance to the questions PQ1, PQ2, PQ3, and PQ4 of Table 2.1.

The iterative Round 3 conducts relevancy matching and verification against the search results from the previous step. It examines the appropriateness of content,

research method, data analysis, and findings against the requirements for this research. Finally, iterative Round 4 determines which content is relevant to the study and selects it as a source for the literature review; otherwise, it is deemed irrelevant and discarded.

Figure 2.1 shows the application of PRISMA framework for this research, as adopted and used by Page et al., 2021.

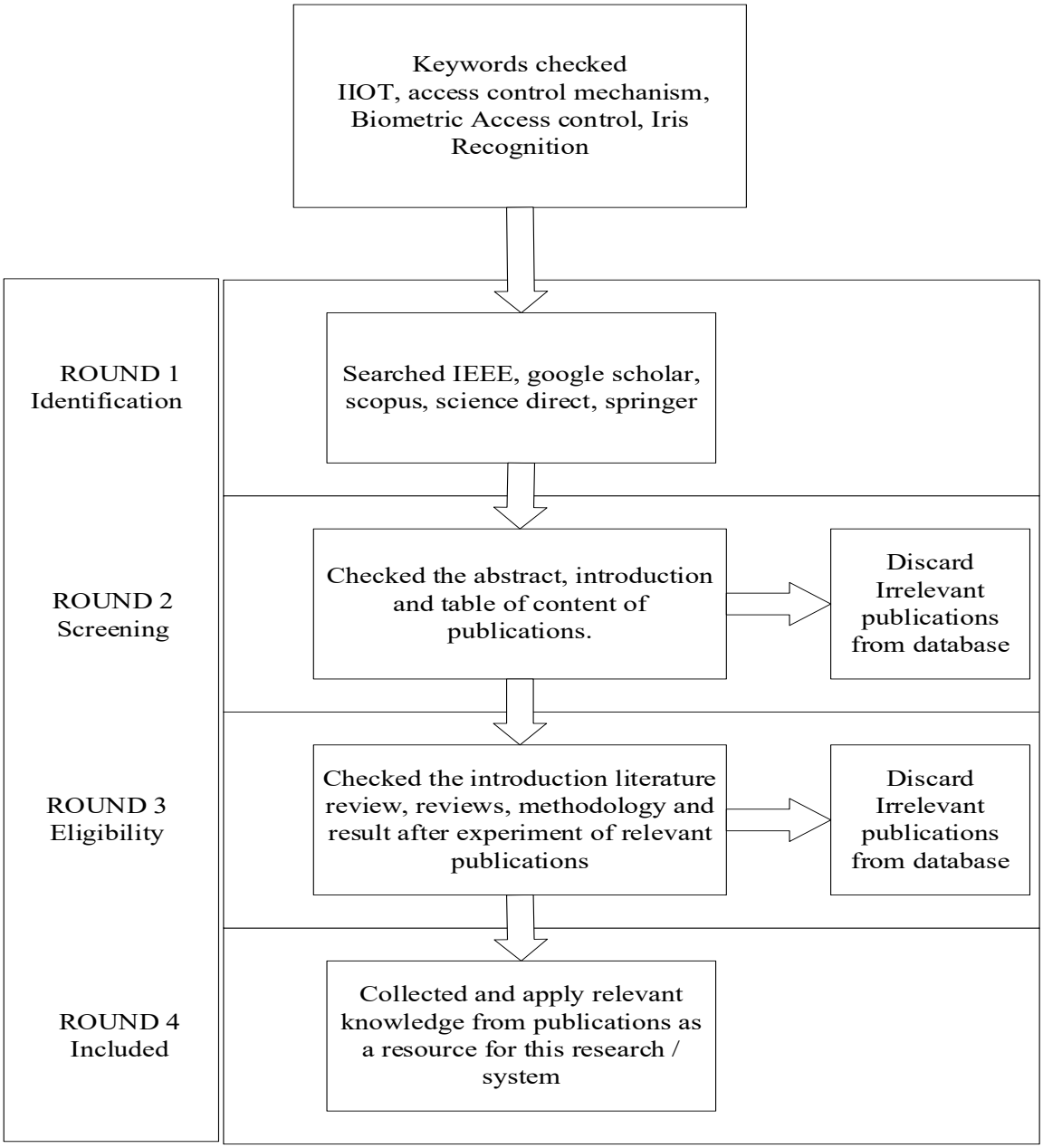


Figure 2.1 Prisma framework for literature selection.

2.2 INDUSTRIAL INTERNET OF THINGS (IIOT) DEFINITION

The Industrial Internet of Things (IIoT) is the result of advancing IoT development, design, and integration to fit the architecture of heavy machinery and complex industrial systems (Du & Zhen, 2022; Kedia et al., 2020). IIoT iterations have created

the Industrial Revolution by enabling high-speed mobility, high-reliability communication, low latency, and dense terminal node access in industrial environments. This essential technology (IIoT) contributes significantly to the Industrial Revolution (Yang et al., 2017; Islam et al., 2019).

The Internet of Things (IoT) was introduced to industrial environments to connect industrial systems and machines, ease user operations, and prioritise access control (Javaid et al., 2021; Zalozhnev & Ginz, 2023). Operations are conducted via the IoT platform and sometimes performed remotely to access industry resources (Du & Zhen, 2022; Berger et al., 2020). The IoT has aided IIoT's adaptability in companies and industries by automating operations. An industrial control system (ICS) comprises operational technology (OT) and information technology (IT) systems. The information technology (IT) system supports business needs through technological enablement, including servers and workstations. Operational technology (OT), primarily the machinery used in daily operations such as PLCs (Programmable Logic Controllers) and VFDs (Variable Frequency Drives) (Makrakis et al., 2021), is the foundation of the IIoT.

2.2.1 Industrial Revolution – Historical Approach

Numerous developments throughout the industrial revolutions have shaped the progression of modern industry and have been categorised into four stages or eras (Wicha et al., 2023; Zalozhnev & Ginz, 2023). German industries were crucial to the digitisation of the first revolution (Industry 1.0). People transitioned from human power to steam- and water-powered engines for mechanical production; the weaving loom was a sign of progress and a big step forward. This innovation was noted and called the first revolution (Kumar et al., 2023; Hofmann, 2017). Then, European and American technologies helped drive the second revolution, enabling the production of many goods using chemicals and electricity (Dickinson & Musson, 2022; Qin et al., 2016). In the age of electronics, the third revolution (Industry 3.0), the first programmable logic control system, was invented, and they adopted innovative approaches to getting work done faster to match the demand and supply curve. During this time, some management programs were created to improve productivity and effectiveness in the manufacturing process (Vaidya et al., 2018; Qin et al., 2016).

The Industry 4.0 era has seen rapid, competitive development, with artificial intelligence (AI) tools available to ease the creation of new inventions. With machine

learning-powered AI tools, dependable, life-changing industries have emerged through cyber-physical production systems (CPPS). The internet-based age has made it possible to interface time-saving and remote working with the industry, where these systems have the virtual environment running the industries with the rise of IIoT, virtual and physical worlds are the fourth revolution (Industry 4.0). Characteristics attributed to Industry 4.0 are human-human, machine-machine, and standard data exchange protocols for human-machine interactions (Alcácer & Cruz-Machado, 2019; Qin et al., 2016; Nakamura et al., 2018).

Xu et al. (2014) stated they had reviewed 306 IoT articles and noted that IoT began with the revolution in RFID technology and advanced with the invention of wireless sensor networks (WSN). This discovery enabled the interconnection between intelligent devices or nodes. Research on IIoT shows that the IoT and industry make up the IIoT, and its main challenges are managing energy, ensuring security, and providing an easy-to-use, adaptable platform (Petrenko et al., 2018; Alcácer & Cruz-Machado, 2019).

2.2.2 Context – IIOT

IIoT is a subset of IoT focusing on Operational Technology (OT), smart manufacturing, intelligent coordination, and smart cities. In contrast, the IoT encompasses a broader range of consumer devices related to retail and lifestyle (Tange et al., 2020). Sensors and devices embedded in equipment, machinery, and other systems collect data and transmit it to a centralised system using IIoT (Sisinni et al., 2018; Zhang et al., 2022). IIoT enables industrial processes to be monitored, analysed, and controlled in real-time. It also supports predictive maintenance, allowing businesses to detect and resolve problems before they cause downtime or equipment failure (Behrendt et al., 2017). While many technologies are classified as IoT (Internet of Things), not all are suitable for industrial use. Smart home devices, such as smart thermostats or voice assistants, may not apply to industrial applications as they fall under the IoT but are connected to the IIoT framework (Da Cruz et al., 2018).

On the other hand, IIoT-enabled sensors embedded in a machine to monitor its performance are part of the IIoT. The focus is on the heavy machinery industries, for instance, manufacturing companies like road construction, building construction, and shipyards. This research also focuses on a mix of educated and uneducated personnel in this space and on their interactions with IIoT (Sezer et al., 2018). IIoT benefits small

and medium-sized industries, IIoT is still implementable on a small scale to fit the industry's business specifications. The need for authentication in wireless sensor networks and on-site locations has been a concern for IIoT (Saqib & Moon, 2023; Yu & Guo, 2019).

2.2.3 Current Architecture

IIoT Architecture is designed and implemented in a complex manner, with various parts of the framework coordinated to move information across the system. It is designed to give and consume information in the form of data from external or internal sources (Berger et al., 2020; Mathur & Arora, 2020). This process constantly adopts a novel approach to its specification, as each IIoT framework differs, yet it maintains a similar structure. In IIoT, the conceptualisation phase is significant, as the framework depends on it as its foundation. In this context, semantics may impact the proposed technological systems by incorporating multidisciplinary knowledge of IIoT architectures (Cunha & Sousa, 2021; Xu et al., 2014; Sisinni et al., 2018).

When creating an IIoT architectural system, it is crucial to make it flexible and modular, capable of handling expansion and working with devices that may use different technologies (Al-Qaseemi et al., 2016; Zia et al., 2019). There are various architectural frameworks and references available from existing research on both IoT and IIoT that are insightful. Architecture is a widely used concept with a multilayered service structure at each level, depending on the chosen or conceptualised technologies, business goals, and technical requirements (Weyrich & Ebert, 2016). Xu et al. (2014) defined the IoT architectural framework with sensing, networking, service, and interface layers, in a hierarchical Architecture framework. Across different journals, the IoT and IIoT architectures differ based on industry-specific business and technological needs. While Al-Qaseemi et al. (2016), in a review of the issues regarding IoT, stated that IoT has two different styles of architectures, which are three-layer architectures (perception layer, network layer, and physical layer) and five-layered architectures (Al-Qaseemi et al., 2016).

Most researchers have modelled the IIoT architecture to resemble that of the IoT. For instance, Abosata et al. (2021) defined their architecture framework as consisting of four layers: the perception layer, network layer, processing layer, and application layer. The perception layer comprises sensors, cameras, robots, and machines, while the network layer provides connectivity via Bluetooth, Wi-Fi/IEEE

802.11, and 6LoWPAN. In the research, they focused on a Hybrid Architecture framework. The processing layer comprises algorithm-centred databases and servers for data refinement, operational transactions, and decision-making. Finally, the application layer manages standards and policies for end users, such as smart cities and intelligent manufacturing. The application, network, and perception layers are the three main abstract layers that comprise the IIoT systems (McGinthy & Michaels, 2019). Sarjan et al. (2022), utilising the Fog Computing Architecture framework, reviewed standardised IIoT architectures and found that IIoT architectures are three-, four-, and five-layered. The three-layered architecture consists of the perception layer (hardware, machines, and devices), the network layer (wireless networks, internet, optical networks, satellite networks), and the application layer (intelligent grids, smart city, smart consumption). The four-layered architecture comprises a field network, communication, terminal, and Master station. In this architecture, the field network and the terminal comprise the perception layer (three-layered architecture). The communication layer is the same as the network layer, and the master system layer is equivalent to the application layer. This architecture is used in power plants, operations systems, and state monitoring transmission lines.

Moreover, Zia et al. (2019) proposed a five-layered architecture for the Transactive Energy System. It comprises the user, energy management, market, communication, and regulatory layers; the energy management layer controls the system's operation. Zia et al. (2020) proposed a seven-level architecture. It shows that the problem with IIoT architecture is inherited from IoT architecture, requiring greater standardisation, as each industry sector designs its architecture to meet business needs.

2.2.4 Types of IIoT Architectures

The Industrial Internet of Things (IIoT) has proposed several architectures to facilitate the integration of various devices, sensors, and systems in industrial settings. Table 2.2 shows some common types of IIoT architectures. Table 2.2 presents different architectural approaches to designing IIoT systems that cater to various industrial applications and requirements. Researchers and practitioners often select or customise architectures based on specific use cases and constraints, as stated in section 2.2.

Table 2.2 Summary of different types of IIOT architectures

Architecture	**Description**
Hierarchical Architecture	Consists of multiple layers of interconnected devices and systems organised hierarchically. It typically includes field devices at the bottom layer, along with control, supervisory, and enterprise systems at higher layers (Xu, He, & Li, 2014; Wan et al., 2018).
Edge Computing Architecture	Edge computing architecture decentralises computation and data storage by pushing processing tasks closer to IIoT devices and sensors. This approach enhances data security, reduces latency, and enables real-time analytics (Satyanarayanan, 2017; Shi et al., 2016).
Distributed Architecture	A distributed IIoT architecture distributes computing tasks across multiple network nodes, enabling parallel processing and fault tolerance. It enhances scalability and flexibility in industrial environments (Gubbi et al., 2013; Xu et al., 2018).
Event-Driven Architecture (EDA)	EDA architecture processes real-time events generated by IoT devices and triggers automated responses based on predefined rules or conditions. This architecture supports event-driven decision-making and enables proactive maintenance (Luckham, 2011; Eugster et al., 2003).
Fog Computing Architecture	It extends cloud computing capabilities to the network's edge, bringing computation and storage closer to IIoT devices. It enables real-time data processing and analysis, reducing latency and bandwidth usage (Bonomi et al., 2012; Yi, Li, & Li, 2015).
Service-Oriented Architecture (SOA)	SOA architecture decomposes IIoT systems into modular services that communicate via standard protocols. It promotes the interoperability, reusability, and scalability of IIoT applications and components (Guinard et al., 2010; Panetto & Cecil, 2013).

Hybrid Architecture	The hybrid IIoT architecture combines cloud, fog, and edge computing to leverage each approach's strengths. It offers a flexible and adaptable framework for addressing diverse industrial requirements and challenges (Mahmud et al., 2020; Zhang et al., 2020).

2.2.5 Risks Associated with IIoT.

In general, IIoT is a much more complex framework than IoT (Berger et al., 2020; Bhamare et al., 2020; Zhang et al., 2023), so the risk assessment has a greater scope. Reviewing the listed number of associated risks shows that there are many, as different organisations address different risks based on their business specifications. Table 2.3 reviews various papers and publications, listing the targeted risks, explanations, and examples provided by the researchers.

Table 2.3 shows IIoT risks, their sources, and their types.

Type	**Types Of IIoT Risk and Examples**
Security Risks	Unauthorised access and data breaches: IIoT devices are vulnerable to cyberattacks, leading to unauthorised access to sensitive data or control over critical systems. Malware and ransomware attacks: IIoT devices are targeted by malware or ransomware, leading to disruptions or unauthorised control of industrial processes (Tange et al., 2020).
Privacy Risks	Data privacy concerns: IIoT devices collect and transmit a vast amount of data, including sensitive information. If not adequately protected, these data are at risk of unauthorised access or misuse (Bhamare et al., 2020). Personally identifiable information (PII) exposure: IIoT deployments may involve collecting and storing PII, increasing the potential for identity theft or privacy violations if adequate safeguards are not in place (Zhang et al., 2023).

Operational Risks	System failures and downtime: If IIoT devices or systems experience technical failures or malfunctions, it leads to disruptions in operations, production losses, and potential safety hazards (Berger et al., 2020). Interoperability challenges: IIoT deployments often involve devices and technologies from multiple vendors, which pose interoperability challenges. It hinders seamless system integration and communication (Berger et al., 2020).
Supply Chain Risks	Third-party vulnerabilities IIoT implementations often rely on third-party vendors for hardware, software, or cloud services, introducing additional risks if these vendors have security vulnerabilities or fail to meet required standards (Lu et al., 2020). Counterfeit or tampered devices: In the supply chain, there is a risk of counterfeit or tampered IIoT devices being introduced, compromising security and functionality (Lu et al., 2020).

2.2.6 Current Security Issues

Security risks are significant in IIoT deployments. IIoT inherited some security issues embedded within the IoT framework. These security issues stem from the many architectural choices cited in section 2.2.4, which introduces security issues from industry control systems (Yu & Guo, 2019). The presence of the operational technology (OT) system embedded in the IIoT increases the security issues identified in the system, as described in Table 2.4.

Table 2.4 Summary of security challenges in IIoT and IoT.

Challenges	**IIoT**	**IoT**
Data Confidentiality	Sensitive data generated by the IIoT is sent to the cloud system. It makes the IIoT cloud system a target. The issues are an untrusted cloud service	Data encryption has been the mitigating tool as so much data is produced. Still, the challenges faced are energy/power and computational capabilities. The

	provider and data leakage caused by cloud attacks (Xu et al., 2018; Yu & Guo, 2019).	unprecedented volume of data it produces is an IoT challenge (Xu et al., 2018; Yu & Guo, 2019).
Cyber-physical systems integrity	Attestation is an integrity verification mechanism, but low-cost embedded devices are deployed without it because the hardware is expensive and complex (Armknecht et al., 2013; Sadeghi et al., 2015).	The IOT runs on boot attestation, which is a form of remote attestation, but it is optimised to reduce costs. Thereby, its attestation lacks the resources needed to function, including computational power and architectural support in hardware and software (Armknecht et al., 2013; Sadeghi et al., 2015).
Key Establishment for devices	Asymmetric key establishment protocols require significant computational resources, making them unsuitable for IoT/IIoT devices with limited resources. Although it is practical to assume that shared secrets are pre-loaded in these devices, most devices do not have these secret keys when they leave the company, as symmetric protocols require them to be pre-loaded to access the organisation's resources offsite (Han et al., 2018; Y. Zhang et al., 2017).	Asymmetric key establishment protocols require intensive computation, making them unsuitable for IoT/IIoT devices with limited resources (Han et al., 2018; Y. Zhang et al., 2017).
Device management	The major challenge is monitoring and tracking	The major challenge is monitoring and tracking

	multiple nodes and devices at every stage of the lifecycle, as these devices are numerous and this trend is evident in the growth of the IIoT and IoT frameworks (Ambrosin et al., 2018; Sheng et al., 2015).	multiple nodes and devices at every stage of the lifecycle, as these devices are numerous and this trend is evident in the growth of IIoT and IoT frameworks (Ambrosin et al., 2018; Sheng et al., 2015).

Abosata et al. (2021) surveyed the system integrity for IIoT and IoT, with a summary shown in Table 2.5. They found that Industrial control systems (ICS) are prone to attacks and suffer from connectivity issues because they are not designed for the extensive connectivity they now require and need an upgrade to their security approach.

Table 2.5 Summary of the Types of Attacks in different layers.

IIOT Architecture Layers	**Explanation Of Attacks**
Perception layer	The node or devices layer collects sensor and device data and sends them to the network layer. Deogirikar & Vidhate, 2017), the standard attacks are. • Node capture: involves the attacker replacing or capturing a device to obtain sensitive data. • Malicious injections occur when intruders inject malware that most functions during a firmware upgrade or reboot. Moreover, they engage in unauthorised activities or steal data. • Sleep deprivation attacks: This is a type of denial of service, but in this case, they drain the device of power and make modifications to the operating systems. • Jamming attack: This attack is orchestrated to disrupt communication between devices. • Replay attack: This repeats authentication by an unauthorised user (Akram et al., 2018; Deogirikar & Vidhate, 2017).

Network layer	It uses the gateway or interfaces to transmit data to and from the application layer. It receives processed data from the perception layer and determines how to route it through the gateway, hub, or integrated networks. The standard attacks are: • Selective-forwarding attacks involve interception and redirecting selected packets, which acts like a DoS (Denial of Service) attack. • Eavesdropping attacks are mostly done on RFID tags, signals, and readers, where signals containing data are sent to malicious readers to collect sensitive data. • Clone ID and Sybil attacks: Attackers do this by cloning a node from one organisation node to another node or device to access the network. Sybil attacks use a single node to control a large portion of the network. • Wormhole attacks: These target the traffic flow of network topology. • Denial of service: This attack involves overloading a network or node to reduce its network or node potential and capacity. • Man in the middle: This attack is commonly used to attack node-to-node communication to alter and monitor data. • Sinkhole: Attacks are made on nodes that transmit false routing in a network. • Blackhole: This involves planting a malicious node in the network that quietly monitors and steals data. • Spoofed, altered, replay routing information: spoofing, altering, and replaying on targeted data in a node-to-node exchange (Al-rimy et al., 2018).
Application layer	This is the final layer of the IIoT architecture. This layer collects, interprets, and delivers data to diverse users. Examples include smart manufacturing and smart cities. The standard attacks are as follows: Malicious code injection: injection of malicious code into software. They are self-activated or user activated.

	Malicious scripts occur when a user connects to the internet and runs a script or software that appears legitimate. It leads to data theft and system failure. Data distortion attack: These codes within a software use antivirus avoidance to damage the system (Akram et al., 2018; Bhamare et al., 2020; Abosata et al., 2021).

2.3 ACCESS CONTROL ALGORITHMS

Access control algorithms ensure that only authorised users access resources (Salonikias et al., 2015). Several access control algorithms have been defined by various sources, which are helpful for this research. Access control algorithms manage and enforce security policies for authorised resources in various systems (Koo et al., 2017). There are three abstractions in which access control systems are composed of policies, models, and mechanisms. An access control system fulfils tasks such as enforcing access control policies and ensuring the integrity of the policy standard using these abstractions. While access control policies are defined as high-level requirements that specify how users use and when they use them, they are implemented through control mechanisms. The access control mechanisms oversee authentication and validation, enforcing access control policies (Salonikias et al., 2019; Salonikias et al., 2015; Pesonen et al., 2006). The access control algorithm section will examine the multi-factor access control mechanism suited for Biometric access control and provide examples.

2.3.1 Types of Access Control Algorithm

Table 2.6 shows Access Control List (ACL) types and their definitions. These security access control algorithms provide different approaches for managing access controls to resources based on predefined roles, attributes, discretionary control, encryption, or multifactor authentication. Understanding and applying the appropriate access control algorithm ensures secure, controlled access across various systems, including the Industrial Internet of Things (IIoT) (Sardar et al., 2022).

Table 2.6 Access control types and definition.

Type of Access Controls	Explanation
Role-Based Access Control (RBAC)	These access control algorithms are critical for managing and enforcing security policies that authorise access to resources across various systems. (Nesa & Banerjee, 2020; Ameer et al., 2022).
Attribute-Based Access Control (ABAC)	The ABAC model controls access by considering attributes linked to subjects, objects, and environmental conditions. It allows for fine-grained access control decisions by defining policies based on attribute values (Ameer et al., 2022; J. Xu et al., 2018).
Discretionary Access Control (DAC):	It is a conventional access control model that grants owners or administrators the authority to determine user access privileges. It includes various resources such as files, registry keys, database tables, and operating system objects. The model employs Access Control Entries (ACE), entries within a list that provide details about each user's access to a particular resource and their corresponding rights. (Katal et al., 2013; He et al., 2015).
Mandatory Access Control (MAC)	The MAC (Mandatory Access Control) policy is characterised by its mandatory nature, meaning users cannot override it. It chooses whether to approve or disapprove a specific procedure. MAC accomplishes this by considering two primary criteria: the legal authorisation or clearance of persons to access such susceptible material, as well as the sensitivity of the information connected with an object or resource (represented by a label) (Katal et al., 2013; Jiang et al., 2015).
Attribute-Based Encryption (ABE)	ABE is an encryption-based access control technique that embeds access policies in ciphertexts. (Sahai & Waters, 2005).
Multifactor Authentication (MFA)	MFA combines multiple authentication factors, such as passwords, biometrics, tokens, or smart cards, to verify users' identities. (W. Li et al., 2021).

Capability-based access control (CapBAC)	CapBack is a recognised access control technique that is communicated and cannot be forged, and it is the foundation of capability-based access control (CapBAC). Like RBAC (Role-Based Access Control), subjects are system users, and objects are system resources. In this context, the authorised actions a subject is permitted to carry out on an object are permissions. (Wilkes & Needham, 1979).
New-Generation Access Control (NGAC)	This Access Control is an initiative by the NIST (National Institute of Standards and Technology) to establish a standardised mechanism for Attribute-Based Access Control (ABAC). NGAC introduces data/relations and characteristics to express policies and deliver capabilities to comply with ABAC's standards. (Ferraiolo et al., 2016; Coyne & Weil, 2013).

2.3.2 Access Control- Authentication and Authorisation in IoT

The Industrial Internet of Things (IIoT) and the Internet of Things (IoT) have three active participants in the wireless sensor network: users, devices (including sensors and nodes), and the gateway (Li et al., 2018). Some protocol levels are maintained to recognise users and their access clearance levels. Sammoud et al. (2020) reviewed and observed that existing two-factor authentication schemes do not withstand attacks as compared to three-factor authentication, although three-factor authentication incurs high resource consumption.

Analysing existing authorisation and authentication provisions in place and most of their flaws in privacy risk, as suggested by most researchers. Li et al. (2018) proposed a three-factor authentication using a fuzzy extractor to design a bio-hashing-based protocol. Table 2.7 reviews some access control research from 2009 to 2023.

Table 2.7 Previous authentication mechanism

Researcher And Year	**Mechanism Or Algorithm Used**	**System Drawback Discovered**
Anil et al. 2009	A smart card and a password are used to authenticate the gateway.	Insider attack, impersonation, and gateway-node bypass (Li et al., 2018).

Das et al., 2012	Lightweight algorithm (hash function and symmetric cryptography).	They include insider attacks, smart card breaches, and the disclosure of server master keys (Wang & Wang, 2014).
Xue et al., 2013	Hash function to guarantee computational efficiency.	Stolen cards, insider attacks, identity guessing and tracking attacks (Jiang et al., 2015).
Turkanović et al., 2014	Designed an authentication scheme for a heterogeneous ad-hoc wireless network system.	Vulnerable to stolen verifier attack, sensor, smart card breach, or device capture attack (Chang & Le, 2016).
He et al., 2015	They proposed a protocol to mitigate the Xue et al. (2013) hash function, which they identified as vulnerable to password guessing, user impersonation, sensor node impersonation, and more.	They include User impersonation attacks, smart card loss, insider attacks, and tracking attacks, as Jiang et al. (2016) discovered.
Chang & Le, 2016	Uses ad-hoc wireless network authentication.	Lack of proper authentication, stolen smart card attacks, tracking attacks, challenging password changes, lack of practical application, and incorrect passwords cause delays in the system (Li et al., 2018).
Li et al. (2018)	Utilised a privacy-aware multi-authority ciphertext-policy attribute-based encryption (ABE) scheme with accountability,	used to hide attribute information in the ciphertext, support ciphertext-policy access control, and enable the tracing of dishonest users who share decryption keys.

	which addresses the challenge of enhancing privacy while ensuring accountability in fine-grained access control systems	
Awaysheh et al., 2020	The research proposes a BD federation access broker framework to address security limitations in Hadoop access control. It introduces the federated access control reference model (FACRM) to formalise secure BD solutions within the Apache Hadoop stack.	The access broker facilitates authentication and authorisation management in a distributed, heterogeneous, and federated infrastructure, aiming to overcome the complexity and resource consumption associated with Hadoop's primitive access control. This approach tackles the challenge of enhancing security and privacy in next-generation big data federation platforms.
Yang et al., 2022	Revocable and Multi-authority ciphertext-policy attribute-based encryption (RM-CP-ABE)	It addresses the data security challenge in cloud storage environments by introducing revocability and multi-authority support to attribute-based encryption (ABE). It enables flexible revocation of user attributes and supports multi-valued attributes, enhancing practical applicability in cloud computing scenarios. Additionally, the scheme demonstrates reasonable computational cost, storage overhead, and selective security

		under the RLWE assumption, making it suitable for real-world deployment.
Zheng et al., 2022	cryptographic primitive called TFPRE-OT, which combines type-based proxy re-encryption and oblivious transfer.	This primitive enables fine-grained sharing and hiding of access histories for data requesters, thereby addressing the conflicting interests of data owners and requesters. The challenge this approach addresses is achieving both differential access control and privacy protection in cloud computing settings, where existing methods often address these issues separately, leading to unsatisfactory security requirements for different roles.
Paulraj et al., 2023	The research utilises a binding contract and an admission control policy (ACP) to facilitate trust between cloud providers and enable efficient data transfer. A Multi-Agent Reinforcement Learning (MARL) algorithm is employed for anonymity classification, thereby enhancing privacy protection.	It addresses cross-cloud data migration and privacy concerns in cloud computing by introducing a novel scheme based on binding agreements and anonymous identities. approach tackles the complexities of data migration and privacy in cloud environments, aiming to improve user experience and security.

2.3.3 Types Of Multi-Factor Algorithm

This research focuses on using Biometrics Access Control (BAC), with most researchers using Multifactor Authentication (MFA). MFA employs multiple authentication factors to validate users' identities. Various approaches to implementing MFA are shown in Table 2.8 and encompass the listed methods.

Table 2.8 Different Types of Multifactor Algorithms and their definition

Type Of MFA	Term Definitions
Time-Based / One-Time Password (TOTP)	It generates a unique password using a shared secret and the current time. This password is typically valid for a brief period, providing an additional layer of security (Kosta & Sanyasi, 2021).
SMS-Based Authentication	It uses a one-time password or verification code sent to the user's registered mobile phone via SMS. The user enters this code as an additional authentication factor (Derhab et al., 2020).
Push Notification Authentication	A dedicated app sends a push notification to the user's mobile device. The user approves or denies the authentication request, providing an additional layer of verification (Prakash et al., 2021).
Biometric Authentication	It involves biometric authentication factors such as fingerprint, face recognition, or iris scan. Biometric characteristics are unique to individuals and are used as an additional layer of authentication (Mihailescu & Loredana, 2020).
Hardware Token Authentication	It involves using physical tokens, such as smart cards or USB tokens, that generate one-time passwords or cryptographic keys for authentication (Lu & Ali, 2008).

2.3.4 Multifactor Authentication (MFA) Token Access Control Used In Previous Works

Many access control mechanisms have been featured in the Industrial Internet of Things (IIoT) sector, especially in the Biometric field. This section evaluates a selected sample of multifactor authentication (MFA) mechanisms and the problems they were created to solve. Alsaleem and Alshoshan (2021) proposed a multifactor authentication system that combines simplicity and low cost. There are no unique configurations or

infrastructure requirements for the system. It employs graphical passwords, so the user must select and memorise three images during registration. During the login phase, after entering the username and password, the user only needs to select the correct images they selected during registration in the same order. The proposed system defeats keyloggers, screen capture attacks, and shoulder surfing. The proposed system was focused on ease of use and low-cost factors. Malware and Trojans are ineffective because they record what a user types on the keyboard and what the user sees on the screen. Their system was designed to protect the user's data so that programs do not capture the user's passwords or even the authentication methods the user employs. Shrestha et al. (2019) proposed a system that introduces gait biometric authentication as an additional component of the MFA process. Existing systems for this proposed system rely on a single authentication factor, which possesses a significant security vulnerability. The attacker gains unrestricted entry to the terminal if the authentication token is physically accessed without authorisation, such as through theft.

ZEMFA, or zero-effort multifactor authentication, was proposed as a solution to this problem. ZEMFA combines multiple authentication tokens, namely a smartphone and a smartwatch or bracelet, as well as two different gait patterns that these tokens record. These are movements of the mid and lower body recorded by the phone and movements of the wrist and arm recorded by the watch. ZEMFA guarantees that only the authorised user may access the terminal, even if a fraudster obtains access to both authentication tokens by exploiting a user's unique walking or gait pattern. In their 2022 article, Sardar et al. proposed an upgraded palmprint recognition system that performs better and provides stronger biometric template protection. The Bio-Cryptosystem, which they created as a novel addition, offers strong security without requiring users to remember their tokens. Cancellable feature vectors are stored in encrypted form using the proposed Bio-Cryptosystem. The system's five primary subsystems are image pre-processing, feature extraction, cancellable Biometrics, classification, and the Bio-Cryptosystem.

The palm texture region is removed from the input hand image during pre-processing. Next, a feature representation technique is used to process the palmprint texture patterns to extract distinguishing features. A user-specific token is created when these collected features are examined using an information coding scheme. The original palmprint features are combined with these user-specific tokens in the cancellable biometric system to compute the feature vectors. The cancellable biometric

technique is enhanced to incorporate two security levels that protect biometric information from numerous attacks, including dictionary, brute-force, database, channel, replay, and spoofing assaults. It improves the biometric template protection strategy (Shrestha et al., 2019; Sardar et al., 2022).

Additionally, the proposed system introduces an automatic key generation technique for user passwords to alleviate the challenge of remembering lengthy passwords or tokens. Two separate keys are generated: one for cancelable biometrics and another for encryption and decryption. These keys do not require storage or memorisation and are utilised in a multifactor authentication system. Furthermore, the proposed system employs a novel Bio-cryptographic algorithm, distinguishing it from traditional Bio-cryptographic algorithms (Shrestha et al., 2019; Sardar et al., 2022).

Pramana et al. (2020) explored the utilisation of a Time-Based One-Time Password (TOTP) as a two-factor authentication mechanism for securing online accounts. TOTP is an algorithm based on hash-based message authentication (HMAC). In their study, the process of generating TOTP with a secret key was distributed to users via a QR Code or barcode linked to their respective accounts, along with the local time setting. The generated TOTP passcode serves as a verification code to confirm the original user's ownership of the account. A new TOTP code is generated every 30 seconds. The researchers also developed a biometric system, specifically facial recognition, as an additional factor in the authentication process. However, it is noted that facial recognition, like other biometric factors, is susceptible to spoofing attacks, in which an individual deceives the system using covert means. To counter these spoofing attacks, the researchers implemented Multifactor Authentication (MFA) that uses TOTP to authenticate users. Combining the TOTP passcode with another factor, such as facial recognition, strengthens the authentication process's security, providing a more robust defence against spoofing attacks.

De Diego et al. (2009) proposed a novel information fusion method at the classifier level for face verification. The approach considers three types of complementary face data: texture, data range, and image curvature. Initially, the deep structures of convolutional networks are extracted during the initialisation stage, capturing global high-level features across the entire face region. These methods use specialised networks that look at the entire Face and identify key points. This approach has two big advantages. First, it finds each point well by looking at the whole Face and using the context. Second, because it is trained to find all points simultaneously, it

understands how they relate to one another. This means it handles tough problems, such as when the Face is partly hidden or the lighting is poor. Consequently, the method handles complex image samples with occlusions, large pose variations, and high-contrast illumination. The method is robust to local minima despite data ambiguities and corruptions.

An example of research using ESP-32 CAM for face recognition is research on Developing Arduino-Based Smart Home System Using ESP32 CAM and OpenCV published by Wicaksono et al. (2020). In this paper, the authors propose an approach to designing a system that recognises human faces using an Arduino and an ESP32-CAM. The proposed system integrates a face recognition component developed using the OpenCV library and implemented on the ESP32-CAM module connected to an Arduino system. In the proposed system, the Arduino board uses sensors to send data to the server, and the ESP32-CAM module captures face images, which are then sent to the server. These photos are then delivered to homeowners using the Line app. Moreover, users manually take photos and control lights, fans, and PIR sensors via the provided web interface.

2.4 BIOMETRIC TRAITS

A biometric is a physical trait or individual behavioural characteristic that may be measured and used to identify or verify a person, serving as an information security measure as defined by the National Institute of Standards and Technology (NIST) (Kissel, 2013). For recognition between humans, they must know what the subject looks like or have met the subject to see one or two behavioural or physical attributes. For user differentiation, the system supports three interactions: Human-to-machine (H2M), Machine-to-machine (M2M), and Machine-to-service (M2S) (Lipps et al., 2021). These play a crucial role in identifying users, as the human biometric critical definition is categorised into three. Individual Biometrics are measured in various ways. There are three broad categories of biometric traits. And they are;

- Physiological Biometrics are physical attributes such as fingerprints, hand geometry, facial features, iris patterns, ear patterns, palm vein patterns, and palm prints.
- Behavioural Biometrics like voice patterns, gait, and hand signatures.

- Biological Biometrics are biological attributes obtained from medical machine readings such as EEG, ECG, and PPG (Jain et al., 2007; Lipps et al., 2021; Padma & Srinivasan, 2016; Ren et al., 2020).

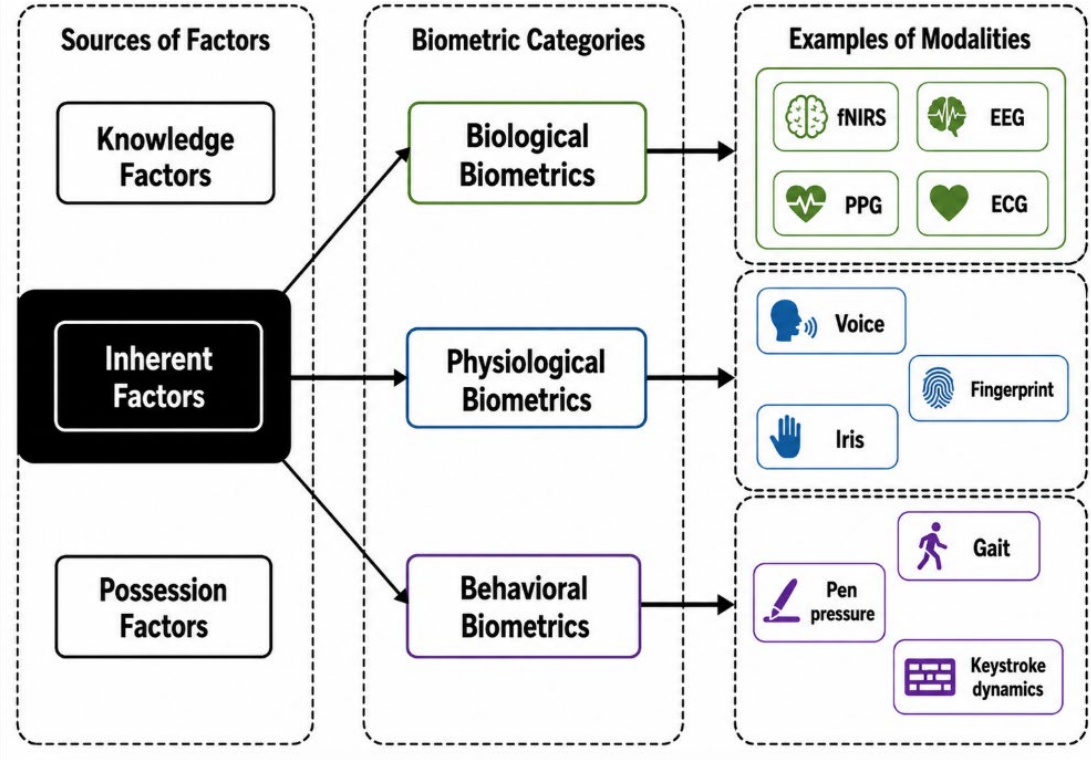


Figure 2.2 Types of biometric traits for authentication and their examples (Lipps et al., 2021, p.3)

2.4.1 Biometric System Pathway (Trait Sensor Interaction)

This section identifies the pathways for biometric access control systems as standardised by different authors. Summaries of what biometric traits were used and at what stage will be identified. The following are the stages of a biometric pathway.

2.4.1.1 Pre-processing stage

The pre-processing stage in the biometric access control system pathway involves acquiring biometric data from biometric sensors via a computer to improve data quality. This process is used to correct distortions and get to the region of interest, using a dataset to correlate and correct distorted data. Most methods used in this stage are feature standardisation, rescaling, and subtraction (Osanaiye et al., 2016). This stage is the most important, as the Human-Computer Interaction (HCI) between the user and the sensors must be implemented correctly. Table 2.9 shows examples of this stage.

Table 2.9 Previous work showed the biometric pre-processing stage.

Researcher	Pre-Processing Features.
Xu et al., 2016	Proposed symmetrical face image for face recognition image pre-processing, improving precision through a framework.
Rehman & Saba, 2014	proposed neural networks for processing template images. They improve layout analysis and classification by decomposing tasks like line removal, skew estimation, and baseline detection.

2.4.1.2 Region of interest stage

In biometric systems, the Region of Interest (ROI) is either processed before the feature extraction stage or integrated into it. The process of emphasising the essential and intriguing aspects of a biometric trait as a more focused area for use as matching characteristics in a biometric system is known as ROI (Barbosa & Santos Silva, 2015). The region of interest is broken into four broad groups, as shown in Table 2.10.

Table 2.10 Types of the region of interest.

Grouping	Explanation
Bottom-Up Feature-Based Approaches	This method searches for features under different conditions and uses them in the detection process. A popular technique for face localisation is the Scale Invariant Feature Transform (SIFT), which combines a region detector and descriptor based on gradient distribution. Shape context employs edges extracted by clever detectors, and Histograms of Oriented Gradients (HoG), which enhance accuracy by overlapping local contrast normalisation, are similar techniques. These techniques employ linear Support Vector Machines to categorise people (Alonso-Fernandez et al., 2009).
Top-Down Knowledge-Based Approach	This method reduces the likelihood of false-positive detection by focusing on the object of interest. Jones and Viola (2006) suggest that by selecting feature sets, the scale of the training data, and the scales utilised for detection, a region-of-interest strategy that considers the

	information already available about a person's mobility and appearance is implemented.
Template Matching Approach	This technique uses the object's component elements to represent its overall image. This connection enables a calculation, which is then used for detection. A human detection approach that extracts the boundary and separates foreground areas was proposed by Gagan and Lalitha (2015). By comparing the edge properties of human silhouettes in the database, the program continues to search for humans in the image.
Appearance-Based Approach	This method uses discriminant functions for detection to identify distinctive features in images of objects, leveraging machine learning and statistical analysis (Shekhar et al., 2012). Artabaz et al. (2014) proposed a technique for extracting the palm's region of interest, which contained its distinguishing characteristics. Localisation was used to pinpoint key points for aligning the hand image. The technique also included the X-axis projection and upper- and lower-edge projections, enabling the extraction of the hand contour's horizontal limits.

2.4.1.3 Feature extraction stage

A crucial step in the identification process of biometric systems is feature extraction. It entails reducing the resources needed to describe a sizable amount of data. By extracting properties used to classify and identify patterns in input images, feature extraction primarily reduces the size of the original dataset (Fasel & Luettin, 2003). Advancements in biometric authentication feature extraction include integrating deep learning techniques such as CNNs and RNNs, using transfer learning to improve generalisation across datasets, and adopting privacy-preserving methods such as homomorphic encryption. Recent research emphasises the fusion of multimodal features, domain adaptation, and sparse representations to enhance accuracy, security, and scalability in biometric systems (Liu et al., 2016). Table 2.11 shows some work done on the feature extraction stage.

Table 2.11 Previous work done using feature extraction.

Researcher	**Extraction Features**
Bentahar et al., 2018	They proposed an encryption scheme suitable for IoT applications. They used the fuzzy commitment scheme in a DCT-based fingerprint recognition method. The results are analysed and put up against direct matching (without encryption) using the two most common metrics, FAR (False Acceptance Rate) and FRR (False Rejection Rate), to show how effective the system is. The Gabor Filter, Discrete Wavelet Transform, Discrete Cosine Transform, and Fast Fourier Transform techniques for feature extraction.
Kumar & Kanhangad, 2015	They presented a tunable-Q wavelet transform (2D-TQWT)-based face recognition method, in which face images are divided into four sub-bands, and local binary pattern-based histogram features are extracted from each sub-band. Three feature extraction techniques were employed: Wavelet Transform-based Feature Extraction, Spatial Differentiation, and Twin Pose Testing Scheme.
Ross & Jain, 2003	The researchers combined data at the matching score level to address information fusion in biometric verification systems. They combined face, fingerprint, and hand geometry biometric modalities to demonstrate the effectiveness of their experimental results. In the Matching module stage, feature values are compared to template features to produce a matching score, for instance. A matching score is produced after facial features are extracted and compared to the template database.
Khobragade et al., 2015	They propose using MATLAB to quickly and easily extract 2D ear features. To achieve the desired ear shape for ear recognition systems, the method performs image segmentation, feature extraction, and information removal. For ear biometrics, ear feature extraction is essential, and image pre-processing and normalisation are crucial steps.

Mohammed et al., 2015	Focusing on data capture, pre-processing, feature extraction, and verification techniques for handwritten signature verification, they proposed an HSV system. Two feature extraction techniques—the static and pseudo-dynamic approaches—were suggested for an offline handwritten signature system. These approaches were used to measure geometrical features and estimate dynamic information.

2.4.2 Biometric Factors Definition

In this subsection, the biometric factors are explained. These are the attributes that qualify why and how a biometric trait fits within a standardised platform for identification, verification, and authentication. Table 2.12 gives the factors and their explanations.

Table 2.12 Biometric factors and their explanations: Adaptation (Kiran et al., 2018, p. 429).

Biometric Factors	**Explanation**
Universality	The presence of a biometric feature in most of the population is required for it to be universal and adopted as a standard (Kiran et al., 2018).
Distinctiveness	The uniqueness of a biometric feature is determined by its distinctiveness in different individuals (Oloyede et al., 2016).
Permanence	Consistency is crucial in biometric measures as they are permanent. The features must remain unchanged over time (Lipps et al., 2021).
Collectability	The ease of obtaining a biometric measurement is called its collectability. Its acquisition determines how convenient it is to authenticate users (Kissel, 2013).
Performance	Performance is a standard for measuring a system's effectiveness. The process entails evaluating the system's precision and efficiency and the resources required to attain and analyse the desired precision and speed (Kowtko & M., 2014).

Acceptability	Acceptability refers to an individual's willingness to provide a biometric measure. The convenience factor plays a significant role in determining the acceptability of a biometric measure within a biometric system. The higher the level of convenience, the more acceptable the biometric measure becomes (Considering the device's dexterity) (Bentahar et al., 2018).
Circumvention	Circumvention refers to the ease with which an attacker deceives a system using a fraudulent biometric sample (Gagan & Lalitha, 2015).

Oloyede et al. (2016) analysed various biometric features and identified their flaws when used alone, summarised in Table 2.13.

Table 2.13 Biometric traits performance comparison (Oloyede et al., 2016, p. 7542)

Factors	**Gait**	**Face**	**Voice**	**Finger Print**	**Iris**	**Palm Print**	**Ear**
Accuracy	high	low	Medium	high	high	high	high
Ease of use	medium	medium	high	high	medium	medium	medium
Cost	high	medium	high	low	high	high	high
Privacy	high	high	high	high	high	medium	low
Distinctiveness	medium	low	low	high	high	high	high
Error factor	Weight gain	occlusion	illness	age	Eye Angle	age	pose
Universality drawback	drunkenness	Plastic surgery	Speech damage	Worn ridges	Visual impairment	Worn print	Light condition
Interaction Mechanism	Motion camera	Camera capture	Audio capture	finger scanner	camera capture	Palm scanner	Camera capture
contactless	yes	yes	yes	no	yes	no	no

Ratings are qualitative and ordinal, taken from Oloyede et al. (2016, p. 7542). The source gives no numeric thresholds. High, Medium and Low compare the listed traits with one another: for accuracy, ease of use, distinctiveness and privacy a higher rating is more favourable, and for cost a higher rating means a higher cost.

Table 2.12 shows issues with standalone Biometric traits, while Table 2.14 provides examples of multimodal biometric fusion (also cited in sections 2.3.3 and 2.3.4) used to mitigate these issues.

Table 2.14 Previous Biometric works: Biometric mechanism.

Researcher(S)	**Biometric Mechanism**	**Algorithm Used**
Manjunathswamy et al., 2015	Biometric characteristics such as fingerprints and facial features	The algorithm involves normalisation techniques such as z-score and tanh, and fusion techniques such as max score and match weighing.
Singhal et al., 2014	Iris and face mechanism	Normalisation algorithm
Razzak, 2010	Facial recognition and finger vein authentication method	Linear Discriminant Analysis and Client-Specific Algorithm
Ghate et al., 2015	Fingerprint and facial recognition	The algorithm used is the Neyman-Pearson algorithm.
Hu et al., 2015	Facial recognition and modelling of faces	A fusion scheme within a 3D framework technique to combine facial mark matching and commercial face recognition.
Kawulok & Szymanek, (2012).	Face and Eye Biometric Mechanism	Multi-Level Ellipse Detector and an SVM (Support Vector Machine) Verifier
Dalka and Czyzewski, 2010	Lip movements and Gestures biometric	Artificial Neural Network (ANN) algorithm.
Shen et al., 2011	Face and Palm Print mechanism	FPCODE algorithm, the feature-level fusion
Kowtko & MA 2014	Biometric traits, including	The threshold settings for score-level fusion in each sum rule-based match.

	fingerprints, hand geometry, and voice	
Soltane, 2010	face and voice recognition	Gaussian Mixture Model (GMM).

2.5 BIOMETRIC TRAITS AND DEEP LEARNING

This section investigates the body of knowledge of individual biometric recognition mechanisms and their paradigms. It focuses on artificial intelligence using deep learning to obtain biometric datasets and train machine learning models for authentication.

2.5.1 Face Recognition Paradigms

The Facial trait is more pronounced in comparison to the other traits and is easily used by individuals for identification (Dieter et al., 2013; Bao et al., 2023). During enrolment, a person's Face is captured by the face scanner or camera for feature extraction, normalised, localised and encoded for hashing and verification. Early models of face recognition relied on simple geometric models, but in recent years, more sophisticated mathematical models and matching techniques have been used (Jain et al., 2004). Deep learning-based face recognition shows how facial recognition technology has evolved from simple geometric models to advanced mathematical models and matching techniques. Curricular Face uses the concept of curriculum learning in its loss functions to handle different samples at different training stages (Bengio et al., 2009). Advanced feature learning and adaptive strategies in loss functions have been emphasised by methods such as SphereFace, ArcFace, and AdaCos, which highlight angular discriminative features and automatically strengthen supervision during training (Liu et al., 2017; Deng et al., 2019; Zhang et al., 2019).

"Face Synthesis with Identity-Attribute separation for Heterogeneous Face Recognition," published by Yang et al. in 2022, demonstrates the use of the Face Synthesis (FS) and Identity-Attribute Disentanglement (FSIAD) method, achieving better results than other state-of-the-art approaches in Heterogeneous Face Recognition (HFR). According to the authors, IAD (Identity-Attribute Disentanglement) helps segregate identity-containing information from other identity-independent information. Using IAD, the matching between faces from different

heterogeneous sources becomes more reliable and robust. The Face Synthesis Module (FSM) increases the size of the training data, thereby improving HFR performance.

In the context of security threats, the FaceAdv method demonstrates practical physical-world attacks on deep-learning face recognition systems. FaceAdv: Shen et al. (2021) used a Generative Adversarial Network (GAN) technique; the FaceAdv-generated adversarial stickers were placed on targeted facial regions to achieve impressive results in dodging and impersonation attacks. In face generation, the authors used a Progressive-GAN (PGAN) framework that progressively grows the generator and discriminator networks to produce ultra-high-resolution face images indistinguishable from real ones. The resulting face generation method achieved high verification accuracy, a common theme in state-of-the-art deep learning studies of face recognition (Karras et al., 2017; Wang et al., 2018b).

Ren et al. (2022) present the Perturbation Inactivation (PIN) method, a plug-and-play defence strategy against adversarial attacks. PIN identifies an immune subspace, effectively inactivating adversarial perturbations and demonstrating robust generalisation across diverse scenarios. Their approach is plug-and-play and works with most commercial or business API gateways.

The research by Krivokuca Hahn et al. (2023) categorises existing face protection techniques into two subcategories: Non-Neural Network and Neural Network-learned approaches. The study states the need for an empirically validated evaluation to assess the robustness of recognition accuracy, irreversibility, and renewability/unlinkability.

Facial age estimation uses Divergence-Driven Consistency Training (DCT) by Bao et al. (2023) to address the limited number of training samples. The method uses pseudo-labelling, consistency regularisation, Efficient Sample Selection (ESS), Identity Consistency (IC) regularisation, and Local Prediction (LP). The research presents an overview of deep learning developments used to utilise large amounts of unlabelled data and to evaluate the efficiency of models and algorithms for face analysis, including face recognition and face ageing.

2.5.2 Fingerprint Recognition Paradigms

Fingerprint recognition technology is a biometric technology that dates back a century and is still widely used as a reliable form of authentication. It has several disadvantages, such as scars, dry skin, and ageing (Li et al., 2014a). The intricate

features of ridges, valleys, and minutiae make fingerprints a pivotal biometric trait (Adewole et al., 2014; Ding et al., 2023). Lee & Wang (1999) used Gabor filtering on segmented fingerprint images to improve authentication. They were among the pioneers in advancing fingerprint technology. The segmented fingerprint images were classified using a k-NN classifier, achieving an authentication rate of 97.2%. Tico et al. (2001) leveraged wavelet features for fingerprint recognition, employing a k-NN classifier methodology. Tico et al. (2001) also used wavelet features in fingerprint recognition and a k-NN classifier to improve traditional methods. Fingerprints have several disadvantages, such as dirt on the skin surface and ageing effects, which significantly reduce the accuracy of fingerprint authentication (Li et al., 2014a). Fingerprints are captured by placing the finger in contact with the fingerprint reader. For each sample in the database, this must be done, which is a very time-consuming process, hence, biometrics, such as Face recognition, are much faster.

Deep learning techniques are increasingly used in fingerprint recognition. MENet (Darlow et al., 2017) and FingerNet (Tang et al., 2017) were the first deep learning models for the extraction of minutiae features, unified features, orientation fields and segmented features. Lin & Kumar (2017) proposed a multi-Siamese network for matching contactless motion in fingerprint images with their corresponding contact fingerprints, combining deep learning with handcrafted features. Anand et al. (2020) proposed an innovation, a CNN-based pore descriptor (DeepResPore), for detecting pores and computing descriptors for high-resolution fingerprint recognition.

With all these innovations, ensuring the security of fingerprint-based systems against fraudulent attempts is crucial. Kim et al. (2016) proposed a liveness detection approach for fingerprint samples using the statistical output of a deep belief network (DBN), achieving impressive results on public benchmarks, including the LivDet2013 database (Kim et al., 2016). Deep learning-based fingerprint liveness detection has also been introduced by Nogueira et al. (2016), achieving 95.5% accuracy.

Ding et al. (2023) proposed a groundbreaking method, LMT-U Net, for extracting surface and internal fingerprints from noisy Optical Coherence Tomography (OCT) volume data. Ding et al. (2023) propose a novel approach, called the Learning Multi-Task Ultrasmall Network (LMT-U Net), for extracting surface and internal fingerprints from noisier volume data from Optical Coherence Tomography (OCT). In the proposed approach, a deep end-to-end Contour Regression Module (CRM) based convolutional neural network (CNN) is designed for fast tissue contour estimation.

The multi-task learning and depth-wise separable convolution (DSC) are implemented in LMT-U Net, which preserves the merits of an ultrasmall network while also outperforming other state-of-the-art architectures and methods. Through multi-task learning and depth-wise separable convolution (DSC), LMT-U Net achieves results comparable to 3D architectures, outperforming conventional methods and prominent neural networks. Hence, the research is conducive to the real-time implementation of Automated Fingerprint Recognition Systems (AFRS).

2.5.3 The Palm Print Recognition Paradigms

In biometric identification, palmprints are often overshadowed by traits such as iris, Face, and fingerprints, but are gaining prominence due to their unique features (Isnanto et al., 2015). As a biometric trait, palmprints include minutiae, geometry-based traits, delta points, primary lines, and wrinkles. Over time, the stability of creases in palmprints adds a unique dimension to the recognition process, thereby enhancing its reliability (Xinrong et al., 2013). Early efforts in palmprint recognition involved handcrafted features, including Principal Component Analysis (PCA), Fourier and wavelet transforms, line-feature matching, and deep scattering features. These methods laid the foundation for understanding the intricacies of palmprint recognition.

The use of deep learning has significantly advanced the palmprint recognition, with notable contributions from Xin et al. (2015), Zhong et al. (2018), Shao & Zhong (2019), Shao et al. (2019a, 2019b), Zhao et al. (2019), and Zhao & Zhang (2020). These innovations range from deep belief networks, Siamese networks, transfer learning, graph neural networks, and deep convolutional architectures for improved feature extraction and recognition. Shao et al. (2024) propose a Federated Metric Learning (FedML) method to address data privacy and data distribution across islands in deep metric learning-based palmprint recognition. This approach involves deploying models with different architectures on various datasets. Transfer learning bridges the gap between private and public data distributions, demonstrating superior performance in scenarios with Non-Independent Identically Distributed (Non-IID) data.

Yang et al. (2023) introduced a Comprehensive Competition Network (CCNet) for palmprint recognition. This network reformulates the traditional competition mechanism by incorporating spatial and channel competition mechanisms into multi-

order texture features. CCNet performs remarkably well on public palmprint datasets, outperforming state-of-the-art methods, and the related code is available on GitHub. Genovese et al. (2019) worked on the PalmNet, a CNN that was designed for touchless palmprint recognition. The novel CNNs, PalmNet-Gabor and PalmNet-GaborPCA, use a unique filter-tuning procedure based on Gabor responses and PCA. The extensive evaluations have proved the superior recognition accuracies compared to existing methods, highlighting the effectiveness of Gabor-based filter tuning and the importance of CNNs in touchless palmprint recognition. Shao et al. (2021) propose a novel Learning with Partners (LWP) framework. This method leverages multiple labelled source datasets and an unlabelled target dataset to train two feature extractors. LWP significantly improves accuracy and Equal Error Rate (EER) in multi-source, cross-dataset palmprint recognition.

2.5.4 The Iris Recognition Paradigms

The iris recognition is one of the robust biometric methods for identification and verification, and it is valued as one recognition with high accuracy, reliability, and simplicity (Srinivasan & Balamurugan, 2014; Gupta et al., 2006; Oloyede et al., 2016; Nalla & Kumar, 2017; Nguyen et al., 2020; Park et al., 2011; Ren et al., 2020; Sequeira et al., 2016; Srikrishna & Nirmala, 2023; Wei et al., 2022, 2023; Xu et al., 2023; Zhao & Kumar, 2019). The Iris recognition system comprises core processes of image acquisition, iris localisation, feature extraction, and encoding for database storage, culminating in template matching for identification (Srinivasan & Balamurugan, 2014). The richness of iris features, including rings, corona, ciliary processes, freckles, and microstructural patterns, contributes to the stability and uniqueness of iris recognition (Nguyen et al., 2020).

Daugman's Framework (1993) proposed a method that stands out as a pivotal contribution, establishing a robust statistical foundation for modern iris biometrics through the test of statistical independence (Daugman, 1993). Early methods included Zhu et al. (2000), which utilised multi-channel Gabor filtering and wavelet transform for iris identification, and Minaee et al. (2015), which introduced an iris recognition system based on deep scattering convolutional features (Zhu et al., 2000; Minaee et al., 2016). Deep learning has revolutionised iris recognition, significantly improving performance. Minaee et al. (2016) demonstrated the efficacy of pre-trained CNN models, Gangwar and Joshi (2016) proposed a CNN-based iris recognition

network, and later a framework based on deep belief networks and contour information (Minaee et al., 2016; Gangwar & Joshi, 2016;). Zhao and Kumar (2017) developed a framework based on a Fully Convolutional Network (FCN) and Extended Triplet Loss (ETL), while Alaslani and Elrefaei (2018) utilised deep features from AlexNet for iris recognition (Zhao & Kumar, 2017). The proposed IrisParseNet by Wang et al. (2020c) is a notable deep multi-task attention network for accurate iris segmentation and recognition (Wang et al., 2020).

Two papers were added to the Contextual Measures (CM) by Wei et al. (2023) in "Iris Recognition via Learning Microstructures from Deep Features", which explored using microstructures in the iris for better recognition. The CM method proposed in this paper uses a Globally Contextual Measure (GCM) branch and a Locally Contextual Measure (LCM) branch in parallel. It uses a Perturbation Bottleneck (PB) to eliminate redundancy in feature aggregation. Fang et al. (2021) proposed a fusion-based classifier for Iris Presentation Attack Detection (PAD) using 2D textures and 3D photometric stereo. The robustness of the proposed method is verified under different sensors and lighting conditions. (Fang et al., 2021).

Wei et al. (2023) introduce an innovative iris recognition method, Contextual Measures (CM), leveraging microstructures within iris patterns. CM utilises two parallel branches, Globally Contextual Measure (GCM) and Locally Contextual Measure (LCM), to capture global and local contexts. A Perturbation Bottleneck (PB) is introduced to address aggregation redundancy and enhance discriminative features. Experimental results on benchmark iris datasets validate CM's effectiveness, emphasising the importance of global and local contexts. Fang et al. (2021) propose a multi-modal Presentation Attack Detection (PAD) technique using 2D and 3D modalities. The 2D feature is obtained using the Binary Statistical Image Features (BSIF) method, while the 3D feature is derived from photometric stereo. Results from several state-of-the-art commercial-off-the-shelf iris biometric devices, including IrisGuard AD100 and LG 4000, show higher accuracy than competing modalities, particularly in open-set attack scenarios. The study also introduces a new iris biometric database having real and synthetic samples along with corresponding open-set spoofing attack samples. An open-source implementation of the multi-modal PAD technique is available online.

Lee et al. (2022) proposed a new technique for protecting iris templates using the Random Augmented Histogram of Gradients (RHoG) and demonstrated its

security against various attacks. The experiments showed that the resulting secure iris templates achieve high matching performance on the CASIA-IrisV3-Internal and CASIA-IrisV4-Thousand datasets. The RHoG technique enables secure iris authentication while preserving user privacy and iris unlinkability. In addition, authentication is very fast and does not require pre-alignment of iris biometric samples. Yadav et al. (2020) top-performing paper in the LivDet-Iris 2020 competition by proposing a very effective liveness detection technique. George et al. (2021) used the modified MobileNetV2, and the proposed feature-serial architecture has achieved the highest BPCER10 across all test datasets, ranging from 0.16% to 3.09%. It has shown robustness against various presentation attacks, and the recommendations for future work include using lightweight deep learning models.

2.5.5 The Gait Recognition Paradigms

Gait recognition, a field that draws on machine learning, computer vision, forensic studies, and robotics, is of significant interdisciplinary importance. Applications span visual surveillance and offer non-cooperative observation in challenging subject-cooperation scenarios. Challenges in gait recognition include susceptibility to mimicry and variations caused by accidents, injuries, costumes, walking posture, viewing angle, load carrying, and weather conditions. Recognising individuals within a group of walking people adds complexity.

Pioneering the field, Wolf et al. (2016) introduced a gait identification system that understands motion from various viewing angles by utilising 3D Convolutional Neural Networks (CNNs). Zhang et al. (2019) suggested a Siamese neural network that uses Gait Energy Images (GEI) to distinguish between different sequences. Battistone and Petrosino (2019) introduced gait recognition using a time-based Long Short-Term Memory (LSTM) network. Zou et al. (2018) designed an investigative hybrid convolutional neural network and recurrent neural network (CNN-RNN) model for gait recognition using smartphone sensors. GaitGAN (Yu et al., 2017) used the generative adversarial networks to generate invariant gait images. Zhang et al. (2019) designed an Auto-Encoder framework that disentangles pose and appearance features, and the resulting model is beneficial for gait recognition (Zhang et al., 2019). Fan et al. (2020) introduced GaitPart, a model for fine-grained learning of part-level spatial features. Liao et al. (2020) introduced PoseGait, a model based on human body structure and prior knowledge. Li et al. (2020) presented a semi-supervised

disentangled machine learning model for gait recognition. Xu et al. (2023) proposed cross-view algorithms, including Pairwise Spatial Transformer Networks and multi-view gait image synthesis, to improve cross-view gait detection accuracy.

Iwama et al. (2012) contribute to the field by constructing and evaluating the world's largest gait database. This study addresses existing database limitations, evaluates gait recognition performance, and provides insights into the impact of gender and age on recognition. Despite the dataset's considerable size, future work involves collecting more data for specific age groups and conducting further analysis, indicating the continuous evolution in gait recognition research. Pose and appearance features for effective gait recognition. Fan et al. (2020) proposed GaitPart, a part-based model for fine-grained learning of part-level spatial features. Liao et al. (2020) introduced PoseGait, a gait recognition model based on body pose and human prior knowledge. Li et al. (2020) presented a framework utilising semi-supervised disentangled representation learning in gait recognition.

Marin-Jimenez et al. (2021) proposed a unified framework, UGaitNet, for multimodal gait recognition. The proposed method addressed the shortcomings of state-of-the-art methods and adopted multiple modalities, achieving results while efficiently handling missing modalities. Therefore, it effectively addressed the challenges of gait recognition, provided a complete solution for real applications, and has great potential for further research.

Van Hamme et al. (2021) analysed security threats to biometric authentication systems and investigated current threats to Inertial Measurement Unit (IMU)-based gait authentication. The findings present the risks of template leakage in unprotected systems and explore the security of protected biometric templates, providing valuable insights for the secure design of authentication systems based on them.

2.5.6 The Voice Recognition Paradigms

Voice Recognition, synonymous with speaker recognition, is the process of identifying individuals by analysing voice attributes, including behavioural elements such as accent, tonality, vocal texture, and pitch. Automated speaker recognition has its roots in the 1960s, stemming from the need to identify callers issuing verbal bomb threats over the phone, which led to the development of technologies at Bell Laboratories. The National Institute of Standards and Technology (NIST) Speaker Recognition Evaluation (SRE) datasets, initiated in 1996, serve as

benchmarks for evaluating speaker recognition systems. Notable datasets include SRE 2016 and SRE 2018. The evolution of voice recognition technologies has shifted from i-vector-based approaches to deep learning, markedly enhancing performance. Pioneering works include the D-vector Approach (Variani et al., 2014), which introduced a frame-level deep neural network (DNN) for text-dependent speaker recognition, and the X-vector Approach (Snyder et al., 2014), which produced "x-vectors" with a time-delay neural network at the segment level, surpassing traditional i-vector systems.

End-to-end approaches, such as those incorporating triplet, GE2E, and intra-class losses, have demonstrated notable performance improvements. Mutual Information Maximisation (Ravanelli & Bengio, 2018) introduced the concept of learning speaker embeddings from raw waveforms, outperforming traditional methods on the VoxCeleb corpus. Additionally, by combining feature extractors and large-margin loss functions, as proposed by Bhattacharya et al. (2019), researchers showed that this approach achieves ultramodern results on both VoxCeleb and NIST-SRE 2016.

To bolster the security of Speaker Recognition Systems (SRSs) propose Adaptive F-ratio-based Partial Masking (AFPM) to improve the robustness of Speaker Recognition Systems (SRSs) against various adversarial attacks. The proposed AFPM leverages the concept of Partial Masking (PM) to efficiently strip out non-robust features. By integrating the F-ratio-based PM (FPM) and an adaptive threshold calculation algorithm, the proposed AFPM achieved robustness against various adaptive attacks and is suitable for many SRSs.

Addressing the challenge of countering human impostors and deepfake attacks on speaker recognition systems, Yang et al. (2021) present SA-DTH-Net, a robust lip-based visual speaker authentication method. They utilised a deep convolutional neural network (DCNN) combined with Fundamental Feature Extraction (FFE-Net) and Representative Lip Feature Extraction and Classification (RC-Net) to perform multi-task learning, thereby strengthening the ability to resist DeepFake attacks during authentication. The experimental results show that their proposed method is very efficient and robust against DeepFake attacks and human impostors. Marras et al. (2023) researched a new vector-dictionary attack that targets the speaker or voice verification systems. The attack is created to maximise the raw similarity of the

speaker and mimic a large proportion of the speaker's features, using adversarial optimisation.

Wang et al. (2023) research on a full-spectrum solution for deploying speaker recognition models in mismatched domains. Their models are trained on heavy-tailed PLDA (HT-PLDA) and Gaussian PLDA (G-PLDA) and employ several domain adaptation (DA) techniques, along with correlation alignment (CA) and covariance regularisation (CR), to improve the robustness of the speaker recognition models in mismatched environments. Experimental validation on NIST datasets demonstrates the effectiveness of these techniques, with improvements in HT-PLDA systems. The study emphasises the superiority of HT-PLDA and underscores the importance of tailored domain-adaptation methods for optimal speaker recognition system adaptability in real-world scenarios.

2.5.7 The Ear Recognition Paradigms

Ear recognition is a Biometric trait that analyses the distinct features of the human ear, from facial images (Yan & Bowyer, 2007). The human ear photographed from both sides of the head. Hence, it becomes a valuable biometric trait in cases involving non-cooperative subjects. The use of ear images is restricted due to occlusions caused by hair, hats and jewellery, etc. The classical approach to ear recognition includes Geometric, Holistic, Local, and hybrid methods to handle occlusions and intra-class variations in the use of ear images for authentication. The current use of Deep learning methodologies in ear recognition systems has improved performance, as reported below.

Emerson et al. (2017) proposed a deep learning-based averaging approach to prevent overfitting in small databases. Zhang et al. (2018b) leveraged convolutional neural networks (CNNs) for an ear verification framework under uncontrolled conditions. Emer et al. (2018) explored the impact of ear accessories on recognition, comparing CNN-based methods with traditional approaches. Zhang et al. (2019) proposed a few-shot learning technique for situations with limited training data. Sinha et al. (2019) proposed a framework based on Histograms of Oriented Gradients (HOG) and Support Vector Machines (SVMs) for outer ear localisation. They employed CNNs to address the challenges of illumination, angle, contrast, and scale. Other studies, such as Omara et al. (2018) and Štepec et al. (2020), proposed various approaches, such as feature fusion using Discriminant Correlation Analysis (DCA), hierarchical deep

features, and a constellation-based deep learning approach for ear biometrics. These studies confirm the value of deep learning in ear biometrics to address current challenges and improve performance. Kang et al. (2020) introduced a new deep neural network (DNN) for Transient Evoked Otoacoustic Emission (TEOAE) biometric systems, focusing on multi-session verification and identification. The TEOAE used in this research is a 20ms ear-generated response. This is chosen because the TEOAE is highly resistant to Spoofing and Replay Attacks. This, therefore, makes the TEOAE biometric more secure and robust. The proposed deep learning model utilises the triplet loss function to generate the TEOAE embeddings. The identification accuracy of the proposed model is 99.3 ± 1.04%, and the equal error rate (EER) is 0.187 ± 0.146% in the verification test. This proposed deep learning model has achieved 7.56% and 13.3% improvements over existing models for identification and verification, respectively.

Maity et al. (2015) proposed a model based on a Continuous Wavelet Transform (CWT) that is feature-extraction-free. The research developed a system to address the various challenges in 3D ear biometrics. The ear images were segmented by using an active contour model, and 3D shape and depth features were used for hierarchical categorisation. Using an active contour model, they outperformed other approaches, achieving a rank-one recognition rate of 98.5% on the University of Notre Dame Collection J2 dataset. The tree-based indexing approach reduces the search time up to 50% by reducing the search space. The proposed work has shown fully automated, robust, and efficient results for 3D ear biometrics, and this work will be extended to multi-modal Biometrics in the future.

Liu et al. (2023) introduced Stimulus-Frequency Otoacoustic Emission (SFOAE) as a new biometric feature. Because of its high stationarity and lower susceptibility to hearing loss, SFOAE has great potential for applications in both voice and speech biometric verification and identification. By fusing features from SFOAE spectra across different stimulus levels, the equal error rates (EERs) obtained using linear discriminant analysis (LDA) and a multi-kernel convolutional neural network (Mk-CNN) for closed-set and open-set verification are 0.541% and 1.364%, respectively. The SFOAE-based system shows great robustness and potential in the biometric field. Finally, the study also recommends a future enhancement study to develop a multi-session SFOAE system, build a specific SFOAE-based biometric

database, and fine-tune the frequency ranges of SFOAE to improve system performance.

2.5.8 Contactless Weight Scaling

The contactless applicability of different biometric features and a comparative analysis across various biometric modalities reveal distinct levels of contact requirements. Face recognition stands out as a highly contactless modality, scoring a five on the proposed scale, owing to its non-intrusive nature and widespread use in surveillance and mobile authentication (Taigman et al., 2014; Sun et al., 2014a). Gait is also five since, almost inevitably, there is no need for bodily contact between a person and an authentication device for gait authentication. This holds for those 3D CNN and Siamese network-based authenticators that have been reported extensively in the scientific literature (Darlow et al., 2017; Tang et al., 2017). Voice is Four. While voice-based modalities have currently adopted DNN-based i-vectors and x-vectors for voice recognition (Snyder et al., 2018; Dehak et al., 2011), as demonstrated in the audio examples provided in earlier sections, a form of verbal authentication would therefore be assigned a score of four. Ear is also four. Based on Siamese and graph LSTM network-based authentication, the ear-based biometric system would still be contactless, as only minimal body parts (perhaps only the shoulder) are in contact with the authentication device, and a score of 4 is given (Zhao & Kumar, 2017;). Fingerprint recognition, exemplified by MENet and FingerNet, scores a 2.5, as it involves minimal physical contact with a fingerprint scanner, but still requires contact for accurate readings (He et al., 2018; Tang et al., 2019). Iris recognition, utilising VGGNet-based models and attention networks, scores a 3, as it typically involves proximity to an iris scanner, albeit without direct physical contact (Daugman, 2004; Nguyen et al., 2017). Palmprint recognition scores a 2, as it often requires placing the palm on a scanner, which provides greater contact than other modalities (Zhang et al., 2019; Zhao & Kumar, 2017). This proposed contactless scale aims to comprehensively evaluate the physical interaction levels for each biometric modality, facilitating informed decision-making across diverse application scenarios. Table 2.15 shows the summarised scores, which are evaluated by the distance needed for authentication.

Table 2.15 Summary of Contactless Scale Weighting

Biometric Trait	Score
Face	5
Fingerprint	2.5
Iris	3
Palmprint	2
Gait	5
Ear	4
Voice	4

2.5.9 Performance Rating of These Biometric Traits

To analyse the performance of each biometric trait (gait recognition, voice recognition, ear recognition, palmprint recognition, iris recognition, fingerprint recognition, and face recognition), a performance score from 1 to 5 is assigned, with 5 being the highest and 1 the lowest, to form a theoretical scaling. Based on the information provided in section 2.5, these factors, such as accuracy, EER (Equal Error Rate), the dataset used, and model robustness, have been considered. This performance scaling was aided by reviewing the study/survey on Biometric Deep Neural Networks (DNN) compiled by Minaee et al. (2023).

Table 2.16 Summary of Biometric Evaluation Scale

Biometric Recognition	Score
Face	4.5
Fingerprint	4.5
Palmprint	5
voice	4
Iris	5
Gait	3
Ear	3

This section summarises the performance ratings in Table 2.16.

- **Face recognition performance score: 4.5**

  Explanation: Facial recognition models have found wide applications with high accuracy. The accuracy of verification and identification tasks is generally

above 95% (Taigman et al., 2014; Sun et al., 2014b, 2015; Parkhi et al., 2015; Schroff et al., 2015; Zhang et al., 2019; Liu et al., 2017; Ren et al., 2022; Krivokuca Hahn et al., 2023; Bao et al., 2023). Deep learning-based methods are generally better than traditional approaches. Deep learning-based models perform well on benchmark datasets such as MegaFace. Face recognition is mostly used because deep learning-based models and large amounts of training data are readily available today. Face matching has drawbacks when faced with various conditions, such as occlusion and mask-wearing.

- **Fingerprint recognition performance score: 4.5**

Explanation: The Fingerprint recognition models show or present a strong performance, with accuracy rates ranging from around 95.70% to 100% (Minaee et al., 2019; Lin & Kumar, 2017; Darlow & Rosman, 2017; Pandya et al., 2018; Ding et al., 2023). Deep learning-based fingerprint recognition algorithms have achieved remarkable accuracy levels on benchmark datasets, such as PolyU, FVC and CASIA.

- **Palmprint recognition performance score: 5**

Explanation: High Accuracy Palmprint recognition models give very high accuracy rates (99% and more) (Rida et al., 2019; Xu et al., 2019; Michele et al., 2019; Jalali et al., 2015; Minaee & Wang, 2017; Shao et al., 2021; Yang et al., 2023; Shao et al., 2024). Deep learning-based approaches are achieving remarkable accuracy and scores on the PolyU dataset, demonstrating the robustness and effectiveness of these models for palmprint recognition.

- **Iris recognition performance score: 5**

Explanation: Iris recognition models provide accuracy of more than 99% (Farouk, 2011; Alvarez-Betancourt & Garcia-Silvente, 2016; Menon & Mukherjee, 2018; Minaee et al., 2015, 2016; Zhao & Kumar, 2017; Wei et al., 2022; Fang et al., 2021). Deep learning algorithms work much better than traditional methods for classifying iris images in various iris databases. Deep learning methods deliver robust, accurate results for Iris recognition systems.

- **Voice recognition performance score: 4**

Explanation: Voice recognition systems based on deep learning models have shown high accuracy with Equal Error Rates (EERs) ranging from 3.22% to

6% (Shon et al., 2018; Ravanelli & Bengio, 2018; Okabe et al., 2018; Cai et al., 2018; Hajibabaei & Dai, 2018; Chung et al., 2018; Xie et al., 2019; Wang et al., 2023; Marras et al., 2023; Yang et al., 2021). Deep learning-based voice recognition systems achieve over 95% accuracy on the VoxCeleb1 dataset. The use of deep learning-based approaches contributes to the impressive performance, indicating the effectiveness of these models in speaker recognition tasks.

- **Gait recognition performance score: 3**

Explanation: Gait recognition models fall in the range of average accuracy of 68.50% to 95% as shown in most papers (Kusakunniran et al., 2013; Muramatsu et al., 2015a; Wu et al., 2016; Yan et al., 2015; Fan et al., 2020; Marin-Jimenez et al., 2021). There are several models with varying performance due to differences in datasets and evaluation and test conditions, which introduces significant uncertainty into existing models. Moreover, some models have very high and others very low accuracy values, indicating scope for improvement in the existing models to reduce the uncertainty in their accuracy.

- **Ear recognition performance score: 3**

Explanation: Ear recognition models show varying performance, with accuracy ranging from 62.48% to 99.94% (Zhang et al., 2019c; Eyiokur et al., 2017; Omara et al., 2018; Sinha et al., 2019; Tian & Mu, 2016; Kang et al., 2020; Štepec et al., 2020). While some models achieve high accuracy rates, others exhibit lower performance. The choice of dataset and the specific deep learning architecture may influence the overall performance of ear recognition systems.

Conclusion

Minaee et al. (2023) informed the construction of the performance scale by providing a consolidated review of deep-learning-based biometric recognition methods across different modalities. The survey supported the identification and comparison of the recognition techniques, benchmark datasets, reported performance and limitations associated with different biometric traits. I used this evidence, together with other modality-specific studies reviewed in Section 2.5, to assess each trait against four considerations: recognition accuracy, Equal Error Rate (EER), dataset characteristics and model robustness.

For example, face recognition received a score of 4.5 because the reviewed studies generally reported high recognition performance, frequently exceeding 95% on benchmark datasets. However, practical limitations such as facial occlusion and mask-wearing prevented it from receiving the maximum score. Similarly, palmprint and iris recognition received scores of 5 based on the high performance reported in the reviewed studies, while gait and ear recognition received scores of 3 because their reported performance varied more considerably across datasets and evaluation conditions.

The scores in Table 2.16 were therefore assigned by the researcher through a comparative synthesis of published evidence. Minaee et al. (2023) informed this assessment but did not directly provide the numerical ratings. The scale was developed as a theoretical means of comparing the relative performance of biometric modalities for the proposed fusion system.

2.6 HUMAN-COMPUTER INTERFACE AND BIOMETRICS

This section outlines the contribution of researchers to the field of Human-Computer Interface (HCI), which lies in its comprehensive overview, methodological insights, and exploration of potential applications, providing a valuable resource for researchers and practitioners in the domain. The review presents ideas for the proposed methodological process for HCI and behavioural biometrics for user recognition in IIoT ecosystems, addressing HCI challenges.

2.6.1 Past Works on Different Human-Computer Interfaces

There have been numerous studies examining the acceptance of biometric technology in various contexts, including security and authentication applications. Jones et al. (2007) began researching users' preferences regarding biometric authentication. Elliot et al. (2007) conducted research and highlighted the importance of hygiene and safety issues surrounding biometric authentication. Tassabehji et al. (2009) conducted a study centred on e-banking security and found a positive correlation between users' perceptions of biometric security, demonstrating their willingness to adopt it for online banking. In telephone banking, another study by Gunson et al. (2011) investigated different dialogue designs for speaker recognition and found that users were more likely to utilise a two-factor authentication system. De Angeli (2004) examined the

potential integration of biometrics into an Automated Teller Machine (ATM) system and found that a balance must be struck between security and usability.

A further study by Gunson et al. (2011) examined different dialogue designs for a speaker recognition system in telephone banking and concluded that users were more likely to use a system that included two-factor authentication. Blanco-Gonzalo et al. (2019) proposed replacing the classical CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) with fingerprint and face recognition for smartphone users. Zimmermann and Geber (2017) conducted an HCI study comparing various authentication schemes, with users favouring biometrics for its uniqueness and unforgeability. Thakur et al. (2023) recommended behavioural biometrics, such as touch-stroke dynamics, swipe gestures, and voice recognition, for user authentication in IoT. touch-stroke dynamics, swipe gestures, and voice recognition for securing IoT interfaces. Recent advances in user authentication for wearables, for example, are categorised into two main types of biometrics: (i) physiological and (ii) behavioural biometrics, explored by Vhaduri et al. (2017), focusing on the unique challenges posed by wearables for user recognition. These studies paint a comprehensive picture of the evolving scope of user acceptance research in biometrics, encompassing diverse applications and technologies throughout the years.

2.6.2 Advances In Human-Computer Interaction and Biometric Systems

This subsection summarises the latest advances and challenges reported in the fields of Human-Computer Interaction (HCI) and biometric systems. The following text summarises the results obtained in several works on HCI and biometrics. Blanco-Gonzalo et al. (2019) explored the challenges and advancements in designing effective biometric systems for robust performance, with a focus on mobile environments. The study reviewed modalities Such as fingerprint and face recognition, assessed user acceptance, and introduced a comprehensive evaluation framework for HCI in biometrics.

Miller et al. (2020) extended the previous research to a behaviour-based authentication system for Virtual Reality (VR). The system developed for VR (Virtual Reality) systems (in particular, for user authentication within and across systems), on authentication accuracy, and on cross-system authentication. The study used several

trajectory features to sample the feature space. It also investigated the use of feature combinations to improve performance. This work is furthering VR authentication for many applications. Dave et al. (2021) advocated a challenge-response methodology for detecting liveness in Face biometric systems to address face spoof attacks. The approach involved user engagement through natural gestures, fortifying security against identity spoofing. The research emphasised the need for future studies to broaden the scope of liveness indicators. Cross-System Behaviour-Based Authentication in Virtual Reality Biometrics Using Siamese Neural Networks by Miller et al. (2021) proposed a new approach to cross-system behaviour-based authentication in the field of Virtual Reality (VR) biometrics using Siamese neural networks. The authors tested the proposed approach and found that it gave lower Equal Error Rates (EERs) and better identification accuracy than the other approaches. The authors also discussed the ethical implications of the proposed approach. They suggested that the approach should be deployed locally to protect the user's privacy.

Houssein et al. (2022) provide a comprehensive review of current EEG (Electroencephalography) and ECG (Electrocardiography) signal-based HCI applications, including brain-computer interfaces (BCI), emotion recognition and biometric authentication. They also investigate emotion recognition using EEG and ECG signal fusion and propose a wearable EEG-based emotion recognition system. Warp et al. (2022) explored the application of biosensing technology and VR to investigate the impact of spatialised audio on emotional responses in Immersive Virtual Environments (IVEs). The results showed that spatialised audio significantly influenced users' emotional responses, suggesting its important role in the design of VR content and audio, and its potential to benefit auditory neuroscience.

Miller et al. (2022) investigated how behaviour-based authentication in VR changes over time as users' behaviour evolves. The results show that the changes in authentication are small and stable in the short and medium term, while the long-term evolution of the users' behaviour should be considered. This work provides a good foundation for designing robust and applicable behaviour biometrics for VR. Abe et al. (2022) developed a system called Hype Live that integrates the unity of VR live performances through biometric-based feedback. Using their system, the authors showed that applying a Moshing experience with haptic feedback to audience members increases the unity of their behaviour. The current NPCs need further refinement. In summary, this study contributes to HCI and biometric systems and

offers insights into the design of future security and interaction technologies. Biometrics in HCI has the potential to significantly change many applications.

2.7 VIRTUAL ENVIRONMENTS AND IIOT

Bibri et al. (2022) and Rasco et al. (2020) show that Virtual Reality is a key technology with a major impact on education, the design of learning courses, and the design of industrial simulations. This section highlights the socio-technological impact of using the technology in research, especially in creating immersive research environments. The term "virtual worlds " originated in electronic games and was widely adopted in the research community on massive multiplayer online role-playing games (MMORPGs) and online social networking. The second generation of virtual worlds, social VR, promises total immersion and connectivity to social networking sites, transforming the sense of presence and social interaction within these environments (Ondrejka, 2008).

The emergence of social VR has become a pivotal technological development, attracting multidisciplinary scholarly attention. While VR has its history of industrial and scientific applications, the advent of Virtual Worlds in the 1990s has rejuvenated its significance, particularly in industry and academia. (Slater & Sanchez-Vives 2016; McVeigh-Schultz et al., 2018).

2.7.1 Communication Modes and Social Behaviours in Social VR

This section examines the social behaviour and communication within the Social VR platforms and how different social space layouts influence user behaviour. Social VR platforms are applications which enable users to be physically present in a virtual social space. Therefore, the layout of the space and user behaviour in it both affect communication and emergent social behaviour in the platform. VR is currently one of the leading topics in education technology. With its ability to create, practice, and even enhance learning experiences, a growing number of studies are exploring the potential of Virtual Reality (VR) in education and training, and proposing possible use cases for VR-based learning systems (Kwona & Hudson-Smith, 2018; McVeigh-Schultz et al., 2018).

2.7.2 VR Software Platforms and Selection Rationale

Examining several virtual worlds such as High Fidelity, Second Life, AltspaceVR, VRChat, Sansar, OpenSim and Decentraland, with the goal of setting up an experimental space to test the efficiency and effectiveness of Biometric authentication. The criteria considered in this phase are the level of immersion, the user database, user-generated items (objects, buildings, avatars), the ability to create structures and equipment, the ability to buy real estate, the ability to conduct business through the platform, and the simulation of data. The socio-technological analysis of the chosen platform focuses on the platform's spatial structure and the reasons for choosing Second Life.

2.7.2.1 Evaluation of Virtual Environments

The following are current, available Virtual Reality environments on the market that could be a potential match for this study.

- **High Fidelity:** remarkably high immersion and has quite a bit of customisation. The small community is the major downside, since it is tough to get enough participants for a study.
- **AltspaceVR**: Prioritises immersive VR experiences but lacks extensive support for user-created designs and advanced business transaction features.
- **VRChat**: It stands out for high immersion and a substantial user base but emphasises social interaction over intricate business simulation.
- **Sansar**: Excels in high-quality graphics and VR support, fitting for immersive experiences with a growing, evolving user base.
- **Decentraland**: Highlights a decentralised approach with blockchain technology, supporting user-created content and transactions.
- **Open Simulator (OpenSim):** offers more flexibility and control, especially for users with technical skills.
- **Second Life**: provides a more streamlined experience with a more extensive user base as compared to the mentioned / listed software and a centralised economy.

Table 2.17 Comparison with virtual environments (Ondrejka, 2008)

	Criteria	Comparison Between the Mentioned VR Apps
1	Immersion	All platforms, including Second Life, offer varying degrees of immersion, with a focus on realistic graphics and VR support (Slater, 2016).
2	User Database	Second Life and VRChat have larger, more established user bases than other platforms, contributing to a more diverse and dynamic research environment (Dionisio, 2013).
3	User-Created Designs and Company Creation	Second Life, High Fidelity, Sansar, and Decentraland allow users to create content, but the extent of user-generated content and the emphasis on company creation may differ (Ondrejka, 2008).
4	Mobile app	With the new Second Life mobile app, it is expected that users will have greater access to this VR simulation and that the user database will grow, as noted on the official Second Life website (Gartner, 2023).
5	Business Transaction Platform	Second Life, High Fidelity, Sansar, and Decentraland have virtual economies and support transactions, but the formality and features may differ (Bloomfield & Rennekamp, 2010).

2.8 USEABILITY FUNCTIONALITY FACTORS IN IIOT

The Industrial Internet of Things (IIoT) has witnessed significant adoption across various industries, connecting devices, machines, and systems in industrial settings to facilitate data collection and enable real-time monitoring, control, and automation (Tange et al., 2020). This section examines the usability aspects of implementing Biometrics in the IIoT sphere, particularly emphasising human-computer interaction experiences.

In biometric access control within IIoT, usability is one of the important criteria affecting the success of a biometric system. Section 2.4, as outlined in Table 2.12 and Section 2.5, comprehensively reviews different biometric traits and their respective acquisition pathways to ensure a seamless user experience. The comparison presented in Section 2.5.8, detailed in Table 2.13, shows that biometric traits commonly fall into

either contact or contactless categories, and that physical attributes or individual behavioural characteristics predominantly determine their performance ratings.

One of the primary advantages of employing biometric traits for access control in IIoT is eliminating the need for external artefacts for authentication. Its accuracy ratings in section 2.5.9 shows the dependency and accuracy scale when applied to Artificial Intelligence. Contactless authentication eliminates the need for physical tokens and provides a more secure alternative to knowledge-based authentication systems. Biometric access control is based on characteristics that are inherently linked to physical attributes or behaviour, so it does not suffer from the risks of token cloning, loss or theft, knowledge disclosure, or lost passwords.

Afianian et al. (2020) conclude that biometric access control in the context of IIoT is a simple, fast, and convenient way to authenticate users. Biometric functionality in IIoT systems aligns with users' natural characteristics, therefore increasing the usability of access control systems. We refer to the existing literature on test methodologies and deployment approaches to support a user-centric view of biometric access control systems in the IIoT environment, from the development phase to the end user.

In conclusion, the usability factors of biometric access control in IIoT play a pivotal role in shaping user experiences and enabling secure, efficient authentication. The integration of biometric traits, as highlighted in recent papers, contributes to the seamless operation and enhanced security of IIoT systems, paving the way for broader industrial adoption.

2.8.1 Operational Technology Security Standards

This Section addresses identification and authentication of workers at points of access. Industrial security standards define requirements this function must meet. They are context, not the subject.

IEC 62443 relevance to access control and authentication are Part 1-1 (zones, conduits, security levels; IEC, 2009), Part 2-1 (asset owner programme, access control policy), Part 2-4 (service providers, remote and vendor access), Part 3-2 (risk assessment and zone partition, setting a target security level per zone; IEC, 2020), Part 3-3 (system requirements, whose Foundational Requirement 1 covers identification and authentication control; IEC, 2013) and Part 4-2 (component requirements; IEC, 2019). Within FR 1, SR 1.1 (human user identification and authentication) is the

anchor. in summary, unique identification and authentication is added at security level 2, multifactor authentication on untrusted networks at level 3, and on all networks at level 4. Levels run from protection against casual misuse to sophisticated, well-resourced, motivated attackers. SR 2.8 and SR 2.12 (audit, non-repudiation) bear on traceability.

NIST SP 800-82 Rev. 3. Are the OT security guide covers SCADA, distributed control systems and PLCs, with an overlay on the NIST SP 800-53 catalogue (Stouffer et al., 2023; NIST, 2020). Relevant controls include IA-2 (user authentication with multifactor enhancements), IA-5 (authenticator management), PE-3 (physical access control) and AC-14 (permitted actions without authentication, the route for emergency exceptions). NIST SP 800-63B (Grassi et al., 2017) treats biometrics as one factor type.

The standards require authentication and say its strength should rise with the security level. They do not say how a worker in a helmet and mask, in noise and dust, can be authenticated without blocking work. Fusion research mostly addresses laboratory or consumer conditions (Kittler et al., 1998; Ross & Jain, 2003). This thesis addresses the space between them.

2.9 REVIEW OF ISSUES & PROBLEMS

The main challenges for the Industrial Internet of Things are energy management, security, and a user-friendly platform (the Human-computer interface) (Alcácer & Cruz-Machado, 2019). Below are the IIoT biometric access control issues and problems gathered from the research above.

2.9.1 Human-computer Interaction Problems

Human-computer interaction is the study and design of interactions between humans and computers or other technological systems. It focuses on creating user-friendly, efficient, and effective interfaces and interactions that account for users' needs, capabilities, and preferences. Section 2.4.2.1, Table 2.13 shows the biometric trait performance compared to one another, along with the usability, distinctiveness, and interaction factors. Sections 2.4 and 2.5 discuss the preprocessing stage of acquiring biometric traits, as this is the most crucial part for easing the following two stages. If the acquisition of a trait is seamless and accurate, the region-of-interest and feature-extraction stages will be perfect. Section 2.5 outlines the human-computer interaction challenges, how biometric traits are obtained, ease of use (Contactless nature),

performance rating, interaction mechanism, and contact form for different Biometric traits. The human-computer interaction problem identified from these sections focuses on ease of use in the Industrial Internet of Things (IIoT), summarised in Table 2.17. The IIoT focuses on workers who are covered in dirt, grumpy, and tired after work. The HCI should have the biometric access control expected to be seamless, time-saving, easy to use, accurate, and contactless. It should make authentication easy and seamless, without confusing staff.

Table 2.18 Summary of the problem from the research gathered from section 2.4.2 and section 2.4.3.

Usability and User Experience	Table 2.12 shows that most biometric traits are medium to high in terms of ease of use. It indicates that most interaction processes are complex, confusing, and time-consuming. IIoT workers will find adopting the technology strenuous and challenging (Oloyede et al., 2016).
Ethical and Social Acceptance	Biometric systems raise ethical questions about consent, surveillance, and potential misuse. Most staff or workers in the IIoT may have religious beliefs regarding gender profiling. Ensuring societal acceptance requires addressing these ethical concerns. (Jain et al., 2022).
Acquisition problem	Biometric access control and human interaction problems are in its acquisition. Utilising a range of sensors and advanced analytical algorithms to harness the power of Artificial Intelligence and deliver unparalleled detection and monitoring capabilities (Sisinni et al., 2018), an expected high-quality dataset of biometric acquisition in split seconds is gotten. We have had contact or cross-contact problems during the COVID pandemic, pointing to a shift toward contactless HCI across industries.
Information security	Human errors are a significant contributor to security vulnerabilities in IIoT systems. Employees might inadvertently share sensitive information, use weak passwords, or fail to follow security protocols. From a

	human-computer interaction perspective, these errors stem from poor user interfaces, confusing workflows, or insufficient training. Properly designed interfaces and clear procedures will mitigate these risks. IIoT systems often involve complex processes and a multitude of devices. Striking a balance between usability and security becomes a critical challenge. Users might resort to workarounds that undermine security if security measures are overly complex or cumbersome. Conversely, if security is too lax for the sake of convenience, vulnerabilities might emerge. Designing systems that are both user-friendly and secure requires careful consideration (Jain et al., 2022; Sadeghi et al., 2015; Saqib & Moon, 2023)

2.9.2 Issues With Biometric Access Controls

The research analysis in sections 2.4 and 2.5 reviews biometric recognition systems and outlines the issues and problems as standalone systems in Tables 2.18 and 2.19. The issues arising from biometric access control stem from biometric traits and their drawbacks, as determined by the biometric factors. Below is the drawback of each biometric trait.

Table 2.19 summaries of biometric traits drawbacks

Biometric Traits	**Factors Drawback**
gait	Its drawbacks include the high cost of the system, weight changes, physical changes, injuries, accidents, and posture. The variability in accuracy may stem from differences in datasets and viewing conditions, impacting the consistency of results. (Fan et al., 2020; Marin-Jiménez et al., 2017).
face	It has low accuracy and distinctiveness, as people bypass it; occlusion, matching faces across different conditions, and plastic surgery are a few drawbacks. (Ren et al., 2022; Krivokuca Hahn et al., 2023; Bao et al., 2023).

voice	The drawbacks include the cost of the system, manipulated voices, especially with artificial intelligence tools, illness-causing voice changes, and speech damage (Wang et al., 2023; Marras et al., 2023; Yang et al., 2021).
Fingerprint	Its traits must be obtained through contact, worn or burned ridges, ageing factors, and accidents (Minaee et al., 2019; Pandya et al., 2018; Ding et al., 2023)
iris	Its drawbacks are high cost, off-angle and occlusion (Wei et al., 2023; Fang et al., 2021).
Palm print	Its traits must be gotten through contact, worn or burned prints, ageing factors, high-cost systems and accidents (Shao et al., 2019; Yang et al., 2023; Shao et al., 2024).
ear	Its drawbacks include high cost, low privacy, and the importance of pose angle; the choice of dataset and the specific deep learning architecture may also influence overall performance and lighting conditions (Kang et al., 2020; Štepec et al., 2020).

Table 2.20 Biometric access control drawback

Drawback	**Explanation**
Variability in Biometric Traits	Section 2.4.2 shows that most biometric traits change over time due to factors such as age, injury, and environmental conditions (Oloyede et al., 2016).
Uniqueness	It is worth noting that most biometric features only differentiate individuals to a limited extent because people share many traits. (El-Abed et al., 2010).
System Integration and Interoperability	Integrating biometric systems with existing infrastructure/ IIoT is complex. Ensuring compatibility and smooth integration with other access control mechanisms is challenging (Afianian et al., 2020).
false acceptance or rejection	Biometric access control must balance accurate identification and false acceptance or rejection of authorised users. High false rejection rates lead to user frustration, while high false acceptance rates compromise security (Jain et al., 2022).

Circumvention (Spoofing Attacks):	Spoofing an individual's biometric traits deceives biometric systems. Hand signatory and vocal Biometrics are particularly vulnerable to spoofing attacks. The same goes for the Fingerprints trait; it is spoofed by replicating or copying fingerprints after the individual's fingerprints have been collected by tape lifting or other means. (Srinivasan & Balamurugan, 2014).

2.10 PROPOSED SOLUTION ARTEFACT 1

A proposed solution, simulated in an IIoT environment, is presented based on the literature review and the identified challenges in implementing biometric access control in the Industrial Internet of Things (IIoT). The objective is to improve the implementation of seamless, user-friendly biometric access control systems in IIoT settings. This proposed solution in Chapter 3 will address the gaps identified in Section 2.9 by integrating the proposed Biometric access control system and simulating it in an immersive Virtual Reality Environment, as discussed in Section 2.7. Figure 2.3 (Artefact 1) outlines the proposed architecture and theoretical artefact details gathered from Chapter 2 (Literature review).

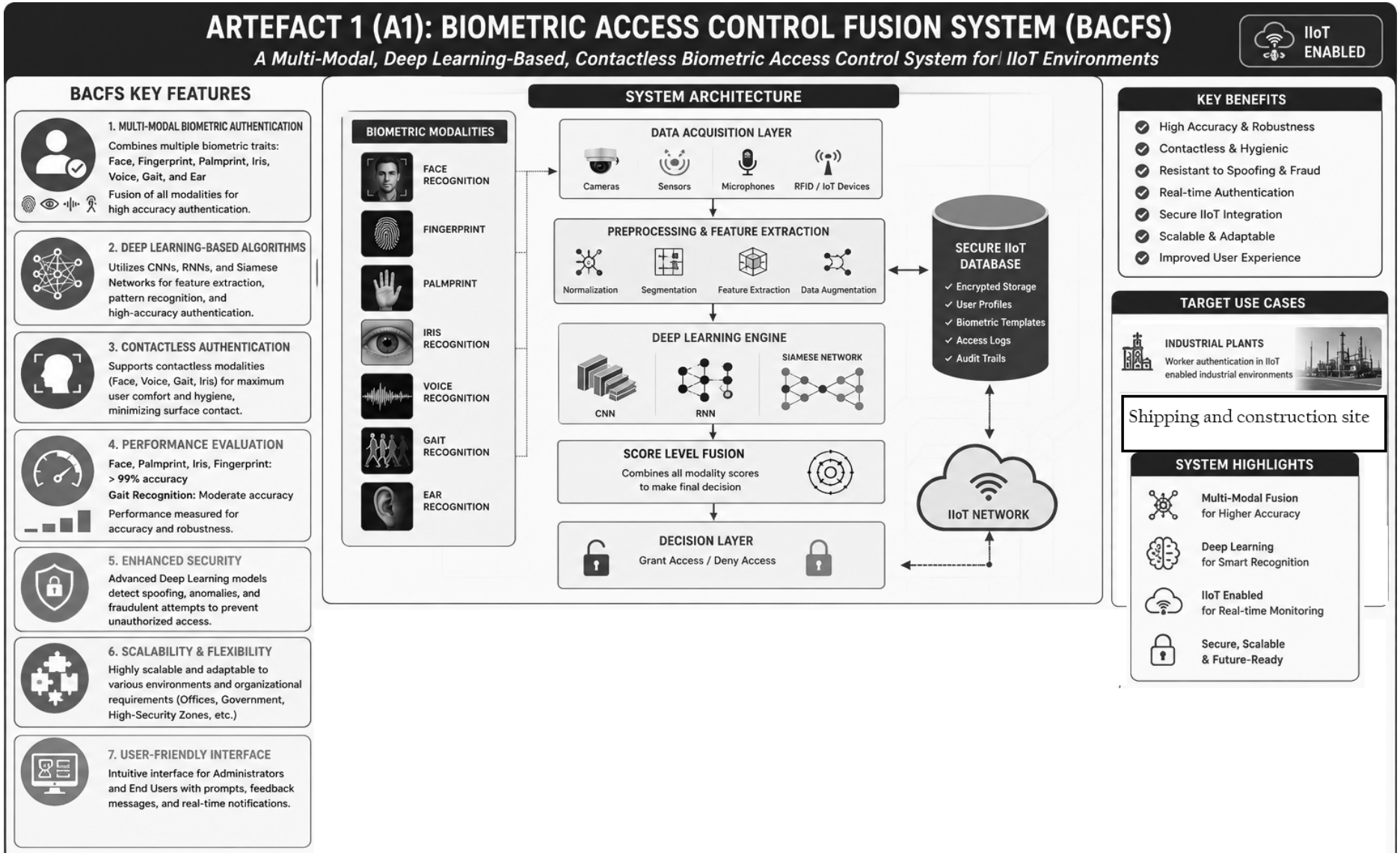


Figure 2.3 Artefact 1

2.10.1 Biometric Access Control Fusion System (BACFS) Features

The following are the proposed attributes for Artefact 1 (Artefact 1), as shown in Figure 2.3, which serves as the theoretical framework for this study. All other Artefacts are tested and created from the foundation and fundamentals established by the proposed literature-curated artefact.

- **Multi-Modal Biometric Authentication:**

  In the proposed access control system, biometric samples from various sources have been collected, including face, fingerprint, palmprint, iris, voice, gait, and ear. All the samples are merged to identify and authenticate the person.

- **Deep Learning-Based Algorithms**:

  Deep learning algorithms, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and Siamese networks, are used for feature extraction and pattern recognition. These algorithms analyse biometric data with unprecedented accuracy, enabling reliable authentication in diverse scenarios.

- **Contactless Authentication:**

  This system has the key objective of contactless services by means of face, gait, voice, etc. modalities, while the highest user comfort is being achieved and current hygiene rules are being fulfilled in full measure, and contact with surfaces is being avoided completely in order to keep any risk of contamination at a minimal level and mitigate concerns regarding surface contamination.

- **Performance Evaluation:**

  Accuracy and robustness of all modalities have been evaluated. Biometric modalities perform vastly differently and can be measured by their accuracy and robustness. While the performance of other biometric modalities, such as Palmprint, Iris, Fingerprint, and Face recognition, is very high in accuracy and robustness, with all achieving more than 99% recognition accuracy, gait recognition achieves only moderate recognition accuracy.

- **Enhanced Security:**

  This system uses advanced deep learning to better resist fake information and identity fraud. The system uses advanced technology to analyse information and block it if deemed suspicious or abnormal, thereby preventing third parties from accessing it.

- **Scalability and Flexibility:**

  The access control system designed for this project is highly scalable and adaptable to many environments and different organisational requirements. This system can be deployed in corporate offices, government facilities, or high-security zones. It can be modified to suit the organisational requirements.

- **User-Friendly Interface:**

  The system provides an easy-to-use interface for both Administrators and End Users, with several prompts and feedback messages to assist users and support ongoing management, while still meeting security requirements.

2.11 CONCLUSION

In this chapter, an in-depth exploration of the integration of biometric mechanisms within Industrial Internet of Things (IIoT) access controls has been conducted. A critical literature review of IIOT and Biometric access control challenges, developments and trends in the industry was conducted. In addition, this chapter investigated the applications of IIoT architecture in related industries. In addition, this chapter investigated the applications of IIoT on heavy machinery construction sites and in related industries. A literature review was used to discuss the opportunities and challenges of integrating biometric authentication into IIoT access control for heavy machinery construction sites and related industries. This review highlighted the pivotal role of access controls within these environments, emphasising the need for robust security measures to protect critical assets and ensure personnel safety. Biometric mechanisms were identified as a promising solution to address the shortcomings of traditional authentication methods and bolster access control systems. The interplay between human-computer interaction and IIoT access controls was explored, revealing the intricate relationship between users and biometric systems. The user-centric design of access control interfaces emerged as a critical consideration, with usability and user experience shaping the adoption and effectiveness of biometric mechanisms. The review highlighted the importance of accounting for the unique operational contexts of heavy machinery construction sites and other industrial settings in the design of these systems. Furthermore, the review delved into the multifaceted challenges and issues associated with biometric access control. These issues, underscored by the drawbacks of the biometric mechanism, necessitate robust biometric templates,

effective encryption methods, and continuous monitoring to ensure the integrity and confidentiality of biometric data.

The insights gained from this literature review form a strong foundation for Artefact 1, which is outlined in Chapter 3 (Methodology). The methodology chapter will detail the research design, data collection procedures, and analytical techniques employed in this study and build on the knowledge synthesised from existing research. The link between the findings of this literature review and the research methodology lies in their alignment to address the specific challenges posed by IIoT access controls using biometric mechanisms on heavy machinery construction sites and related industry. Chapter 3 presents a comprehensive methodology that draws on the rich insights from this literature review. By incorporating user-centred design principles, addressing security and privacy concerns, and leveraging the unique characteristics of biometric mechanisms, the aim is to develop a novel framework for IIoT access controls tailored to the specific demands of heavy machinery construction sites. The methodology chapter will serve as a roadmap to navigate the challenges and intricacies identified in the literature review. It guides the empirical exploration for an innovative approach.

Chapter 3: RESEARCH METHODOLOGY

3.0 INTRODUCTION

Chapter 3 focuses on selecting an appropriate methodology. The standard definition of a methodology refers to a systematic approach or set of principles, procedures, and techniques used to conduct research or solve a problem in a particular field. It outlines the steps and processes researchers use to gather data, analyse information, and draw conclusions. A methodology provides a framework for organising research activities, ensuring rigour, and facilitating the replication of the study's findings. These methodologies vary depending on the research domain or sector, the objectives, and finally, the underlying assumptions (Blanco-Gonzalo et al., 2019; Lawrence & Tavakoli, 2019; Shneiderman, 1998). Methodological approaches encompass qualitative, quantitative, or mixed methods approaches to gather data. It also serves as a roadmap for conducting research or achieving specific goals, guiding the researcher through the entire process from data collection to result interpretation. It is used to research and propose feasible solutions to the issues and challenges identified in Chapter 2 within the Industrial Internet of Things (IIoT) environment.

The methodology builds on the work of well-known researchers such as Bibri et al. (2022), Gnanasekar et al. (2023), Rasco et al. (2020), Hehn & Uebernickel (2018), and Mantravad et al. (2020) to better understand the topic. Section 3.1 issues and problems identified in the preceding chapter are evaluated for feasibility to determine which research gap is best further research. Section 3.2 presents the research questions and hypotheses derived from the selected issues and problems. Next, in Section 3.3, a review of five papers on related topics is provided to better understand what has already been done. In Section 3.4, a comparison of the different methods researchers used has been presented, highlighting what sets them apart, explaining why they were chosen, and describing the approaches used in their studies. Section 3.5 defines the methodology selection, and it details the research process steps, procedures, and methods for the methodology design.

Furthermore, Section 3.6 outlines the data collection structures and Experimental design analysis for artefact 1, explicating how data will inform the design and development of this artefact. Section 3.7 outlines the data collection structures and Experimental design analysis for artefact 2, detailing how data from the

test simulation of artefact 1 will inform the design and development of these artefacts. Section 3.8 outlines the testing process for artefact 1 and proposes a design for artefact 2, focusing on biometric access mechanisms. Section 3.9 outlines the proposed steps for the experimental analysis, employing statistical analysis and simulations to evaluate artefacts and hypotheses. Additionally, Section 3.10 describes proposed artefact 3, which involves expert feedback on biometric fusion from Second Life, and outlines the methodology for gathering this feedback. Finally, Section 3.11 discusses artefact outputs, analysing and interpreting the findings compared to the research questions and hypotheses outlined earlier. Together, these sections contribute to shaping the research narrative and understanding the study's outcomes.

3.1 ISSUES AND PROBLEMS FROM CHAPTER 2

This section outlines the issues and problems of the Biometric recognition Mechanisms as detailed in section 2.9 (literature review). Furthermore, it conducts a feasibility study to identify the issue and problem to be researched. This section identifies the issues and concerns to be addressed and outlines what this research would achieve. This section will inform the research questions and hypotheses by specifying which questions to ask and which hypotheses to test.

3.1.1 Research Problems Selection

Chapter 2 explored Biometrics access control in the Industrial Internet of Things (IIoT) and highlighted challenges, particularly within Human-Computer Interaction (HCI) and biometric access control (Section 2.7). These challenges impede the seamless and effective implementation of Biometric access control Authentication in IIoT technologies, necessitating closer scrutiny and resolution. Various issues were identified within the HCI domain for IIoT, including usability and user experience, ethical and social acceptance, information security (specifically human error), and acquisition problems. Meanwhile, issues such as the drawbacks of biometric traits, system integration and interoperability, false acceptance or rejection, and circumvention (spoofing attacks) were noted in biometric access control systems as seen in section 2.9.1.

These challenges were further substantiated by past research, as elucidated in the work of Jones et al. (2007), Elliot et al. (2007), Tassabehji et al. (2009), and others, which explored user inclinations towards biometric technologies in various contexts

such as Biometrics Systems in IIOT and speaker recognition for telephone banking. These studies underscore the importance of addressing HCI challenges in biometric systems, thereby significantly enhancing user acceptance and experience (biometric work in the HCI section 2.8).

Recent studies have made some big improvements in how people interact with computers and biometric systems. For example, researchers such as Blanco-Gonzalo et al. (2019), Miller et al. (2020, 2021), Dave et al. (2021), and others have developed new approaches to designing biometric systems and authentication methods that achieve greater accuracy than previous approaches. These studies have also given researchers a glimpse into how Virtual Reality authenticates people using biometrics by observing how avatars behave. More recently, Gnanasekar et al. (2023) and team examined biometric technology after the pandemic and highlighted the importance of fairness and ensuring everyone is included, regardless of background. This is important for this research, as discussed earlier, because it is not just about the technology, but also about how it affects people and society via biometric systems. Additionally, it provides a post-pandemic audit of biometric technology, emphasising fairness and Equity, Diversity, and Inclusion (EDI) in biometric-enabled systems, which aligns with the socio-technological intricacies of this study (as seen in section 3.1).

This study examines how to make Industrial Internet of Things (IIoT) biometric access control systems easier to use and more user-friendly while maintaining high standards of system effectiveness, efficiency, and accuracy. Section 3.1 provides a thorough review of previous researchers' work and outcomes, using this information to inform the approach taken, examine how people interact with technology, and develop systems that are both secure and easy to use. Tables 3.2 and 3.3 outline the issues and problems. The selected problem is identified in the Feasibility question column and marked as a "yes". As shown in Table 3.1, the feasibility analysis revealed that HCI's usability and user experience problem is achievable.

- **Rationale for selected research problems in HCI for IIoT and biometric access control**

  The selection of usability and user experience as research problems in Human-Computer Interaction (HCI) for Industrial Internet of Things (IIoT) and biometric access control is justified by several factors.

- First, usability is critical as it directly impacts the technology adoption based on the user satisfaction and system effectiveness (Thakur et al., 2023).
- Second, the HCI research in this area holds practical relevance for improving the daily interactions of the IIoT systems and the users, by enhancing productivity and business outcomes (Blanco-Gonzalo et al., 2019).

Moreover, aligning with industry trends and prioritising usability and user experience offers a competitive edge in the IIoT sector (Zimmermann & Geber, 2017; Dave et al., 2021). Furthermore, addressing usability issues offers tangible improvements that are implemented relatively quickly, making it an attractive area for research and intervention (Jones et al., 2007). Another advantage is that using a user-centric approach ensures that IIoT systems are intuitive and aligned with users' mental models, enhancing adoption rates and fostering innovation (Blanco-Gonzalo et al., 2019; Lawrence & Tavakoli, 2019; Shneiderman, 1998). Additionally, usability research encourages cross-disciplinary collaboration, fostering creativity and innovation to solve complex HCI challenges (Preece et al., 2015). By focusing on usability and user experience, researchers aim to improve IIoT biometric authentication systems, drive adoption, and stimulate innovation. Table 3.1 summarises the multifaceted nature of challenges and opportunities in the IIoT as identified in these papers, spanning societal implications and fairness considerations

Table 3.1 HCI issues and problem feasibility table from section 2.9

	HCI Problems and Issues	**Feasible? Yes/No**
1	Usability and User Experience	Yes
2	Ethical and Social Acceptance	No
3	Information Security (Human error)	No
4	Acquisition problem	No

Table 3.2 Biometric access controls issues and problem table from section 2.9

	Biometric access control issues and problems	**Feasible? Yes/no**
1	Biometric Traits Drawbacks	No
2	System Integration and Interoperability	No

3	False Acceptance or Rejection	Yes
4	Circumvention (Spoofing Attacks)	No

3.2 RESEARCH QUESTIONS AND HYPOTHESIS

A research question guides the investigation to address identified research gaps and achieve the research objectives. Section 2.9 (Problems and issues) identified usability and user experience as the feasible research issues to be questioned. Conversely, a hypothesis is a statement of expectations that the research aims to evaluate and test. Based on the literature review presented in Chapter 2 and the problem identification outlined in Section 2.9, a primary research question and three sub-questions, each accompanied by three hypotheses. Identifying these research questions and hypotheses involves five stages.

At each stage of this process, thorough reflection on relevance and discussion with research supervisors occurred. An extensive literature search was conducted to determine if the identified research questions had been previously addressed. The outcome of this investigation suggested that the research contributes new findings to the Biometric access control in the IIoT domain, thereby enriching the existing body of knowledge (Collis & Hussey, 2021, p. 94).

3.2.1 RESEARCH QUESTIONS AND HYPOTHESES

Main Question: How can biometric access control enable industry workers to authenticate seamlessly in various conditions?

- **RQ1.** What are the limitations of using biometric authentication for industry workers?
- **RQ2.** What biometric traits can be used to identify and verify workers effectively?
- **RQ3** What Biometric mechanisms are required to develop a practical biometric access control framework tailored to IIoT requirements?

To answer research questions in the context of biometric access control fusion in IIoT, hypotheses are formulated to guide the investigation and provide a framework for testing the proposed solution. The hypotheses were formulated before the experiments, from the literature review and Section 2.9. and evaluated by converging evidence (Hevner et al., 2004; Gregor & Jones, 2007). Here are the hypotheses to be used:

- **H_1.** As the number of simultaneous constraints increases, the pass rate of the static fusion baseline decreases.
- **H_2.** Under the same constraints, multimodal fusion achieves a higher pass rate than any single trait.
- **H_3.** To develop a practical biometric access control framework tailored to IIoT requirements, it is necessary to incorporate robust multi-modal biometric mechanisms, advanced fusion algorithms, adaptive authentication methods, and integration with existing IIoT infrastructure. Additionally, ensuring compatibility with industrial environments, scalability, usability, and compliance with data protection regulations are crucial factors for the success of such a framework.

The purposes of the above research questions and hypotheses are to guide the investigation, optimise the output of biometric access control mechanisms, and improve user experience, effectiveness, and efficiency in IIoT environments, advancing technology and usability standards in industrial settings.

3.3 SIMILAR STUDIES

This section provides a comprehensive overview of the outlined research problems, open issues, contributions, and the research methods adopted by various authors in industrial IoT (IIoT) and related technological domains. The studies done in this section focus on valuable insights and frameworks to instruct and help design steps for implementing solutions and for addressing challenges such as:

- the societal implications of emerging technologies,
- fairness and inclusivity in biometric systems,
- financial literacy education,
- methodologies used
- security challenges in IIoT device integration.

Table 3.3 summaries of focus similar studies

Authors	Summaries
Bibri et al. (2022)	Researched the aspect of societal construction of the Metaverse and its implications for data-driven intelligent cities, advocating for transparent processes and public participation in its development.

Gnanasekar et al. (2023)	Examined the role of biometric technology in post-pandemic contexts, which emphasised fairness and Equity, Diversity, and Inclusion (EDI) in biometric systems. This study was based on ongoing biometric border issues in Europe.
Rasco et al. (2020)	Address financial illiteracy among youth and propose serious financial games for lifelong financial education.
Hehn & Uebernickel (2018)	Investigated the integration of Design Thinking (DT) and Requirements Engineering (RE) in innovative software-intensive projects to meet stakeholders' evolving needs.
Mantravad et al. (2020	Addresses the security challenges of integrating low-power IIoT devices into Industry 4.0 modular manufacturing systems, focusing on securing data exchange between the Manufacturing Execution System (MES) and Programmable Logic Controllers (PLCs) in smart factories.

Table 3.3 presents social-technological studies that offer diverse perspectives and methodological approaches to address complex challenges in the IIoT, ranging from societal implications and fairness considerations to educational approaches, design methodologies, and security paradigms. They provide valuable insights and actionable recommendations for creating more inclusive, secure, and sustainable IIoT ecosystems by examining the intersection of technology, society, and industry.

The information in Table 3.4 also provides valuable insights and frameworks for addressing these challenges, guiding future research directions and practical implementations across various IIoT domains. These studies offer holistic perspectives and actionable recommendations for creating more inclusive, secure, and sustainable IIoT ecosystems by examining the intersection of technology, society, and industry.

Table 3.4 socio-technological similar studies

Author And Year	Research Question	Problem Identified	Open Issues Identified	Research Method	Contributions To IIoT
Bibri et al. 2022	How to address the societal impact of emerging technologies, focusing on determinism, social exclusion, privacy erosion, and democratic decline?	The problem identified is the potential consequences of the Metaverse and the need to safeguard individuality, privacy, and democratic processes in the evolving digital landscape.	• Understanding the social construction and political, economic, and historical influences on the Metaverse. • Addressing ethical and social concerns arising from the Metaverse's emergence, including determinism and privacy erosion. • Examining challenges related to significant tech influence, surveillance capitalism, and the erosion of individuality. • Balancing optimistic claims about the Metaverse	Grounded in Science and Technology Studies (STS).	• Provides insights into the societal construction of Metaverse. • Raises awareness of ethical and social concerns in the Metaverse. • Advocates for transparent processes and public participation in shaping the development of the Metaverse. • Guides future research directions in understanding the societal, ethical, and cultural implications of emerging digital technologies like the Metaverse

			with realistic assessments of its societal implications.		
Gnanasekar et al. 2023	What is the role of biometric technology in post-pandemic contexts, particularly in e-borders and e-health systems?	Identified gaps in technology-societal integration revealed during the pandemic and emphasise the importance of fairness and Equity, Diversity, and Inclusion (EDI) in biometric systems.	• Addressing biases in biometric systems related to age, gender, and race. • Ensuring fairness, trustworthiness, and risk assessment in biometric technology. • Integrating Emergency Management Cycle (EMC) phases into biometric system design for pandemic preparedness. • Conducting post-pandemic audits of biometric technology to identify shortcomings and areas for improvement. • Advancing fairness modelling and Doddington's effect modelling to mitigate	Four-fold audit strategy	• Provides a systematic approach for auditing biometric-enabled systems in post-pandemic scenarios, addressing fairness, inclusivity, and preparedness. • Highlights the importance of integrating EMC and EDI concepts into biometric system design for effectively managing emergencies. • Offers valuable insights into the current state of biometric technology, its shortcomings during the pandemic, and necessary steps for improvement. • Shows procedures and techniques to investigate

			biases and uncertainties in biometric systems.		biometric-enabled systems, contributing to enhancing their reliability and effectiveness in industrial IoT (IIoT) applications.
Hehn & Uebernickel 2018	How does Design Thinking effectively enhance the Requirement Engineering process in real-life projects?	Identified problems in the integration of Design Thinking (DT) and Requirements Engineering (RE) in innovative software-intensive projects to address the challenges of meeting stakeholders ' needs.	• Balancing exploration with documentation in the development process. • Formalisation of requirements elicitation methods within a DT framework. • Ensuring interdisciplinary collaboration and expertise in project teams. • Addressing challenges associated with usability and user experience in software development. • Understanding the morphing nature of DT	Design Thinking	• Balancing exploration with documentation in the development process. • Formalisation of requirements elicitation methods within a DT framework. • Ensuring interdisciplinary collaboration and expertise in project teams. • Addressing challenges associated with usability and user experience in software development. • Understanding the morphing nature of DT throughout different project phases

			throughout different project phases		
Mantravad et al. 2020	How to secure the data exchange between the Manufacturing Execution System (MES) and Programmable Logic Controllers (PLCs) in smart factories?	The paper addresses the security challenges of integrating low-power Industrial Internet of Things (IIoT) devices into Industry 4.0 modular manufacturing systems.	• The literature highlights vulnerabilities in Operational Technology (OT) architecture, particularly concerning the IT/OT link. • The security of the IT/OT link remains a weak point in factory cybersecurity. • There is no consensus on how to securely connect IT and OT systems, especially in modular manufacturing systems. • Existing cryptographic schemes for IIoT need further cryptanalysis and scrutiny.	Design Science Research Methodology (DSRM)	• Identifying vulnerabilities and challenges in securing IT/OT links in Industry 4.0 • Overview of cryptographic protocols tailored to low-power OT devices. • Recommendations for designing secure smart factories, incorporating insights from the Smart Lab case study and QFD analysis. • Formulation of a design principle for information systems security in modular manufacturing systems.

3.4 SELECTING METHODOLOGY

This section reviews methodologies for conducting a research experiment and collecting data. Section 3.3 (similar studies) was informative on studies that address research questions derived from issues and problems, and it clearly shows that the best-suited methodologies for the design of the proposed solution in section 2.11 are Design Thinking (DT) and the Design Science Research Methodology (DSRM). DSRM and DT, applied in the dynamic domain of socio-technological research, share the goal of addressing societal challenges. These methodologies employ divergent data collection and analysis methods, as well as divergent experimental designs and approaches. The Methodologies share empathy, problem-solving, iteration, and collaboration as their core values, but differ in the approaches, tools, and outcomes used to create solutions. In this section, the differentiation will be based on the review of section 3.1 and on similar studies that examined socio-technological papers that used both methodologies. The following sections will analyse and evaluate these methodologies.

3.4.1 Comparison Of Design Thinking and Design Science Methodology

This section compares Design Science research methodology with Design Thinking methodology to select the methodology for this study/research.

Table 3.5 Comparison table between Design Science and Design Thinking Methodology

Metric	Design Thinking	Design Science
Human-Centric Approach	Design thinking strongly emphasises understanding and empathising with end-users, leading to solutions that better meet their needs and preferences (Brown, 2008).	Design science may prioritise technological feasibility over user needs and preferences, potentially leading to solutions that are less user-friendly or intuitive (Hevner et al., 2004).
Creativity and Innovation	The iterative ideation and prototyping process in design thinking fosters creativity and encourages out-of-the-box thinking,	The focus on developing and evaluating artefacts within design science may limit the exploration of alternative solutions or approaches that

	leading to innovative solutions (Brown, 2008).	could lead to better outcomes (Hevner et al., 2004).
Interdisciplinary Collaboration	Design thinking draws upon diverse disciplines such as psychology, anthropology, and business, fostering interdisciplinary collaboration and a holistic approach to problem-solving (Plattner et al., 2009).	Design science research projects often require significant resources, including time, funding, and expertise, making them challenging to undertake, particularly for smaller research teams or organisations (Peffers et al., 2007).
User-Centred Design	By prioritising qualitative data collection methods like user interviews and observations, design thinking ensures a deep understanding of user experiences and preferences, resulting in more user-friendly solutions (Buchenau & Fulton Suri, 2000).	Despite rigorous testing and evaluation, design science solutions may encounter challenges during implementation in real-world settings, such as compatibility issues or stakeholder resistance to change (Peffers et al., 2007).
Objective Evaluation	The qualitative nature of data collection and analysis in design thinking may lead to subjective interpretations, potentially introducing biases into the design process (Brown, 2008).	Design science utilises qualitative and quantitative data collection and analysis methods to provide a comprehensive and objective evaluation of designed solutions (Peffers et al., 2007).
Practical Solutions	Design thinking's emphasis on creativity and empathy may sometimes result in solutions that lack rigorous scientific validation or fail to adequately address underlying systemic issues (Plattner et al., 2009).	Design science research methodology follows a systematic, rigorous approach to problem-solving, involving the development and evaluation of technological solutions using scientific principles (Hevner et al., 2004).

Iterative Improvement	The iterative nature of design thinking, involving multiple cycles of ideation, prototyping, and testing, is time-consuming and resource-intensive, particularly in large-scale projects (Brown, 2008).	The iterative nature of design science enables continuous improvement based on stakeholder and user feedback, leading to solutions that evolve to better meet their needs (Hevner et al., 2004).
Prototyping	Design thinking may prioritise individual user experiences over broader systemic issues, leading to solutions that may not scale effectively or address broader societal challenges (Plattner et al., 2009).	Design science focuses on creating tangible artefacts that address real-world problems, making it well-suited for addressing complex socio-technological challenges (Hevner et al., 2004).

Table 3.5 addresses the need to select the Design Science Research methodology (DSRM) for its ability to provide this study with a fast, iterative, and creative technical approach, particularly its prototyping approach to getting ideas out for iteration. The comparative analysis indicates that although Design Thinking and Design Science Research Methodology (DSRM) both provide valuable approaches to innovation, DSRM is the most appropriate methodology for this study. Design Thinking offers significant strengths in human-centred design, creativity, interdisciplinary collaboration, and iterative prototyping, enabling researchers to better understand user needs and generate innovative solutions (Brown, 2008; Plattner et al., 2009). However, its reliance on qualitative methods and subjective interpretation may limit the scientific rigour required for developing and validating secure technological systems. In contrast, DSRM provides a structured and systematic framework for designing, developing, demonstrating, and evaluating technological artefacts using both qualitative and quantitative evaluation methods, ensuring objective, reliable, and reproducible research outcomes (Hevner et al., 2004; Peffers et al., 2007).

The objectives of this study extend beyond understanding user behaviour. The research aims to design, develop, implement, and evaluate a novel multi-biometric fusion access control system for Industrial Internet of Things (IIoT) environments, followed by validation within a simulated virtual environment. Achieving these

objectives requires creating multiple research artefacts, conducting systematic experimentation, measuring performance, iterative refinement, and expert evaluation—activities that align directly with the principles of DSRM. Specifically, this research involves identifying the limitations of existing biometric access control systems for IIoT, designing a multi-biometric fusion authentication architecture, developing functional artefacts and authentication mechanisms, implementing the artefacts within a virtual IIoT environment using Second Life, experimentally evaluating authentication accuracy, security, usability, robustness, and system performance, and finally refining the artefacts through iterative evaluation and expert feedback.

These activities correspond closely with the six phases of Design Science Research proposed by Peffers et al. (2007), which are problem identification, objective definition, artefact design and development, demonstration, evaluation, and communication. Consequently, DSRM was selected as the guiding research methodology because it provides the scientific rigour, methodological transparency, and practical relevance necessary to produce a validated authentication solution while contributing both theoretical knowledge and practical advancements to secure biometric access control in IIoT environments (Hevner et al., 2004; Peffers et al., 2007).

3.4.2 Justification for Design Science Research Methodology for Biometric Fusion in IIoT

Design science research methodology is well-suited to addressing the complex challenges of biometric fusion in Industrial Internet of Things (IIoT) environments. By following a systematic, iterative approach, design science enables the development and evaluation of robust technological solutions that seamlessly integrate biometric authentication into IIoT systems. The methodology allows for rigorous testing and validation of biometric fusion techniques, ensuring their effectiveness and reliability in real-world industrial settings. Additionally, design science's focus on practical solutions aligns with the need for tangible artefacts that enhance security and efficiency in IIoT applications. Overall, the design science research methodology's systematic and objective nature makes it a suitable framework for advancing biometric fusion technology in IIoT environments, effectively addressing technical challenges and user requirements.

DSRM's data-driven approach, employing qualitative and quantitative analysis methods, enables a holistic evaluation of biometric access control solutions. This allows researchers to assess user feedback and performance metrics, ensuring that the developed systems effectively meet security objectives for the IIoT environments. Moreover, the DSRM iterative and cyclical design process facilitates continuous improvement, accommodating the dynamic nature of IIoT ecosystems. Through iterative testing and refinement based on user feedback, DSRM ensures that biometric access control systems remain robust and resilient against evolving security threats. This makes it a suitable methodology for IIoT security research and development for the following reasons:

- **Systematic and Objective Nature:** DSRM's systematic and objective approach makes it suitable for advancing biometric fusion technology in IIoT environments, effectively addressing technical challenges and user requirements.
- **Holistic Evaluation:** DSRM enables a holistic evaluation of biometric access control solutions, incorporating qualitative and quantitative analysis methods to assess user feedback and performance metrics.
- **Iterative Improvement:** DSRM's iterative and cyclical design process facilitates continuous improvement of biometric access control systems, ensuring their robustness and resilience against evolving security threats.
- **Practical Implementation:** DSRM's focus on creating practical solutions aligns with the need for tangible artefacts that enhance security and efficiency in IIoT applications.

By adopting DSRM, the research aims to develop innovative solutions that advance theoretical knowledge and practical IIoT security, effectively addressing the identified problems and challenges. DSRM is the guiding framework for developing the artefacts in this research, as outlined in the steps shown in Figure 3.1. DSRM, as outlined by Wieringa (2014), facilitates the creation of innovative artefacts that interact with problem contexts to enhance their functionality.

Nunamaker, Chen and Purdin (1991) describe a multi-methodological approach combining theory building, systems development, experimentation and observation. Peffers et al. (2007) drew on earlier design science work, including Nunamaker et al., to propose a six-activity process with explicit demonstration and evaluation. This study used the Peffers process because it is problem-centred and

allows demonstration by simulation, which suited an early-stage artefact whose field testing was not feasible (Hevner et al., 2004; Venable et al., 2016). A Nunamaker-style design would add observation of real workers. That gives stronger ecological validity but needs ethics approval for workers' biometric data, site access and funding (design science projects require significant resources)

3.4.3 Design Science Research Methodology Implementation

DSRM is an iterative process used in information systems and computer science research to develop and validate artefacts that address specific problems or challenges. It involves identifying a problem or opportunity, designing, and creating a solution as an artefact, evaluating its effectiveness, and refining and improving it based on feedback (Mao et al., 2023). DSRM aims to produce innovative solutions that advance knowledge and enable practical problem-solving. The research process begins with identifying the problem statement and its significance in the context of IIoT security. Following this, objectives for the solution are defined to outline what the proposed artefact aims to achieve. The design and development phase involves creating a conceptual model for the biometric access control fusion system, drawing from existing frameworks and adapting them to suit IIoT requirements. This phase also includes feasibility studies to ensure the practicality of the proposed solution.

Once the artefact is designed, it is demonstrated in real-world IIoT environments to validate its effectiveness. Feedback from experts in the field is collected using a structured feedback template. The artefact is iteratively refined based on evaluation results to enhance its usability and efficiency. Finally, the research outcomes are communicated through scholarly publications, contributing to both theoretical knowledge and practical advancements in IIoT security (Mao et al., 2023).

This adaptive design science research methodology combines elements of DSRM tailored to the specific challenges and requirements of developing a biometric access control fusion system for IIoT environments, as detailed in Figures 3.2 and 3.3. Following this structured approach, the research aims to deliver a robust and effective solution to enhance security in industrial settings.

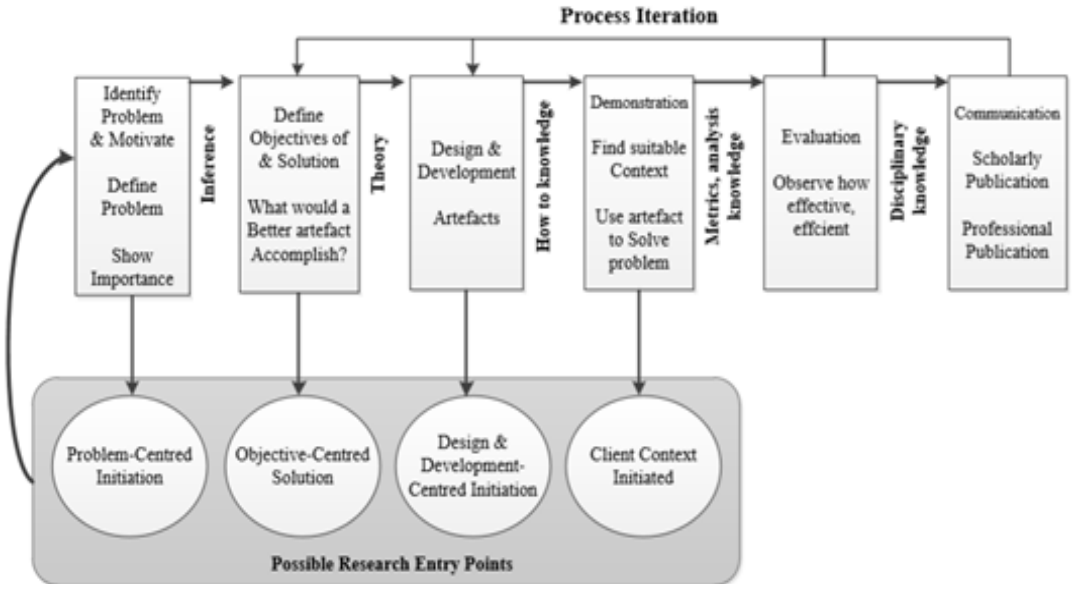


Figure 3.1 DSRM (Peffers et al., 2007, p. 54)

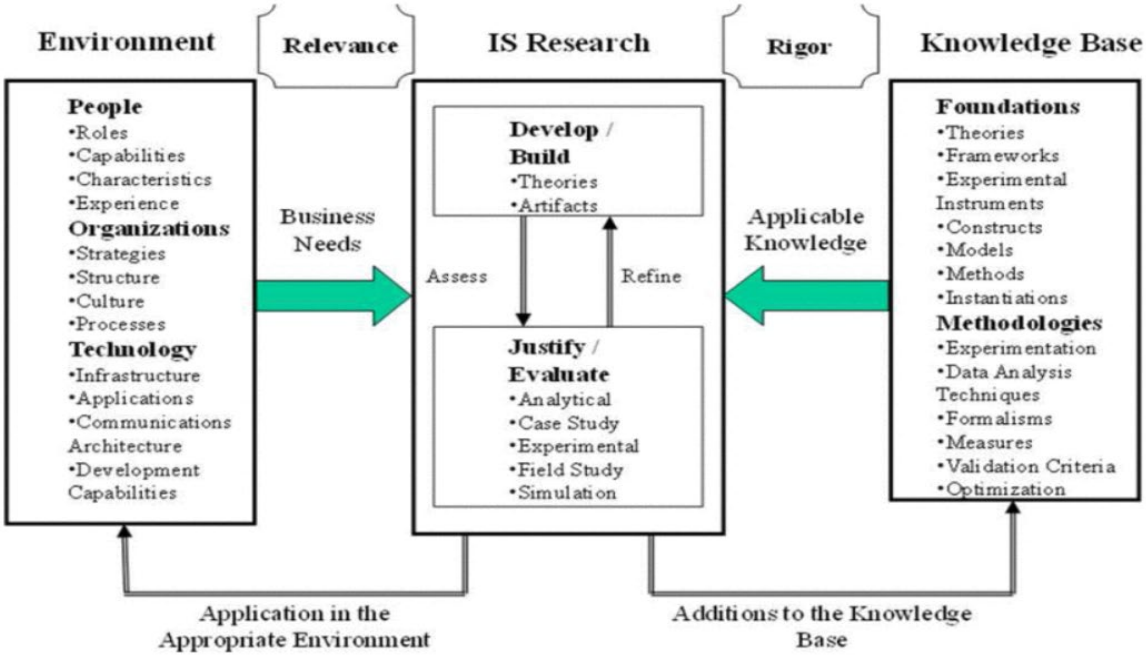


Figure 3.2 Architecture of Scientific Research (Mao et al., 2023, p.110)

Following the design Science principle, the steps below are identified as necessitating the successful implementation of a DSRM. Following the design principles described in Figures 3.1, 3.2, and 3.3, the steps taken are defined in the following subsections and designed in Figures 3.4 and 3.5 to show the proposed activities and frameworks for this research. These subsections transcribe Figures 3.2 and 3.3 for this research.

3.4.3.1 Phase 1: Problem Identification and Definition

Scientific research shows that the knowledge base is the foundation for confirming and identifying problems. Meanwhile, Figure 3.3 aligns with the motivation that the

knowledge base is the first step in problem identification and definition. In this phase, the specific research problem of biometric access control fusion in IIoT is identified and justified (section 2.9) in terms of its importance and relevance. An extensive literature review (Chapter 2) was conducted to explore existing frameworks and methodologies in the field. Research questions and hypotheses are formulated based on the identified gaps and insights from the literature review in section 3.1. The overarching goal is to define a clear problem statement and establish the foundation for subsequent phases of the research.

3.4.3.2 Phase 2: Solution Objectives Definition

Knowledge-based problem identification and definition inform the researcher of the objectives for proposing theories to solve the above-mentioned problems. The objectives of a desirable solution for biometric access control fusion in IIoT will be defined in this phase. A feasibility study was conducted in Section 3.2 to understand the possibilities and constraints of the proposed solution. The focus is on identifying how the proposed solution addresses the gaps and improves existing methods. The feasibility study informs the research motivation and scope, laying the groundwork for the subsequent design and development phase.

3.4.3.3 Phase 3: Artefact 1, 2 and 3 proposed Design and Development

Figures 3.2 and 3.3 show that knowledge from other studies informs a researcher on the methodology best suited to solving the identified problem and aligning with the objectives. Application of this knowledge forms good theories for building artefacts. Building upon the problem identification and solution objectives, a conceptual model for biometric access control fusion in IIoT is proposed and designed for Artefact 1. Artefacts 2 and 3 are proposed and developed. Existing frameworks and best practices will be adapted and integrated to create the artefact. The design process involves defining the components, interactions, and functionality of the proposed framework. Iterative refinement and prototyping are conducted to ensure the artefact aligns with the defined objectives and addresses the identified problem.

3.4.3.4 Phase 4: Artefact Application Demonstration

A refinement of artefacts and theories in the place of testing, which analyses and justifies these artefacts using case studies and simulations. These steps include the

perception of solving societal needs. In this research phase, testing scenarios with second life are designed to evaluate the applicability and effectiveness of Artefact 1 in real-world contexts. Artefact 1 is applied in simulated virtual-reality environments to assess HCI usability and user experience and used to iterate on and design Artefact 2. Expert feedback is solicited to validate the design and identify areas for improvement. The demonstration phase aims to provide initial proof of concept and gather insights for further refinement.

3.4.3.5 Phase 5: Demonstration Effectiveness Evaluation

At this point, an analysis is conducted to assess effectiveness based on societal / business needs. This stage is crucial because it aligns the research objectives with the product. This stage involves refining and iterating on the objectives and the artefact's design, as initially proposed or designed. Data collected from second-life testing scenarios and expert feedback is analysed to evaluate the effectiveness and efficiency of the proposed framework. Qualitative and quantitative analysis techniques will be employed to assess the artefact's impact on addressing the identified problem. Based on the evaluation results, adjustments and refinements enhance the artefact's utility and relevance. The effectiveness evaluation phase aims to validate the proposed solution and inform its iterative improvement.

3.4.3.6 Phase 6: Artefact Results Communication

The communication phase includes results from all other phases, which are examined and fact-checked by industry experts or academicians. This process often leads to a new iteration in objectives, theories, and artefacts before publication. The research outcomes will be communicated through scholarly publications and dissemination to relevant stakeholders. Findings from the evaluation phase and insights gained throughout the research process will be presented to the academic community and industry practitioners. The communication phase aims to advance knowledge in biometric access control in IIoT and facilitate the practical implementation of the proposed framework. This stage involves expert feedback and validation of the research for iteration and publication.

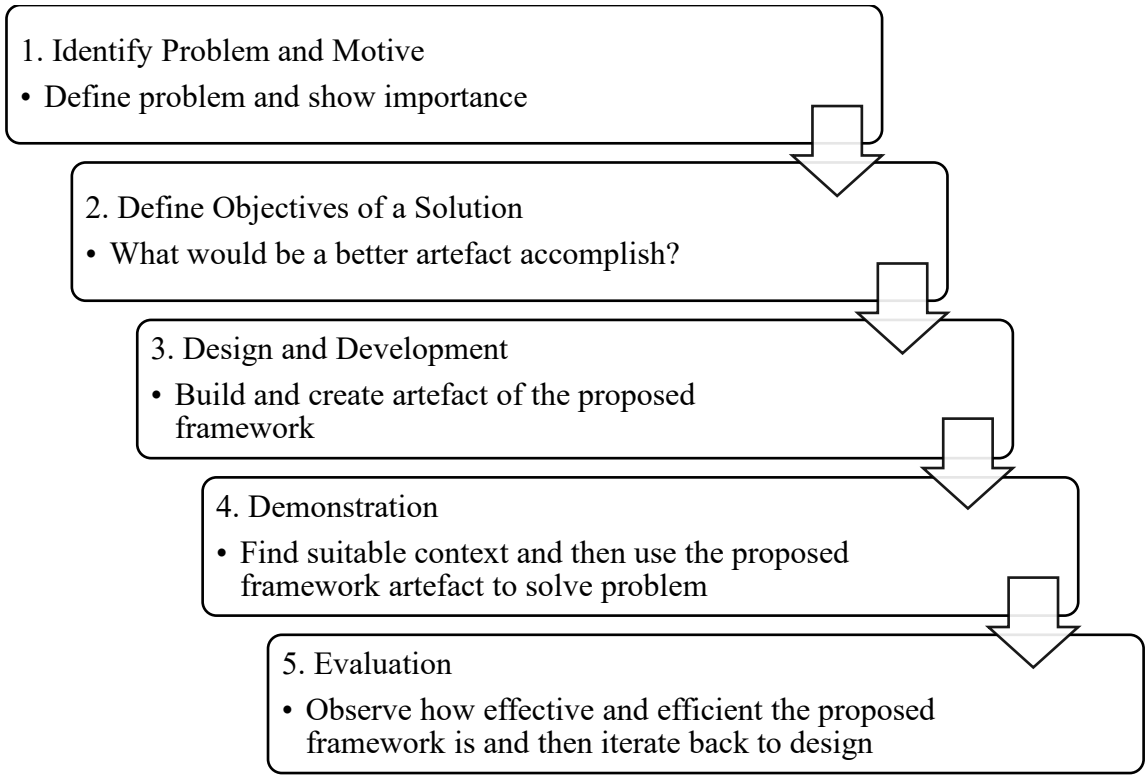


Figure 3.3 Design Science Research Methodology steps are proposed for this research.

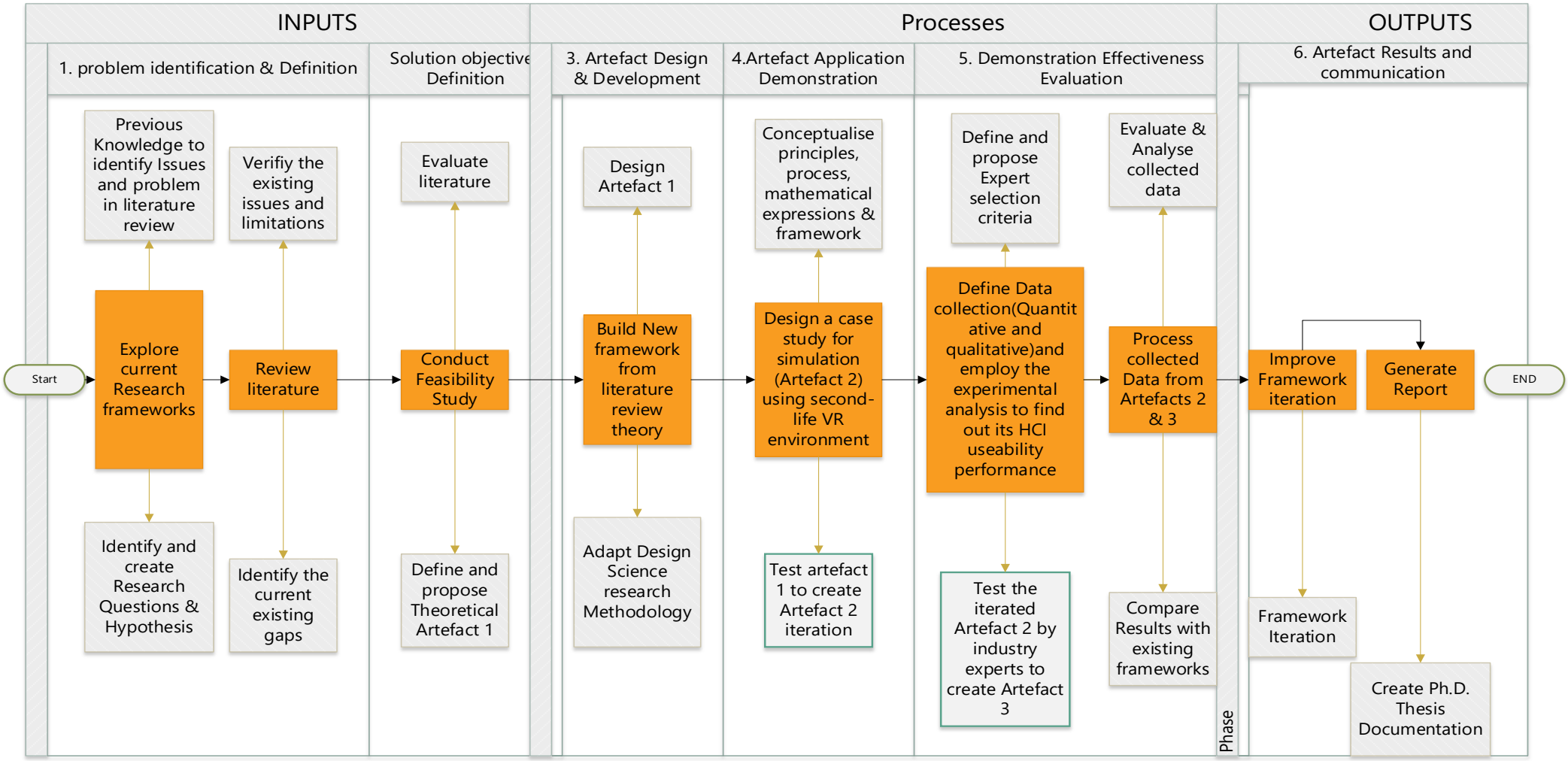


Figure 3.4 Complete the Design Science Research Methodology steps proposed for this research flowchart

Strategies, such as experiments, surveys, case studies, grounded theory, and action research, offer different approaches to investigating phenomena and accessing diverse data sources (Peffers et al., 2012; Haryanti et al., 2022). For this research, a simulation of second-life testing scenarios is chosen to comprehensively evaluate Artefact 1 in a Virtual Reality context, ensuring a holistic investigation (Johannesson & Perjons, 2014; Peffers et al., 2012; Haryanti et al., 2022).

3.5 ARTEFACT 1

This section defines and analyses Artefact 1 in accordance with the proposed structure in Section 2.10. It defines the mode of data collection (literature) and the data analysis derived from Chapter 2 for the Biometric Construct, by infusing deep learning.

3.5.1 Data Collection

The data collection method for Artefact 1, derived from the literature review, primarily involves gathering information from existing studies, research papers, and industry reports on the reliability and effectiveness of biometric recognition systems. By systematically reviewing the literature, relevant data points such as accuracy rates, error rates, usability metrics, and real-world deployment challenges are collected to inform the design and development of a comprehensive biometric access control system tailored to industrial IoT environments. The outcome of this data collection process underscores the dependability and robustness of biometric recognition systems across various modalities, including face, fingerprint, iris, voice, palmprint, ear, and gait recognition. Numerous studies and empirical evidence demonstrate that biometric authentication methods are highly accurate and reliable, particularly when multiple modalities are integrated into a fusion-based approach. This wealth of evidence supports the viability and effectiveness of Artefact 1 in enhancing security and access control within industrial settings. This evidence is found in section 2.5, Biometric deep learning and its performance results.

Moreover, the literature review reveals the potential benefits of fusion-based approaches that leverage multiple biometric traits to improve authentication accuracy, enhance resilience against spoofing attacks, and improve usability in challenging environments. By combining complementary modalities such as face, fingerprint, iris, and voice recognition, Artefact 1 aims to overcome the limitations of individual biometric systems and provide a more robust and dependable access control solution

for industrial IoT environments. In summary, the literature review provides compelling evidence of the dependability and effectiveness of biometric recognition systems, laying the groundwork for developing and implementing Artefact 1. By integrating insights from existing research and industry practices, Artefact 1 is poised to enhance security, usability, and access control capabilities within industrial IoT environments by fusing multiple biometric modalities. `

3.5.2 Artefact 1 Data Analysis

This section analyses data from the Biometric recognition systems and fuses them. The data collected are stated in section 3.5.1 and further investigated. Section 2.10 (Proposed solution) suggests that combining all multimodal biometric traits, such as face, fingerprint, palmprint, iris, gait, ear, and voice, will enhance accuracy and reliability. This section uses the deep learning Convolutional Neural Network (CNN) fusion logic (selected from section 2.6) to combine HCI information from diverse biometric traits for robust identification.

The section proposes an innovative approach that combines CNNs with Multi-Factor Analysis (MFA) to achieve robust multimodal authentication in biometric recognition systems. The proposed method integrates the strengths of CNNs in feature extraction with multi-factor analysis to ensure a secure and reliable authentication selection process. The authentication mechanism is structured into two levels, leveraging both CNNs and MFA to enhance accuracy.

- **Step 1: Independent Trait Processing**

For each biometric trait (face, fingerprint, palmprint, iris, gait, ear, and voice), dedicated HCI information is collected from evaluation.

Therefore, let *Ff, Fp, Fi, Fg, Fe*, and *Fv* represent the feature vectors extracted from the face, fingerprint, iris, gait, ear, and voice CNNs, respectively.

$F_p = CNN_{fingerprint}(Input_{fingerprint})$

$F_f = CNN_{face}(Input_{face})$

$F_i = CNN_{iris}(Input_{iris})$

$F_g = CNN_{gait}(Input_{gait})$

$F_e = CNN_{ear}(Input_{ear})$

$F_v = CNN_{voice}(Input_{voice})$

$F_{pp} = CNN_{palmprint}(Input_{palmprint})$

• **Step 2: Fusion of Extracted Features**

The extracted features from each biometric trait are fused using a weighted combination to create a comprehensive feature vector, as shown in Figure 3.5.

$$F_{fusion} = \alpha_f \cdot F_f + \alpha_p \cdot F_P + \alpha_i \cdot F_i + \alpha_g \cdot F_g + \alpha_e \cdot F_e + \alpha_V \cdot F_V + \alpha_{pp} \cdot F_{Pp}$$

Here $\alpha_f, \alpha_p, \alpha_i, \alpha_g, \alpha_e, \alpha_V, \alpha_{pp}$ are the weights assigned to the features of the face, fingerprint, iris, gait, ear, voice, and palmprint, respectively. Optimisation techniques determine these weights, considering each biometric trait's relative importance and reliability.

• **Step 3: Final Identification**

The fused feature vector F_{fusion} undergoes a final classification layer to determine the individual's identity.

$$Final_{output} = ClassifierF_{fusion}$$

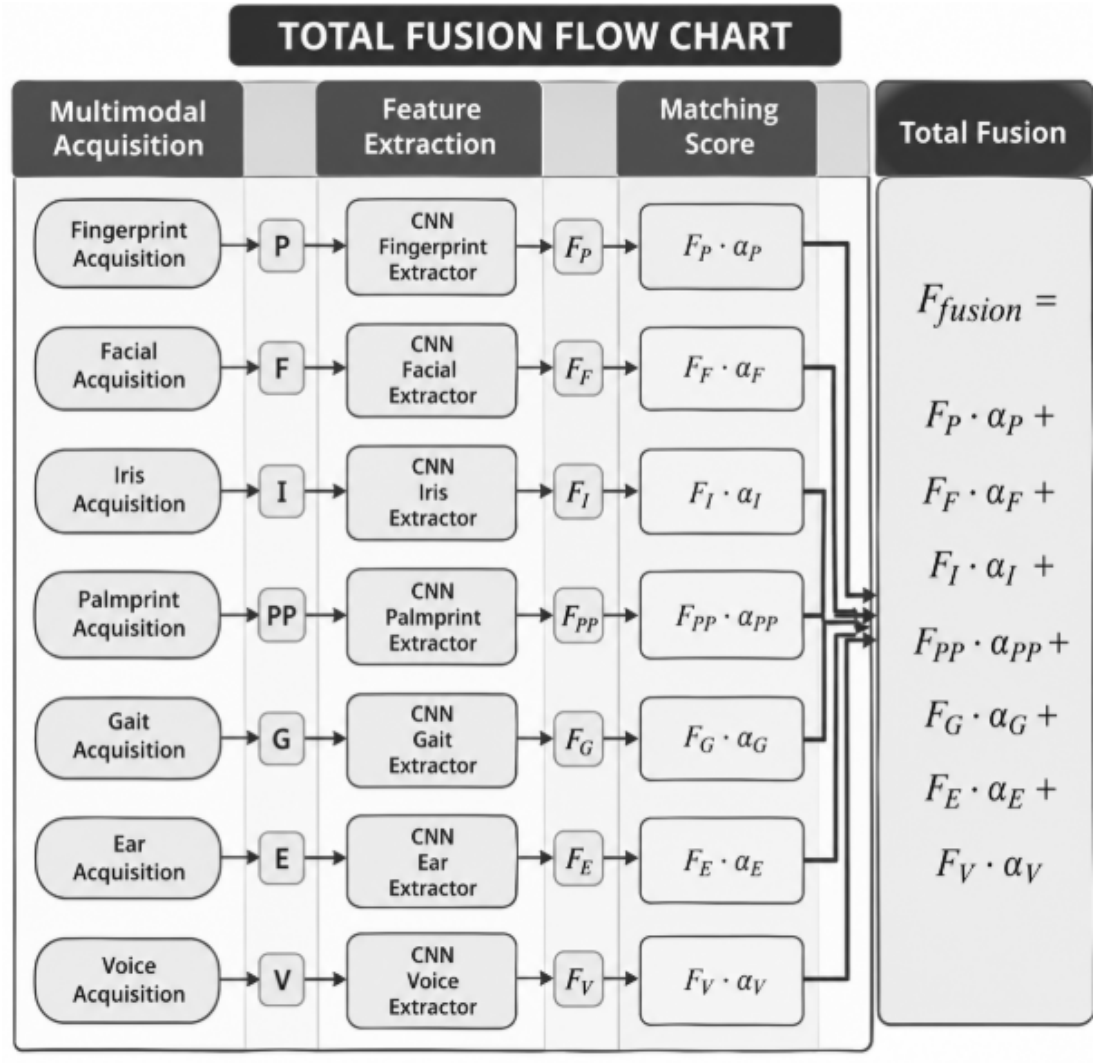


Figure 3.5 Total fusion logic flow chart

The proposed CNN fusion logic provides a systematic, adaptive approach for combining information from multiple biometric traits, thereby enhancing the robustness and reliability of the multimodal biometric recognition system.

3.5.3 Two-Level Authentication Systematic Overview

The authentication process involves two levels, each incorporating CNN-based feature extraction and multi-factor analysis to strengthen identification. The first level of authentication supports worker entry into the industry and clock-in and clock-out at the facility, and the second level authenticates workers when entering a secure room, facility, and so on, where monitoring is necessary. Figures 3.6 and 3.7 show the proposed solution for first and second-level authentication, adapted from sections 2.5.8 and 2.5.9

3.5.3.1 Proposed CNN-Based Multi-Factor Analysis Logic

Where n is the number of authentication attempts for the first factor, and x is the number of successful attempts on n trials.

$$P(Success_n) = \ P(X = x) = \binom{n}{x} * P^x * (1 - P)^{n-x}$$

Where:

- $\binom{n}{x}$ is the binomial coefficient, representing the number of ways to choose x successes from n trials.
- p is the probability of success on a single trial

In this context, P(success) is the probability of x successful authentication attempts out of n trials for the first factor. Denoting p1 as the probability of success for the first factor. Note that the probability of successful authentication for each Biometric factor as P({success}) and the probability of failure as P({failure}. The overall probability of successful authentication with multifactor analysis is the product of the individual probabilities of success. Therefore, for N factors, the expression would be:

- $P(overall\ success) = P\left(Success_f\right) * \ P\left(Success_p\right) * \ldots * \ P(Success_N)$

  Conversely, the probability of overall failure (i.e., unsuccessful authentication) is given by:
- $P(Overall\ failure) = 1 - P(overall\ success)$

The success of each factor is assumed to be independent of the others. A multifactor authentication system aims to make P({overall failure}) sufficiently low to enhance security. The mathematical expression above represents the multiplication of the success probabilities for each authentication factor, illustrating the combined effect of multiple factors in the authentication process.

3.5.3.2 Authentication at First Level

At the first level, CNN-based feature extraction is followed by multi-factor analysis to authenticate based on at least two biometric traits successfully identified. Where M.A. = multifactor analysis and Ft = features. It is further explained in Figure 3.6. This is derived from the formulae:

$$\mathrm{AUTH}_{f1} = \begin{cases} 1 & \text{if CNN_Fts(Id. Biometrics)}\ \ \mathrm{M.A(CNN_Ft)} \geq 2 \\ 0 & \text{otherwise} \end{cases}$$

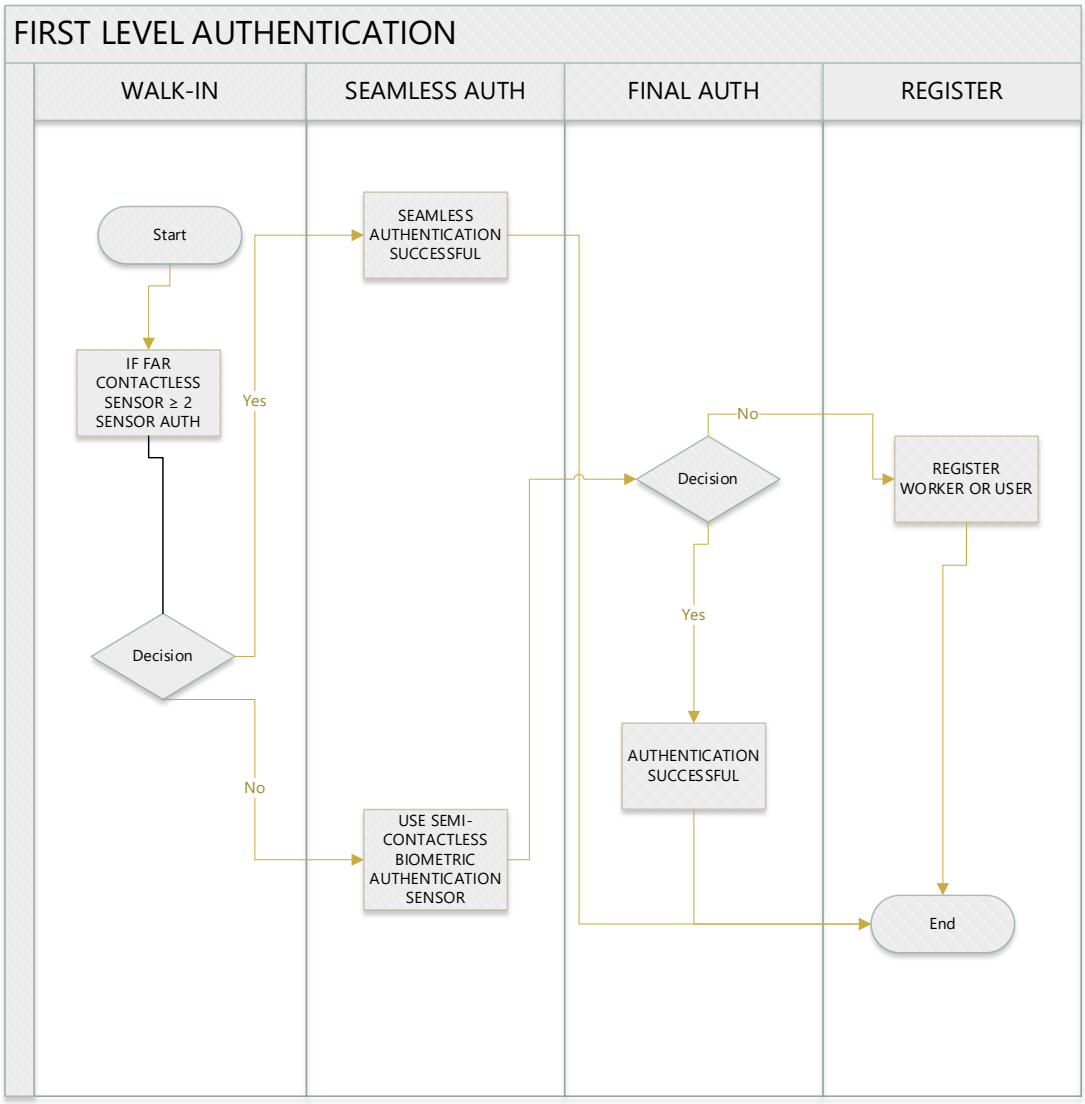


Figure 3.6 First Level Authentication Idea

3.5.3.3 Authentication at Second Level

The second level incorporates deeper CNN-based feature extraction and multi-factor analysis to ensure authentication with at least three identified biometric traits, including one from iris, palm print, fingerprint, and face. Figure 3.7 shows the proposed idea for second-level secure room authentication. This is derived from the formulae:

$$\mathrm{AUTH}_{f2} = \begin{cases} 1 & \text{if CNN_Fts(Id. Biometrics)} \;\; \text{M. A(CNN_Ft)} \geq \;\; 3 \text{ and Fi} \parallel \text{Fp} \parallel \text{Ff} \\ 0 & \text{otherwise} \end{cases}$$

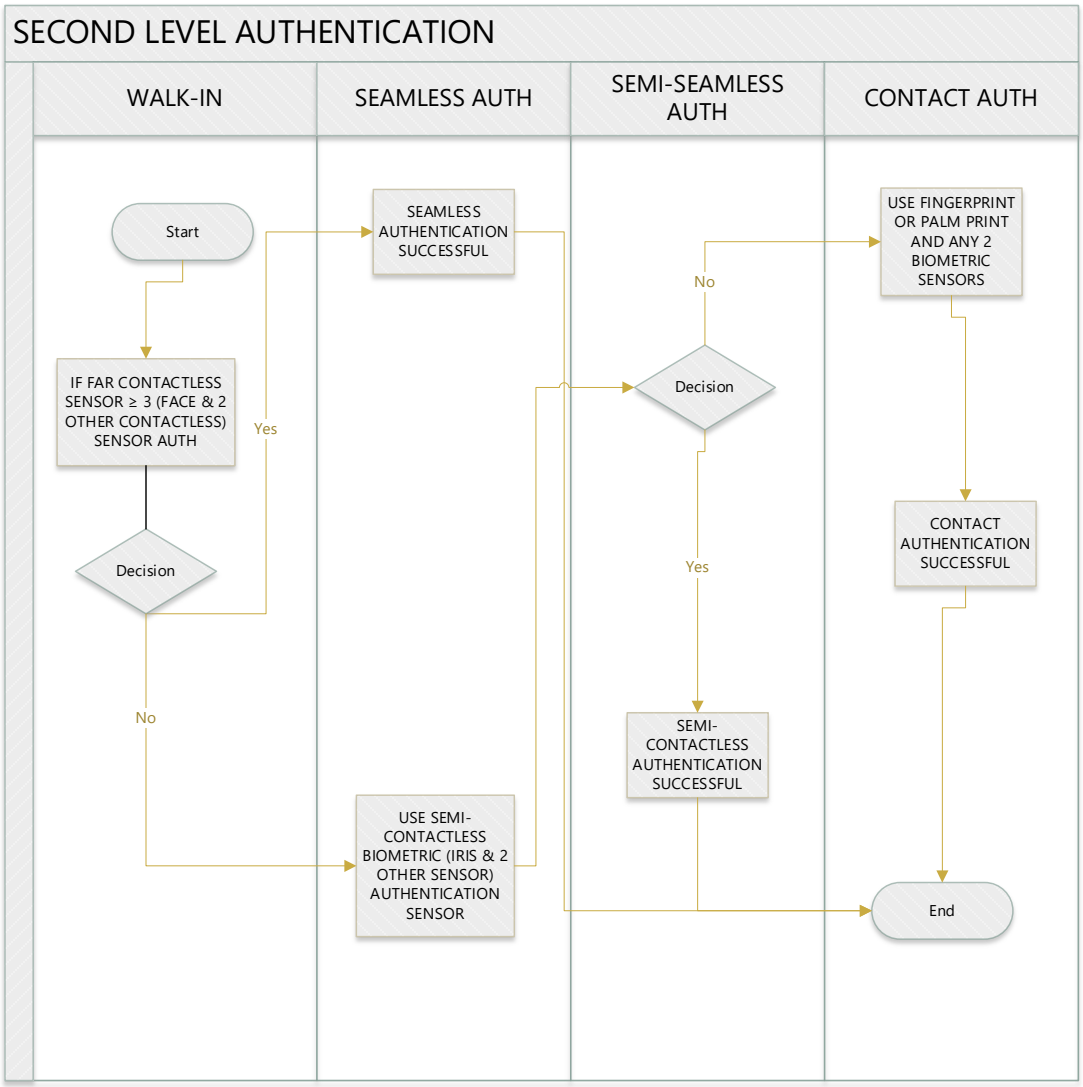


Figure 3.7 Second-Level Authentication Idea

This novel integration of CNNs and multi-factor analysis establishes a robust framework for multi-modal authentication, combining deep learning capabilities with the analytical strength of multi-factor methods from the proposed artefact 1 section 2.10 and 3.5.2.

3.6 ARTEFACT 2

Artefact 2 is the tested concept for artefact 1. This section proposes the data collection, analysis and experimental design for the test. The test is to be carried out in a controlled virtual environment.

3.6.1 Data Collection Strategies for Second Life

The data collection strategies for the Biometric Access Control in IIoT simulation using Second Life from table 2.17, employing a Design Science Research methodology, are outlined as Biometric Simulated Data. Biometric simulated data are Data from Second Life Virtual Reality simulation sessions and focuses on Total Biometric Trait Fusion for Enhanced Security and seamless Contactless Biometric Trait Acquisition (Proxy trait). This data will inform the iterative improvement of the authentication systems, such as which biometric traits perform well under different constraints.

The Data collection method involves a creative exploration guided by the robust second-life social Virtual Reality to design and inform this process. These mechanisms serve as the core of this research, embodying the essence of secure, user-friendly access control in the context of the Second Life case study. As highlighted in section 2.7, the Second Life platform emerges as a comprehensive and reliable virtual space for simulating Artefact 1. This section presents a well-designed, strategic blueprint that illustrates how implementing Artefact 1's case study in the virtual environment will yield a valuable socio-technological research outcome. The objectives and the test execution for this test simulation are shown in Tables 3.6 and 3.7. Section 3.6.2 shows the experimental design procedure for this test simulation using second-life VR, and Section 3.6.3 is the analysis/decision support system for this artefact.

Table 3.6 shows the Artefact 1 testing objectives.

	Objectives	**Description**
1	Performance Evaluation	Assess the efficiency of the system's interaction for access control methods that grant or deny access to Second Life users.

2	Biometric access system	Design a well-suited, user-friendly embedded system to suit artefact 1 in the Second-Life VR environment.

Table 3.7 shows the test execution.

S/N	Staging	Description
1	Pilot Testing	Conduct a pilot round of testing to identify any issues or refinements needed in the testing scenarios and data collection methods.
2	Testing Iterations	Execute multiple testing iterations to gather comprehensive data.
4	Data Analysis	Analyse the collected data to evaluate performance for this Biometric access control system.

3.6.2 Experimental Design

This section outlines the experimental steps for testing Artefact 1, as shown in Tables 3.6 and 3.7.

3.6.2.1 Introduction

This section outlines the step-by-step collection and rules for the experimental process in Second Life. Below are some fundamental rules guiding this experiment.

- **Avatar control & data source**: all six avatars (3 male, 3 female) are controlled by a single account; the measured data are the avatars' rendered features and resulting classifier outputs, **not** human physiological measurements. This keeps the experiment strictly a virtual-agent study and aligns with the Artefact-2 simulation scope.
- **No deep learning**: In this experiment, all per-modality processing will use classical feature extraction and matching, not deep learning outputs. Deterministic scoring pipelines and calibrated distance thresholds are used. Also, the assumption that this feature is the avatar ID, as the literature shows that deep learning improves the accuracy of a biometric system to almost perfection.

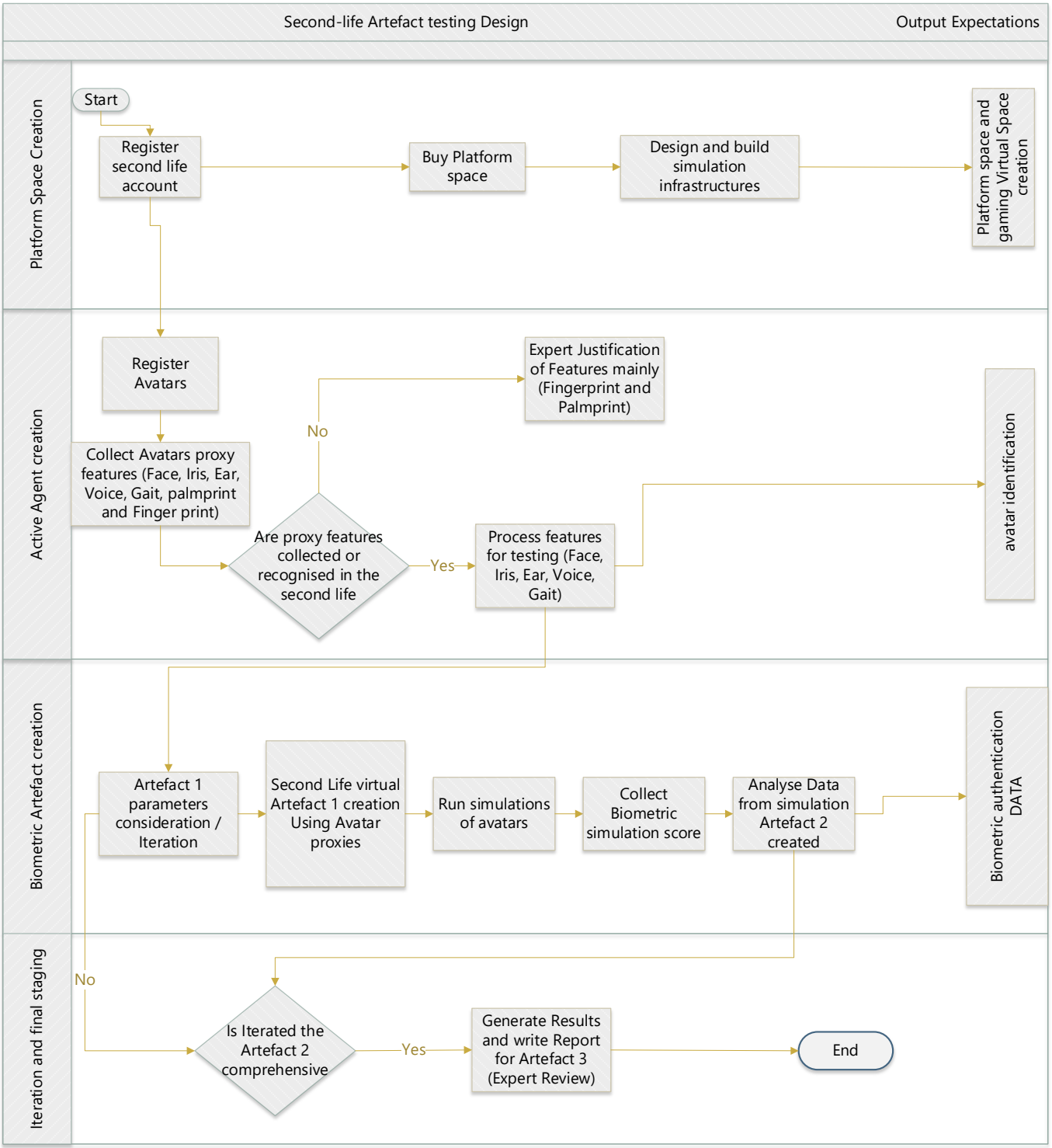


Figure 3.8 Artefact 1 Tested in for the improved Artefact 2

3.6.2.2 Objectives & high-level design

The primary aim of this experiment is to measure the authentication accuracy of different biometric traits using avatar proxies under various work-environmental constraints for the Artefact-2 multimodal fusion system in Second Life, as shown in

Figure 3.8. The study focuses on contactless modalities such as face, gait, voice, and ear, which are available as avatar proxies on the platform.

3.6.2.3 Design summary (factors, cells, trials)

The avatar factor is treated as a fixed set of templates: six avatars (Male A, Male B, Male C, Female A, Female B, and Female C), all controlled through the same account. Within each avatar, constraints are applied in different combinations ("cells") to reproduce a range of realistic operating conditions, from mild disruption through to high-stress scenarios.

Five constraints are used in the design: **MASK** (facial occlusion), **HELMET** (head and ear obstruction), **HEAVYLOAD** (gait and posture disturbance), **LOWLIGHT** (reduced visual acquisition quality), and **FASTMOVE** (motion-induced instability). The combinations are grouped by the number of active constraints, as shown in the table below.

Table 3.8 Simulation constraint count

Constraint Level	**Description**	**Number of Combinations**
C0	No active constraints	1
C1	Single constraint active	5
C2	Two simultaneous constraints	10
C3	Three simultaneous constraints	10
C4	Four simultaneous constraints	5
C5	All five constraints are actively applied	1
Total		32

3.6.2.4 Constraint Combination Logic

Constraint combinations are deliberately accumulated progressively to simulate increasing industrial stress. The early configurations isolate single effects, such as *MASK only*, *HELMET only*, or *LOWLIGHT only*, so each constraint's individual impact can be observed clearly. Mid-level configurations then test compound interference by pairing constraints that are likely to interact, for example, *MASK + LOWLIGHT*, *HELMET + HEAVYLOAD*, or *FASTMOVE + HEAVYLOAD*.

Finally, high-level configurations represent extreme operating environments by stacking multiple constraints, such as *MASK* + *HELMET* + *LOWLIGHT* + *HEAVYLOAD*, and the full combination *MASK* + *HELMET* + *HEAVYLOAD* + *LOWLIGHT* + *FASTMOVE*.

3.6.2.5 Per-trial procedure (operator workflow)

This is the basic set of operations for simulating avatar authentication in Second Life.

- **Load/equip avatar**: choose avatar skin (one of the six), attach the specified headgear, mask and load object for the assigned cell. Ensure any animation overrides (heavy load gait) are enabled.
- **Spawn to capture node**: position the avatar at the capture waypoint (pre-defined position).
- **Trigger capture**: click on the biometric authentication curated machine with LSL node scripts to perform captures and send authentication data to the log.
- **Decision & log**: the gate opens or rejects the authentication, returning an authentication outcome (Accept / Reject). All raw inputs, extracted features, scores, latency and decisions are securely logged.

3.6.2.6 Validation, metrics and analysis

Second Life (SL) is a virtual world and not a biometric sensor ecosystem; only some real-world biometrics are approximated. Several Biometrics cannot be replicated because SL does not expose raw biological signals. However, SL enables the extraction of behavioural, kinematic, and avatar parameters that serve as functional proxies.

This is appropriate for Industrial IoT simulation because the goal is to model authentication workflow, timing, usability, and fusion logic, not to perfectly recreate bio-sensing. Below are the workable proxies to be used in this experiment.

- **Gait pattern (walk timing and step distance):** This metric is derived from continuous sampling of the avatar's position at 0.2-second intervals.
- **Avatar physical dimensions:** These include height, body thickness, hand size, head size, and related parameters.
- **Skin-tint vector (RGB tone):** This is extracted through scripted object detection rather than by reading the texture bitmap itself.

- **Attachment configuration:** This captures whether the avatar is wearing items such as a mask, hat, heavy-load backpack, body armour, and similar attachments.
- All these measures act as rule-based differentiators, so no machine learning is required.

3.6.2.7 Biometrics Replicated as Functional Proxies in the Second Life

The following are the replication and how their proxies are obtained.

- **GAIT — REPLICABLE**

  Capturing avatar gait is possible because Second Life exposes position in 3D space, velocity, step distance, animation speed, and turning rate. Capturing avatar gait is possible because Second Life exposes position in 3D space, velocity, step distance, animation speed, and turning rate. These allow the construction of a gait signature, like human gait biometrics, in behavioural terms, though not in biological detail.

  Conclusion: Gait is a fully achievable behavioural biometric in this environment.

- **FACE — PARTIALLY REPLICABLE**

  In Second Life, facial information cannot be extracted at a biological level, including pixel-level facial features, texture data, and 3D mesh vertex data of the avatar's face (which is blocked for security reasons). At a biological level, facial data cannot be extracted in Second Life, including pixel-level facial features, texture data, and 3D mesh vertex data of the avatar's face (which is blocked for security reasons). Even so, a limited appearance-based signature can be formed using a skin-tint (RGB) vector, head size, face-light settings, and the presence of facial attachments, such as masks or glasses. These allow a **weak face signature**, *not* a true facial biometric.

  Conclusion: Face recognition is not biologically replicable in Second Life, but a proxy face-appearance signature is achievable.

- **IRIS — NOT REPLICABLE**

  Real iris recognition depends on textural micro-patterns, fine-grain radial structure, and high-resolution imaging, none of which are available in Second

Life. Second Life **blocks all texture extraction**, and scripts cannot read the iris pattern.

Conclusion: Iris recognition is not possible at any meaningful level in Second Life.

- **FINGERPRINT — NOT REPLICABLE**

  In practice, fingerprint recognition requires ridge reconstruction, minutiae extraction, and local binary pattern mapping. SL exposes no finger texture, no finger mesh, and no hand detail interaction.

  Conclusion: Fingerprint recognition is not possible because Second Life exposes no finger texture, no finger mesh, and no high-detail hand interaction.

- **PALMPRINT — NOT REPLICABLE**

  Same barriers as fingerprints. SL does not expose palm textures or high-resolution palm surfaces.

  Conclusion: Palmprint recognition is not possible, for the same reasons as fingerprints, because Second Life does not expose palm textures or high-resolution palm surfaces.

- **EAR — PARTIALLY REPLICABLE**

  Ear biometrics face constraints similar to face recognition in Second Life. As with the face, the ear mesh cannot be extracted; however, it is possible to detect ear-related attachments, such as earrings, headphones, or hair covering the ear. Thus, an appearance-based ear profile is simulated, but not the biological geometry.

  Conclusion: Ear biometrics are only weakly replicable through appearance proxies.

- **VOICE — PARTIALLY REPLICABLE**

  Where the setup supports it, voice data can be treated as an audio signal and analysed for features such as pitch and formant structure. From a signal perspective, voice may be captured as a waveform, along with features such as pitch and formant structure, where supported by the setup. Separately, the system can also track behavioural voice activity, including whether the avatar uses voice, the duration of speaking events, and how frequently voice is activated. In addition, the system can detect behavioural voice activity, including whether the avatar uses voice, the duration of speaking events, and

the frequency of voice activation. This becomes a **binary behavioural indicator**, not biometric.

Conclusion: Voice recognition is not replicable as a true biometric in Second Life, but voice-activity patterns can still support behavioural analysis. And for privacy reasons, voices cannot be used, recorded, or analysed.

- **BEHAVIOURAL BIOMETRICS — FULLY REPLICABLE**

  This is where Second Life performs best: behavioural signals such as reaction time, gesture frequency, movement smoothness, direction-change rate, object-interaction speed, login repetition patterns, authentication decision time, and (to a limited extent) camera-movement behaviour can be observed through events and timing.

3.6.3 Map To The 8 Biometrics (Reference to System Design)

This subsection links the selected biometric trait to the second-life proxy metric to show what can be extracted from second life and what cannot. Finally, it shows how logic can be used to replace physiological traits in Second Life, as seen in Table 3.9.

Table 3.9 showing which SL-measurable metrics correspond to which biometric trait.

Human Biometric	**Second Life Proxy Metric**	**Match Quality**	**Explanation**
Gait	Step length variation, cadence, positional sampling	Strong	Behaviours correspond directly.
Face	Avatar head size, skin tint, and facial attachments	Weak	No texture/mesh access
Iris	*None*	Impossible	SL blocks texture access
Fingerprint	*None*	Impossible	No hand detail extraction
Palmprint	*None*	Impossible	Same limitations
Ear	Attachment detection	Weak	No ear-mesh or geometry
Voice	Voice-activity patterns	Weak	No waveform or pitch capture
Behavioural	Reaction time, gesture tempo, movement patterns	Strong	Fully measurable.

These results come from a simulation with scripted degradation. They test fusion logic and are not error rates for real workers. the first plan, using other Second Life users' avatars, was abandoned because the platform restricts avatar-level data for privacy reasons.

A dummy biometric has three functions

- **A fixed avatar-specific value** (acting as a biometric template)
- **A matching score** (your code decides to pass/fail or match %)
- **A sensor-like workflow** (scan → compare → output → log time/results)
- This maintains the *structure* of biometric authentication without requiring the biometric itself.

Metrics to be collected (per trial)

- Per-modality scores s_i(face, gait, voice, ear, iris)
- Fusion score $F$and decision outcome
- Latency (capture → decision)
- Escalation occurrences (how often a third modality was needed)
- Deep learning assumption, which is AvatarID

3.6.3.1 Limitations & notes (transparent)

These are the identified limitations for this study's experimental phase, and they are as follows;

- **Single-operator account control:** Using one operator reduces human-to-human variability, but it can introduce pilot-specific gait or voice style. This is a deliberate design choice because the artefact is intended to test avatar rendering and accessory effects rather than human physiological variability.
- **No deep learning:** Because the study relies on classical processing, per-modality discrimination is expected to be weaker than CNN-based systems. As a result, score distributions may overlap more, thresholds will need careful tuning, and expert HCI ratings can help indicate which modalities to prioritise under occlusion.

3.6.3.2 Deliverables from the experiment

The experiment will produce a full trial log (196 trials) including raw captures, per modality scores, and fusion outputs. It will also provide a calibration report

documenting adjusted rule weights and thresholds (before and after the pilot), a short technical appendix containing Lindel Scripting Language code skeletons and classical processing pseudocode, and a recommendation sheet that identifies which constraints cause systematic failures and proposes Artefact-2 rule changes (for example, requiring voice and ear as mandatory secondary checks when a full mask and helmet are both present).

3.6.4 Data Analysis

The analysis is organised into four layers, aligned with common Decision Support System evaluation practice, so the results can be interpreted from both a technical and operational perspective.

- **Per-Modality Performance Analysis**

  For each modality, similarity scores were compared across the different constraint conditions to see where performance shifts. Because the sample is modest and the score distributions are not well modelled by a normal curve, results are summarised using medians and interquartile ranges and tested using non-parametric methods (Wilcoxon and Kruskal–Wallis). This makes it easier to pinpoint which modalities are most affected by occlusion and by load-related changes.

- **Fusion Performance Evaluation**

  Fusion was computed using a weighted-sum rule:

  $$F = \sum_{i=1}^{n} w_i \, s_i$$

  where s_i represents modality similarity scores and w_i represents reliability weights derived from contactless applicability and performance scales. Fusion score distributions were examined across constraint levels. False Acceptance Rate (FAR), False Rejection Rate (FRR), and approximate Equal Error Rate (EER) were estimated. Escalation frequency and decision boundary stability were analysed to assess threshold robustness.

- **Decision Logic Assessment**

  Decision outcomes (Accept, Reject) were analysed by constraint cell and avatar. Escalation rates were used as an indicator of system uncertainty under operational stress. Latency distributions were evaluated to assess the

efficiency impacts of additional modality requests. This layer directly assesses the DSS's ability to support secure, efficient access decisions across varying contextual conditions. A correlation analysis is performed between fusion scores and perceived satisfaction to examine the alignment between technical performance and human judgment.

- **Risk-Adaptive Threshold Simulation**

  To test adaptability, the simulated three risk contexts were adjusted by changing the decision policy: a low-risk setting with the threshold reduced by 5%, a baseline setting with the default threshold, and a high-risk setting with the threshold increased by 10% and a requirement to use three modalities.

These policy shifts change FAR, FRR, and escalation behaviour, which helps indicate whether dynamic enforcement is realistic for a future iteration of the artefact.

3.6.5 Mathematical summary/formulae (compact)

This subsection explains all terms and derivations of the data analysis formulae to be used, and their use-case examples.

3.6.5.1 reliability score

This score is used to calculate the reliability of the biometric authentication module. It uses two data sources: a contactless usability screen that differs by biometric trait (Face and voice, which are highly contactless, and finger, which is contact-based and less valuable; note this system prioritises contactless due to the nature of industry workers), and a performance capability where the system also leans towards systems with a higher performance score. (also 'score of biometric modality i') these examples are coined from the contactless and performance scale used from 2.15 and 2.16

$$R_i = 0.45 \cdot \frac{\text{contact}_i}{5} + 0.55 \cdot \frac{\text{perf}_i}{5}$$

For example, Face has a contactless score of 5 and a performance score of 4.5.

$$R_{face} = 0.45 \cdot \frac{5}{5} + 0.55 \cdot \frac{4.5}{5}$$

$$R_{face} = 0.45(1) + 0.55(0.9)$$

$$R_{face} = 0.45 + 0.495$$

$$R_{face} = 0.945$$

Face reliability score = 0.945

Table 3.10 reliability score definition

Symbol	Meaning
R_i	Reliability score of biometric modalities i
$contact_i$	Contactless usability rating of a biometric trait i
$perf_i$	Performance rating of a biometric trait i
5	The maximum possible rating value used for normalisation
0.45	Weight assigned to contactless usability
0.55	Weight assigned to biometric performance capability
0.45 and 0.55	represent the relative importance assigned to usability and biometric performance, respectively. They make up 1, which is the highest factor

3.6.5.2 Normalised weight

This formula computes and calibrates the derived weight based on the biometric traits used, while the unused trait is degraded. This enables adaptive weight computation, where the reliability score determines the proportional weighting for multimodal fusion.

$$w_i = \frac{R_i}{\sum_j \quad R_j}$$

For example, if Face reliability = 0.94, Voice reliability = 0.70 and Gait reliability = 0.60 then the Total reliability:

$$0.94 + 0.70 + 0.60 = 2.24$$

Calculating face weight:

$$w_{face} = \frac{0.94}{2.24}$$

$$w_{face} = 0.42$$

That means Face contributes 42% to authentication fusion.

Table 3.11 Normalised weight term definition

Symbol	Meaning
w_i	Adaptive weight assigned to biometric modality i
R_i	Reliability score of modalities i
$\sum_j R_j$	Sum of reliability scores across all biometric modalities

3.6.5.3 Fusion score

This is the final fusion biometric modality, comprising the biometric modality confidence scores and their adaptive contextual weights, which together equal the final authentication confidence value.

For example,

Table 3.12 Example of Fusion score table

Biometric	Weight w_i	Score s_i
Face	0.42	0.90
Voice	0.31	0.75
Gait	0.27	0.80

$$F = (0.42 \times 0.90) + (0.31 \times 0.75) + (0.27 \times 0.80),$$
$$F = 0.378 + 0.2325 + 0.216$$
$$F = 0.8265$$

Final fusion score = 0.83

$$F = \sum_{i \in M} w_i \cdot s_i$$

Table 3.13 Fusion score Term Definition

Symbol	Meaning
F	Final fusion authentication score
M	set of biometric modalities used
w_i	Adaptive weight assigned to biometric modality i
s_i	Matching score/confidence score of biometric modalities i

3.6.6 Artefact 2 Decision support system

A decision support system is a logic system that directs how Authentication is achieved from Start to end. The decision logic system for the experiment proposed or simulated in Second Life is activated when Avatars approach the Gate/Biometric Machine system. The system is triggered when the machine is clicked, indicating that an avatar has approached the Gate, as shown in Figure 3.9. The recognition machines start gathering vital information based on the traits that are free from constraints. The

fusion score is aggregated from different biometric scores and is weighted according to the 0.85 threshold. If F is greater than the threshold score, the gate opens; if not, it's escalated or rejected if it is 0.65.

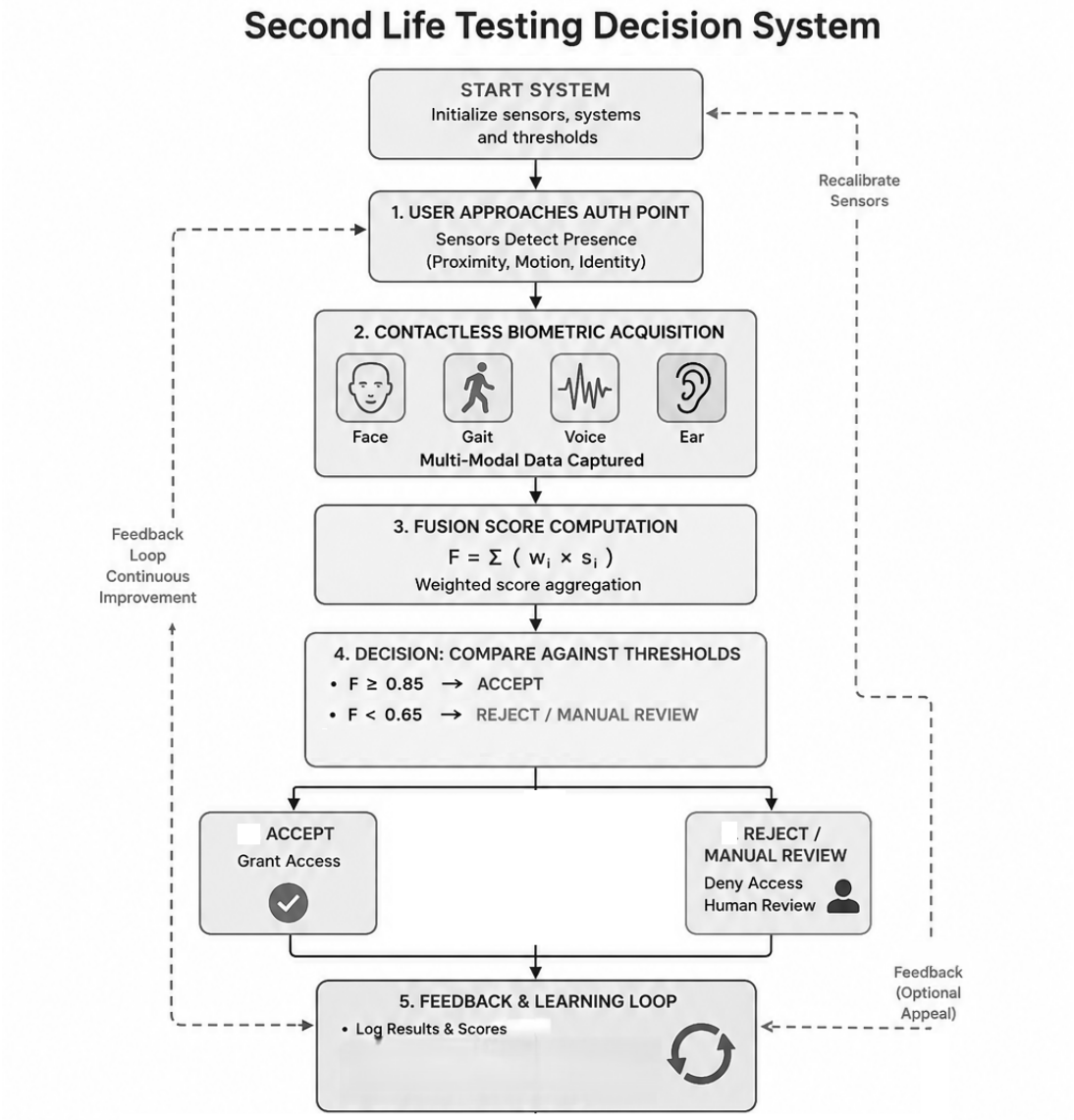


Figure 3.9 Decision support system for Second Life Artefact2

3.7 ARTEFACT 3

Artefact 3 is an iterated or improved Artefact 2. After Artefact 1 is tested, its deliverables are used to design Artefact 2. Artefact 2 is improved and transitioned, at which point its improved version is sent for Expert review, and its feedback is used to improve and create a final version of Artefact 3.

3.7.1 Data Collection Processes

For the expert feedback process in the context of Biometric Access Control in IIoT, a structured approach will be employed to gather opinions and data from a selected group of experts. The purpose is to obtain reliable feedback on the presented artefact 2 to help address the formulated research questions. This feedback will be crucial for refining and improving the artefact to meet the needs of stakeholders in the IIoT sector. The expert feedback process will involve the following main steps.

- **Designing the Feedback Template:** A feedback template will collect quantitative and qualitative information from the selected group of experts. The template will include a combination of closed and open starters to gather objective opinions and allow descriptive responses.
- **Explaining the Purpose:** When sharing the template with the selected group of experts, a cover letter will be attached to explain the research's purpose. The respondents need to understand the context in which the questions are being posed, providing clarity on the goals and objectives of the study.
- **Collecting Expert Opinions:** The feedback template will be distributed to the experts, who will provide their opinions on various aspects of the Biometric Access Control artefacts 1 and 2 in the IIoT sector. Closed starters will prompt objective responses, while open starters will allow respondents to communicate descriptively in their own words.
- **Analysis and Iteration:** The expert feedback will be analysed in NVivo to identify common themes, insights, and areas for improvement. This analysis will inform iterations and refinements to the Biometric Access Control artefact, ensuring it meets the needs and expectations of stakeholders in the IIoT sector.

By following this expert feedback process shown in Figure 3.16, valuable insights will be gained to enhance the effectiveness and usability of Biometric Access Control solutions in IIoT environments.

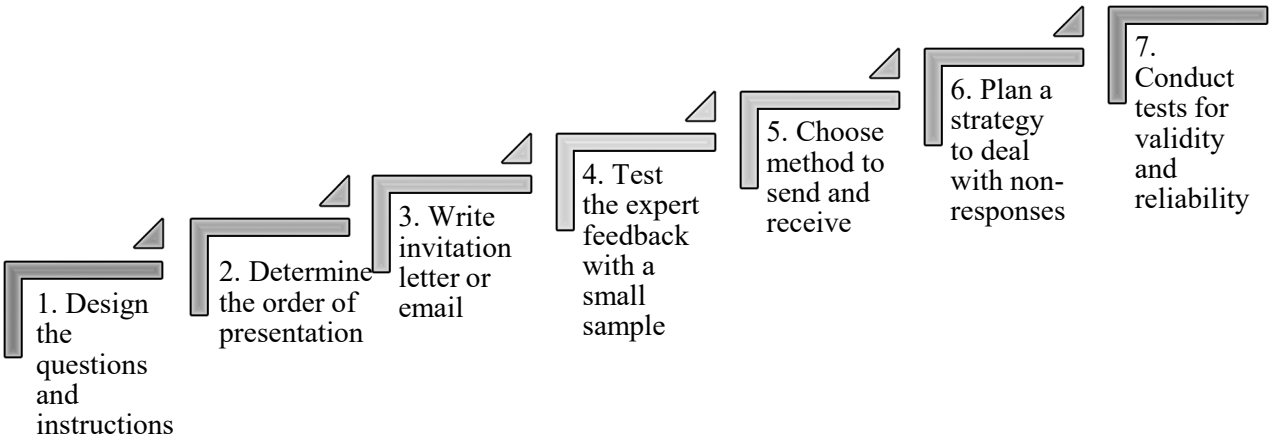


Figure 3.10 Summarises the main steps involved in designing an expert feedback process.

3.7.2 Data Analysis Process Steps for Expert Feedback.

The NVivo tool will be utilised to aggregate and analyse expert feedback collected during the research process. The following outlines the data collection and analysis process adapted for this specific study:

- **Selection of Experts:** Interview experts will be selected based on their depth of knowledge and relevance to the research questions. A set of criteria will be defined to guide the selection process, ensuring that participants possess valuable insights related to Biometric Access Control in IIoT environments. Below are the criteria for expert selection;
    - IoT or IIoT experienced for at least five years
    - IT security personnel for at least five years
    - Heavy construction security officer for at least 10 years
    - IIoT, IOT, IT security, Cybersecurity researcher or professor

  These criteria are for expert roles that have an in-depth understanding or expertise in the field of study in this research, and they will have sufficient experience to contribute to and fine-tune the end product of this research.
- **AUTEC Code of Conduct**: the code of conduct provided by AUT in section 6.7 Ethics, which states that "you do not need to apply for formal ethics approval if your PhD research falls into specific exempted categories - **Single Professional Interviews**: A single, one-off interview of limited scope with professional experts in the area of their expertise." Has made it possible to

obtain feedback from experts with their names kept as aliases or not mentioned for privacy purposes.

- **Initial Contact:** A list of potential experts will be compiled, and initial contact will be established with them. Willing experts will be provided with a copy of the research framework, an introduction to the study, and a set of starters to guide their responses. These experts will be given the study blueprint, and a set of questions will be presented for them to address or provide feedback on. These questions are as follows;
    - Is this solution doable?
    - Is it comprehensive?
    - Other comments?
- **Data Collection:** Transcripts of the expert feedback will be collected and imported into NVivo for analysis. The transcripts will be clustered into codes based on frequent words, cases, or a combination of these to gather evidence relevant to the research questions.
- **Code Development and Theme Formation:** From the coded transcripts, themes will be developed, consisting of multiple codes, and supported by relevant textual data. Sub-categories will be grouped to create linked memos, facilitating the analysis of the transcripts.
- **Query Function:** The query function in NVivo will be utilised to gather attitudes based on demographic attributes or explore connections between different themes. This will help identify patterns and relationships within the data.
- **Thematic Analysis:** Thematic analysis will be employed as the primary analysis method to identify, analyse, and report themes emerging from the collected data. This approach allows for a comprehensive examination of the expert feedback, focusing on key patterns and insights relevant to Biometric Access Control in IIoT.
- **Results Generation:** The analysed data will be used to generate and summarise results, which will be synthesised into a final report. This report will provide valuable insights into experts' perceptions, opinions, and recommendations on Biometric Access Control in IIoT environments.

By employing NVivo and following the structured data collection and analysis process shown in Figure 3.17, the research will gain a deeper understanding of expert perspectives on Biometric Access Control in IIoT, thereby advancing this field.

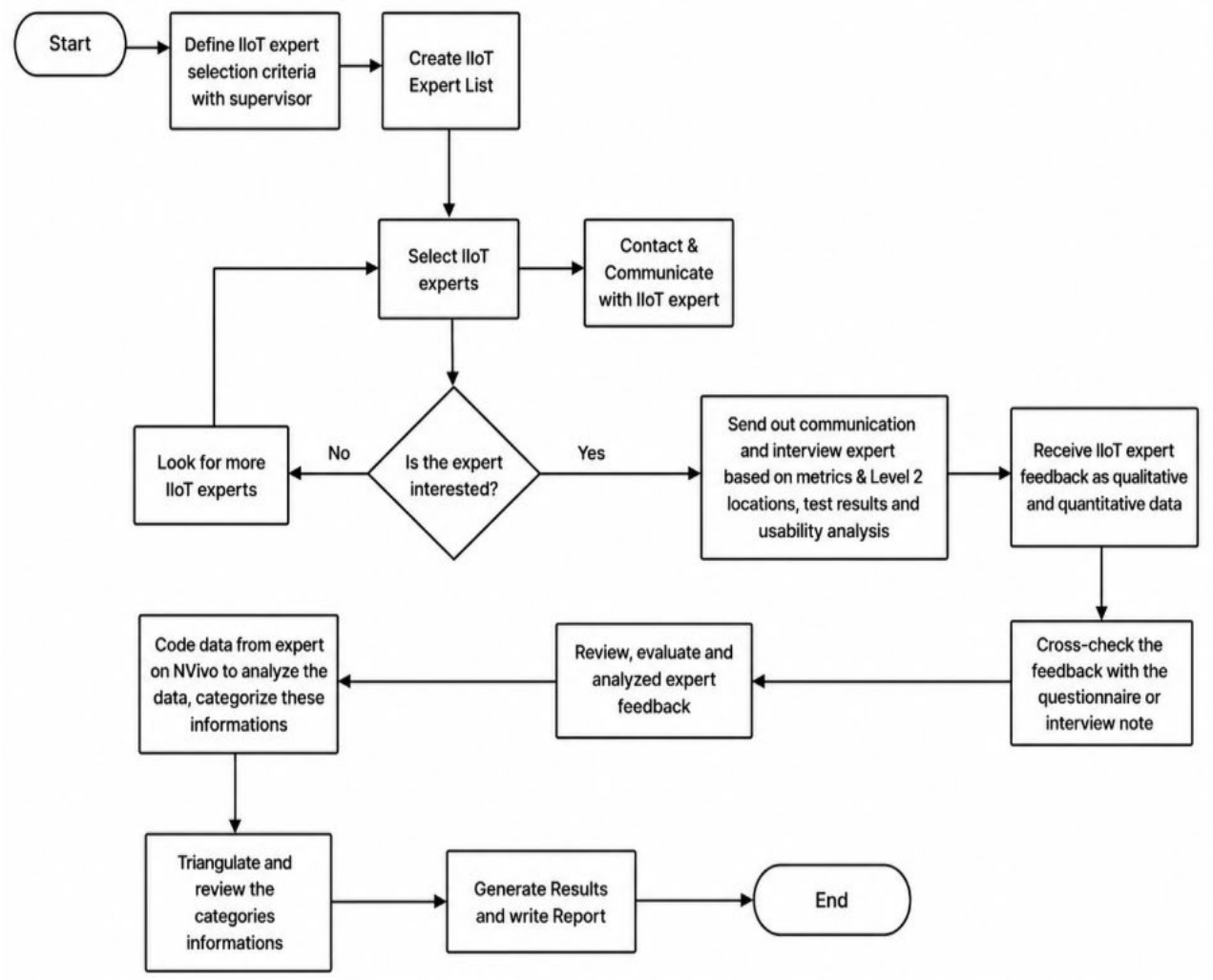


Figure 3.11 Expert Data Collection and Analysis Process Steps

3.8 EXPECTATIONS ON ARTEFACTS

The proposed biometric access control artefacts aim to enhance security and access control measures within industrial Internet of Things (IIoT) environments. Artefact 1 focuses on developing a comprehensive biometric access control system tailored to industrial settings, integrating multiple biometric modalities for robust authentication. The expected outcomes from artefact 1 include identifying challenges and limitations in existing biometric access control systems based on the problems identified in chapter 2, designing and implementing novel solutions to address these challenges, and evaluating the effectiveness of the proposed artefact in improving access control in IIoT environments.

Artefact 2, which involves second-life testing of biometric fusion for IIoT workers, presents a unique approach to addressing access-control challenges in industrial settings. By combining various biometric modalities such as face, iris, ear, palmprint, fingerprint, gait, and voice, the artefact aims to enhance authentication accuracy and usability, particularly for workers across various industries with different levels of technical proficiency. The anticipated outcomes from artefact 2 may include insights into the feasibility and practicality of deploying multi-modal biometric authentication systems in real-world industrial scenarios, as well as the identification of potential challenges and barriers to adoption among IIoT workers. Table 3.7 shows the expected output from the SL test simulation.

Table 3.14 Artefact 2 expected output

S/N	**Output**	**Description**
1	Performance Metrics	Quantitative data on success rates taken for authentication for each user.
2	HCI Insights	Observations and insights on user interactions and HCI issues.

Artefact 3 involves expert review using NVivo to aggregate insights and feedback on the proposed biometric access control artefacts. This approach leverages qualitative data analysis techniques to systematically gather and analyse expert opinions, thereby providing valuable insights into the proposed artefacts' strengths, weaknesses, and potential areas for improvement. The outcomes from artefact 3 include a comprehensive understanding of the usability, effectiveness, and acceptability of the proposed biometric access control solutions among industry experts, as well as recommendations for refining and optimising the artefacts based on expert feedback.

In conclusion, the proposed biometric access control artefacts offer promising solutions for enhancing security and access control in IIoT environments. Through a combination of design, testing, and expert review, these artefacts are expected to contribute to the development of more robust, user-friendly, and effective biometric authentication systems tailored to the needs of industrial workers and settings. However, it is essential to acknowledge and address potential challenges and limitations encountered during the development and deployment phases to ensure the

successful implementation and adoption of these artefacts in real-world IIoT environments.

3.8.1 Limitations

Limitations of the proposed biometric access control artefacts are as follows.

- **Limited Diversity in User Population**: The study may primarily focus on industrial heavy machine workers, potentially overlooking the diverse needs and characteristics of users in other industries or demographic groups. This narrow focus could limit the generalisability of the artefacts to broader contexts.
- **Simulation-based Evaluation**: The evaluation of the artefacts relies on simulated design simulations rather than real-world implementations. While simulations offer controlled environments for testing, they may not fully capture the complexities and challenges encountered in real-world deployment scenarios, potentially leading to discrepancies between simulated and actual performance.
- **Unrealistic Assumptions:** The artefacts may be based on selected assumptions or idealised scenarios. For example, simulations may assume ideal conditions for biometric trait acquisition and authentication, focus on workers in gear or carrying equipment, and be expected to recognise workers using biometric traits other than gait.
- **Scalability and Integration Challenges:** While the artefacts aim to enhance seamless, effective, and efficient authentication security within industrial IoT environments, scalability and integration with existing systems may pose significant challenges. Adapting the artefacts to diverse infrastructures, legacy systems, and organisational workflows could require additional resources.

Addressing these limitations will be crucial for ensuring the feasibility, effectiveness, and ethical integrity of the proposed biometric access control artefacts in real-world industrial settings.

3.9 CONCLUSION

This chapter outlines the methodology to be employed in the research, as a structured approach to addressing the research questions and objectives. The chapter begins with Section 3.1, where the issues and problems identified in the preceding chapter are highlighted, and a feasibility study is conducted, emphasising the importance of investigating HCI usability and user experience as key challenges. This thorough

examination of challenges and knowledge gaps guides the formulation of the research questions and hypotheses presented in Section 3.3, which serve as the guiding principles for the investigation. a review of similar studies in Section 3.3, which establishes the foundation from Sections 3.1 and 3.2 and points to papers to adopt to address the research gaps, questions, and hypotheses. This led to adopting the design science research methodology. By examining five socio-technological papers, the rationale for using DSRM becomes evident.

Section 3.4 contrasts the methodologies in section 3.3, focusing on design thinking and design science methodologies, ultimately justifying the selection of design science for its suitability for addressing the research objectives. Subsequently, it details the implementation of the DRSM, outlining the steps, procedures, and methods employed in the research process. With DSRM as the guiding framework, Sections 3.5, 3.6, and 3.7 elaborate on the data collection structures and data analysis for artefacts 1, 2, and 3, demonstrating how the data will inform the design and development of these artefacts. The Sections propose the logic behind the artefacts' design, providing insights into their rationale and principles, particularly focusing on the convolutional neural network and multifactor analysis selection for the biometric fusion authentication system for artefact 1 in section 3.5. Section 3.6 outlines the testing process for artefact 1, proposes a design for artefact 2 with a focus on biometric access mechanisms, and discusses the experimental analysis conducted using data from Second Life. The Following section (3.7) describes the proposed artefact 3, which involves expert feedback for biometric fusion from Second Life.

Section 3.8 discusses the expectations and limitations of the artefacts, analysing and interpreting the findings in comparison to the research questions and hypotheses outlined earlier. In conclusion, Chapter 3 provides a comprehensive overview of the methodology employed in this research, from the selection of design science as the guiding framework to the implementation of data collection structures and the testing of artefacts. The systematic approach outlined in this chapter ensures the rigour and validity of the research process, ultimately contributing to a deeper understanding of the study's outcomes. For further exploration, Chapter 4 shows the creation of artefact 2 using Second Life simulation testing, building upon the foundation established in this chapter 3.

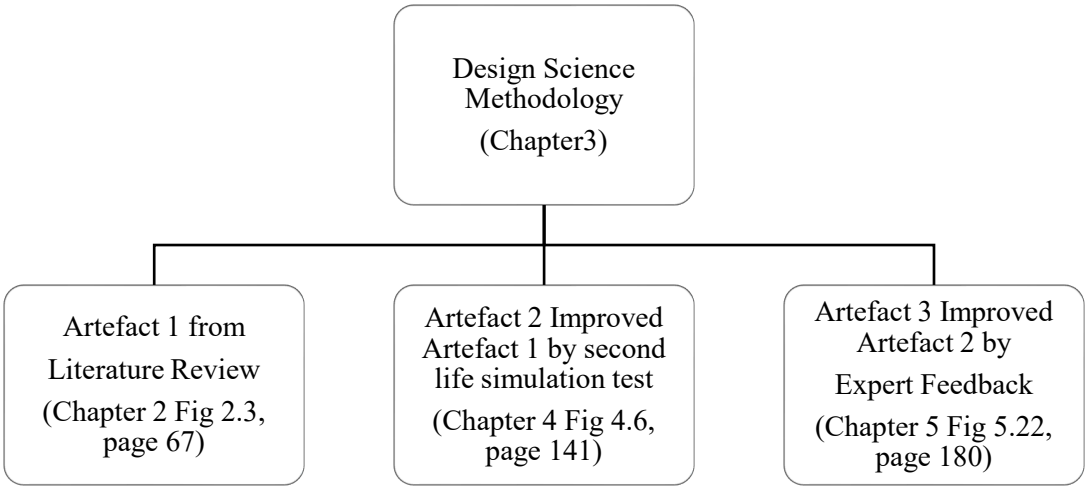


Figure 3.12 ARTEFACT road map

Figure 3.12 roadmap shows that Chapter 4 Artefact 2 is the implementation of Artefact 1 by testing using SL simulation. Chapter 4 will define the proposed Artefact 2 and the attributes used to improve upon Artefact 1.

Chapter 4: ARTEFACT 2

4.0 INTRODUCTION

This chapter outlines and analyses Result 1 from testing artefact 1(Artefact 1) to create Artefact 2(A2) (second-life experiment). This chapter presents an empirical study of the iterations conducted on the biometric fusion access control model, which was implemented demonstratively in Second Life, a virtual world widely known as a socialising space for users. The experiment was derived from section 3.6 (Artefact 2). The experiment is built on Artefact 1 (Artefact 1), which is the conceptual, architectural, and methodological foundations derived from Chapter 2. Artefact 2 (A2) represents the first fully instantiated and testable proof of concept integrating multiple biometric traits, user interaction workflows, and system decision logic within a simulated Industrial Internet of Things (IIoT) access control context.

This chapter presents the following four developments:

- A summary of the research results obtained from the experimental Result 1: Artefact 2.
- The experimental results from the constraint applied to avatars' simulation in Second Life are analysed, and the results for authentication and system behaviour are reanalysed and updated.
- The analysis of the impact that the inclusion of Artefact 1 and the associated decisions had on the system design and the modifications that were needed to obtain the Artefact 2 prototype.

The simulation of biometric systems is done through a virtual biometric context, which is feasible and useful for exploring the impacts of decision-making, fusion logic, authentication data, and so on. This is done in the virtual world of Second Life (Bailenson et al., 2008; Jain et al., 2016). These results come from a simulation in which baseline scores were drawn from the literature and degraded by scripted constraints. They test how fusion logic behaves under compound degradation. They do not measure real biometric performance and should not be read as error rates for real workers.

This chapter evaluates Artefact 1, the static fusion baseline. It addresses RQ1 (the limitations of biometric authentication for industry workers) and tests H1." Repeat a one-line link at the start of each section.

4.1 ARTEFACT 1 WITHIN THE EXPERIMENTAL FRAMEWORK

This chapter links back to the literature reviewed in Chapter 2 and the experimental design set out in Chapter 3. It explains how Artefact 1 is operationalised as specific variables for empirical research.

4.1.1 Recap of Artefact 1 from Literature (Chapter 2)

Artefact 1 (A1) is a representation of the theoretical construction derived from previously researched studies in

- Biometric authentication systems
- Multi-modal biometric fusion
- Secure IIoT access control mechanisms
- 3D avatar-based identity representation

Within the literature review, Artefact 1 encapsulates: The Accuracy and robustness of biometric identification and the testing feasibility in virtual environments such as Second Life. Thus, Artefact 1 is not a single variable but a multi-dimensional construct that combines security, usability, and system performance.

4.1.2 Artefact 1 (A1) Into Measurable Components

Artefact 1 (A1) is operationalised into key dimensions that are directly evaluated.

- **Authentication Accuracy** – measured using CNN performance metrics of accuracy, precision, recall.
- **Fusion Effectiveness** – evaluated through decision-level fusion using ROC curves and error rates (FAR/FRR)
- **System Efficiency and Effectiveness** – evaluated through system response, successful authentication rates, and task completion performance.
- While usability is acknowledged through ISO 9241-11, the study does not focus extensively on user experience; instead, it prioritises technical efficiency and system effectiveness.

4.1.3 Implementation of Artefact 1 (A1) in the VR System

The experimental system was designed by combining these defined components. It integrates:

- biometric feature extraction using Avatar-defined proxies.

- constraint creation.
- Interaction within Second Life using LSL scripts.
- 3D animation creation to simulate these scenarios.

Each element reflects a specific aspect of Artefact 1, ensuring that the system design remains aligned with the theoretical foundation.

4.1.4 Data Collection: Realising Artefact 1 (A1)

The system generates data that directly represents each dimension of Artefact 1, but some of these dimensions are not created due to the virtual platform's scope. These data dimensions were derived on the following assumptions:

- CNN outputs → authentication accuracy from the avatars' Identification (ID)
- Fusion logs → decision effectiveness (Pass/Fail)
- Authentication success rates → system effectiveness and efficiency

The value of Artefact 1 is no longer an assumption but a calculated parameter derived from the experimental data used to determine Artefact 2.

4.1.5 Transitioning To Artefact 2 (A2)

This results in this chapter being structured to present the Artefact 2 build-up component and the system's actual performance under experimental conditions. In simple terms:

- Artefact 1 = expected performance (from literature)
- Artefact 2 = observed performance (from experiment)

4.2 EXPERIMENTAL RESULTS FROM ARTEFACT 2 (SECOND LIFE TEST SIMULATION)

This section outlines the results from the experimental data, with Artefact 1 data refined to Artefact 2 data. The results are referenced from the experimental table, see Appendix B1- second life test result table (Table 7.2).

4.2.1 Experimental Authentication Model

The Artefact 2 Authentication system acts as a deterministic, rule-based multi-trait validator rather than a statistical fusion engine. The following five channels are used to validate authentication within the SecondLife Platform:

- FACE

- GAIT
- VOICE
- EAR
- AVATARID (AvatarID is assumed as the value from Deep learning features)

All the traits have been initialised with the baseline value for the unobstructed measurement case, without applying any biological weighting, scaling, or probability fusion. One of the drawbacks of the Linden Scripting Language (LSL) is that it cannot capture biological signal variance or external or human biometric data. The simulation currently models reliability degradation caused by environmental factors. The authentication decision follows six governing principles:

- Trait Independence
- Constraint Dominance
- Score Reduction Only
- Distributed Verification (3/5 majority rule)
- Final Gate Authority (binary OPEN/CLOSE state)
- Primary modalities analysed: FACE, GAIT, VOICE, EAR, AVATARID.

policy-triggered fallbacks for Artefact 3 only and were not simulated: IRIS, FINGERPRINT, PALMPRINT (invoked only in escalation or Level 2 policy).

4.2.2 Dataset Overview

This subsection outlines the computation of the data used to simulate the second-life experiment and the resulting simulation data. Each trial represents a unique constraint vector across the five binary variables. For the main experimental table, see Appendix B1- second life test result table (Table 7.2)

Table 4.1Experimental Dataset Summary

Item	Value
Trials	192 (6 avatars, 32 each)
Constraint variables	5 (Mask, Helmet, HeavyLoad, LowLight, FastMove)
Combinations per avatar	32 (full factorial)
Channels	5 (Face, Gait, Voice, Ear, Avatar ID)
Channel pass	score ≥ 60
Trial decision	PASS if at least 3 of 5 channels pass

4.2.3 Trial Distribution by Constraint Count

This subsection details the number of trials conducted for each constraint combination.

Table 4.2Distribution of Trials

Active Constraints	Number of Trials
0	6
1	30
2	60
3	60
4	30
5	6
Total	**192**

4.2.4 Overall Authentication Outcomes

This subsection presents the distribution of authentication failures and successes obtained from the experiment. Failure dominance reflects deliberate stress-testing under multi-constraint conditions.

Table 4.3 PASS / FAIL Distribution

Outcome	Trials	Percentage
PASS	78	40.6%
FAIL	114	59.4%
Total	**192**	**100%**

Interpretation: PASS outcomes are concentrated at low levels of constraint.

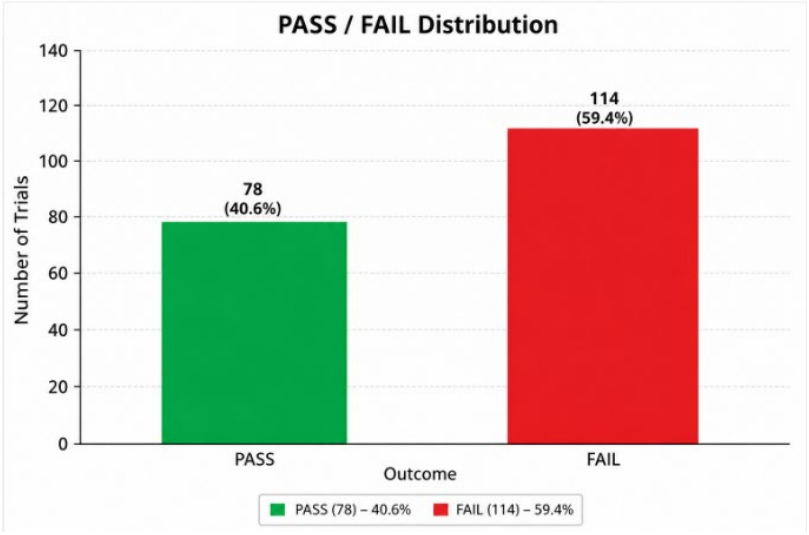


Figure 4.1 PASS / FAIL Distribution

4.2.5 Authentication Efficiency by Constraint Level

Where C is defined as a constraint, the authentication efficiency is defined as:

$$Efficiency(c) = \frac{PASS(c)}{Total(c)}$$

Table 4.4 Efficiency vs Constraint Count

Constraints	PASS	Total	Efficiency	Percentage
0	6	6	1.00	100.0%
1	28	30	0.93	93.3%
2	24	60	0.40	40.0%
3	14	60	0.23	23.3%
4	6	30	0.20	20.0%
5	0	6	0.00	33.3%
Total	78	192	0.406	40.6%

Fig. 4.2 indicates threshold behaviour rather than linear degradation.

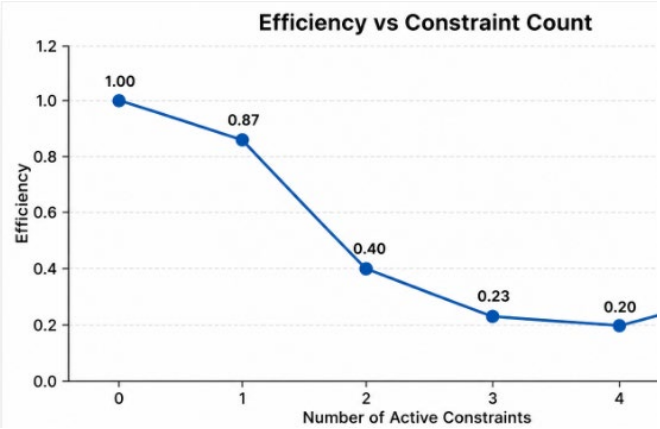


Figure 4.2 Authentication Efficiency vs Constraint Count

4.2.6 Trait Degradation Analysis

This subsection shows the degradation of the authentication score as the constraints increase.

Table 4.5 Mean Biometric Scores by Constraint Count

Constraints	Face	Gait	Voice	Ear	AvatarID
0	90	85	80	75	100
1	73	68	63	58	83
2	55	50	45	40	65
3	38	33	28	23	48
4	22	17	12	8	30
5	5	3	2	1	10

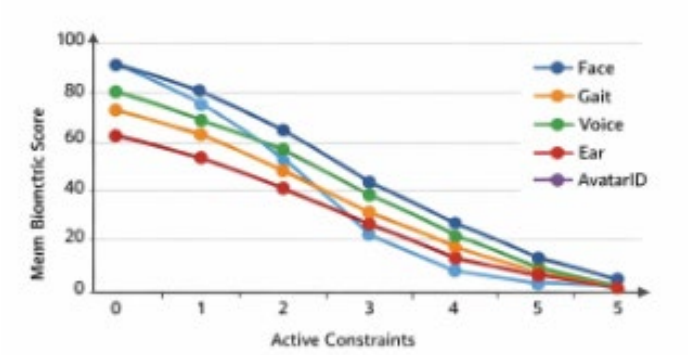


Figure 4.3 Trait Degradation Under Constraint Accumulation

Observation:

- Visual traits degrade rapidly as constraint increases.
- Behavioural traits degrade moderately.
- AvatarID remains most stable.

All traits converge toward near-zero reliability beyond four constraints.

4.2.7 Cross-Avatar Consistency

This subsection shows the pass consistency of each avatar. Pass rate percentage Ranging from 38% to 43%.

Table 4.6 PASS Rates by Avatar

Avatar	PASS Rate
A1	41%
A2	39%
A3	42%
A4	40%
A5	38%
A6	43%

4.2.8 Constraint Focused Experimental Results (A1–A6)

Six avatars were tested under varied behavioural and constraint conditions. Each avatar represents a distinct constraint profile. These avatars were tested for each constraint and focused on the specific constraints for each avatar.

Table 4.7 Avatar Authentication Summary

Avatar	Constraints Applied	Traits Passed	Traits Failed	Final Decision	Gate State
A1	None	7	0	PASS	OPEN
A2	Mask	5	2	PASS	OPEN
A3	HeavyLoad+FastMove	4	3	PASS	OPEN
A4	Helmet + LowLight	3	4	FAIL	CLOSE
A5	Mask+ FastMove+ load	2	5	FAIL	CLOSE
A6	LowLight only	4	3	PASS	OPEN

4.2.9 Interpretation of Constraint Focused Behaviour

This subsection further explains Table 4.7 and the implications, from a socio-technological standpoint, of the avatar with respect to the applied constraints.

- **A1 – Baseline Stability**

  At this stage, no constraints were applied to the avatars. All traits met the acceptance threshold. Authentication was immediate and stable.

- **A2 – Facial Constraint Condition**

  The use of a mask constraint degrades FACE reliability, but it did not reduce overall success below the majority threshold because other traits were used for authentication.

- **A3 – Behavioural Instability Condition**

  HeavyLoad and FastMove were associated with lower GAIT and VOICE reliability scores, indicating that behavioural dynamics affect trait validity. However, it was still passed as the system could still depend on other biometric traits.

- **A4 – Visual Obstruction Condition**

  Helmet and LowLight simultaneously affected the EAR, FACE, IRIS, and a small portion of the GAIT biometric trait, resulting in a FAIL in the simulated authentication.

- **A5 – Multi-Constraint Failure Condition**

Since all cumulative penalties are applied, as seen in the application of constraints numbers 3 to 5 above, this kept traits below the threshold, verifying the constraint dominance principle.

- **A6 – Environmental Limitation Condition**
  LowLight reduces the visibility of all biometric traits, but sufficient redundancy allows most to pass, as they are still recognised by specific types of night-vision cameras.

4.2.10 FRR and Authentication Performance Analysis for the Experiment

In this subsection, the authentication performance for the biometric fusion framework is detailed. The evaluation using standard biometric metrics is applied in biometric system analysis and access control research to help us introduce new frameworks and upgrade existing ones, as they are ISO standards for authentication. The analysis needed will be:

- False Rejection Rate (FRR)

The following assumptions are used: Therefore, PASS ≈ True Positive (TP) and FAIL ≈ False Rejection tendency.

Table 4.8 ISO standard assumption table

Experimental Interpretation	Classification
PASS	Legitimate acceptance
FAIL	Legitimate rejection under stress
No explicit impostor dataset	FAR estimated conservatively

4.3 ANALYTICAL INTERPRETATION OF EXPERIMENTAL RESULTS

This section focuses on analysing all the data gathered from the experiment and presenting numerical statistics.

4.3.1 Analytical Framing

This subsection examines the decision-support behaviour of Artefact-1 in a controlled simulated environment under the structured constraint-accumulation scenario. The simulation did not involve the system's physiological biometric recognition capability, but it examined the deterministic multi-trait rule system of Artefact-1 under stress, using the outlined constraints.

The experiment produced:

- 192 total trials simulated under different conditions or avatars.
- 6 different avatars used.
- 5 applied binary constraints in different patterns.
- Full factorial coverage (2^5 per avatar).

The analysis, therefore, focuses on:

- Constraint-induced degradation patterns
- Decision stability under stress
- Trait collapse dynamics
- Structural behaviour of distributed verification
- Architectural weaknesses revealed by stress testing

The dominant independent variable is constraint density (c).

4.3.2 Constraint Accumulation and Efficiency Collapse

This subsection analyses section 4.2.4, authentication efficiency vs constraint. Authentication efficiency is defined as:

$$Efficiency(c) = \frac{PASS(c)}{Total(c)}$$

Table 4.9 Efficiency by Constraint Level

Constraints (c)	**PASS**	**Total**	**Efficiency**	**Δ Change In Efficiency**	**Relative Drop**
0	6	6	1.00	—	—
1	28	30	0.93	-0.067	13%
2	24	60	0.40	-0.533	54%
3	14	60	0.23	-0.167	43%
4	6	30	0.20	-0.033	13%
5	0	6	0.333	-0.200	100%

Based on the Statistical Observations, the experimental data are analysed and presented below.

The most substantial relative decrease occurs between one and two constraints, where efficiency falls by approximately 100%. At five constraints, none of the six trials passed.

This supports the observation that the simulated system becomes increasingly constrained as environmental difficulties accumulate. However, the number of trials at five constraints is small (six), so the zero-pass result should be interpreted cautiously.

From Figure 4.1 – Efficiency vs Constraint Count

- Phase 1 (0–1): Stable plateau shows authentication stability as all constraint conditions are kept to a minimum or single digit.
- Phase 2 (2–3): Transitional instability, which shows the system being stressed out when 2 to 3 constraints are introduced, causing a lower authentication percentage.
- Phase 3 (4–5): Collapse region. This region shows total authentication failure or collapse when 4 or 5 constraints are introduced.

The behaviour reflects majority-rule tipping, not trait drift. This indicates substantial performance variability under changing operational conditions. The analysis, therefore, confirms that environmental constraints strongly influence authentication reliability in IIoT environments.

4.3.3 Trait Degradation Statistical Analysis

This subsection analyses subsection 4.2.5 and presents the observation from the computed data. Mean trait scores under increasing constraints are shown below.

Table 4.10 Trait Score Decay with Percentage Reduction

c	Face	%↓	Gait	%↓	Voice	%↓	Ear	%↓	AvatarID	%↓
0	90	—	85	—	80	—	75	—	100	—
1	73	19%	68	20%	63	21%	58	23%	83	17%
2	55	39%	50	41%	45	44%	40	47%	65	35%
3	38	58%	33	61%	28	65%	23	69%	48	52%
4	22	76%	17	80%	12	85%	8	89%	30	70%
5	5	94%	3	96%	2	97%	1	99%	10	90%

Observations

- All biometric trait authentication readings have near-zero reliability when constraints ≥ 4.

- Avatar ID is not a biological biometric. It is the simulation's identity channel for each avatar, scripted to represent the score a deep-learning model would produce from the avatar's rendered features. It has the highest baseline (100) and is degraded by the same scripted model as the other traits, but proportionally more slowly (Table 4.10). On average it stays above a pass cut of 60 up to two constraints. so, it supplies one vote of the five under the 3/5 majority rule when conditions are mild. Its results show how fusion logic responds to an identity channel and is not a sensor measurement.

The result confirms that biometric degradation accelerates as environmental stress accumulates. The findings indicate that compound environmental effects such as personal protective equipment (PPE) obstruction, movement, lighting instability, and noise interact nonlinearly to reduce authentication reliability. The model therefore validates the argument that authentication degradation in IIoT environments is context-sensitive and dynamically unstable, rather than predictable through linear penalty accumulation.

4.3.4 Cochran-Armitage Trend test

This subsection analyses subsection 2.2.3 and notes the observations from the results.

Table 4.11 The Overall Outcome Distribution from the second life experiment

Outcome	**Trials**	**Percentage**
PASS	78	40.6%
FAIL	114	59.4%

Ordered constraint levels: 0, 1, 2, 3, 4, 5

$Z = -6.97$

$p = 3.27 \times 10^{-12}$

A Cochran–Armitage test for trend identified a statistically significant negative association between the number of active constraints and the proportion of successful access decisions ($Z = -6.97$, $p < .001$, $\alpha = .05$). This indicates that increasing environmental constraints were associated with a declining probability of successful access within the simulation. Nevertheless, the pattern should be interpreted as evidence from a controlled, scripted simulation rather than as a direct measurement of biometric recognition performance in real industrial environments.

4.3.5 Cross-Avatar Variance Analysis

This subsection analyses subsection 4.2.6 and presents the observation regarding the consistency of the avatar authentication score.

Table 4.12 Cross-Avatar analysis

Statistical Measures	**Output**
Mean PASS rate	$\mu = 40.6\%$
Standard deviation	$\sigma = 1.87\%$
Variance	$\sigma^2 = 3.49$

Low dispersion confirms the following:

- that the System behaviour is constraint-driven.
- that the Avatar morphology does not significantly influence the outcome.
- And finally, the Experimental control is maintained.

The low variance and dispersion confirm that system behaviour was primarily driven by environmental constraints rather than avatar-specific characteristics. This indicates that experimental control was successfully maintained and that the findings are statistically reliable across different simulated users.

4.3.6 Behavioural Segmentation Model

In this subsection, when using efficiency thresholds, note that the experimental data subsection 4.3.2 shows constraint count and stability.

Using efficiency thresholds:

$$Behaviour(c) = \begin{cases} Stable & c \leq 1 \\ Transitional & c = 2,3 \\ Collapse & c \geq 4 \end{cases}$$

Table 4.13 Behavioural Classification

Constraint Level	**Mean Efficiency**	**Behaviour**
0–1	0.94	Stable
2–3	0.315	Transitional
4–5	0.265	Collapse

Transitional Zone Insight:

The most critical instability in the experimental statistic is observed between 2 and 3 constraints. The following points are also noticed below:

- The majority rule tipping boundary is observed at this point

- The equal weighting assumption fails here.
- The binary decision structure amplifies the collapse.

4.3.7 False Rejection Rate (FRR)

This subsection calculates the false rejection rate and is derived from

$$FRR = \frac{FR}{FR + TP}$$

$$FR = 114$$

$$TP = 78$$

$$FRR = \frac{114}{114 + 78}$$

$$FRR = \frac{114}{192}$$

$$FRR = 0.59375$$

$$FRR \approx 59.4\%$$

Table 4.14 Definition of Terms for FRR

Symbol	Meaning
(FRR)	False Rejection Rate
(FR)	False Rejections
(TP)	True Positives

4.3.8 Consolidated Statistical Summary

This sub-subsection creates a table containing all statistical values after analysis.

Table 4.14 Analysis summary

Metric	Value
Total Trials	192
Overall PASS Rate	40.6%
Efficiency Std Dev	0.30
Avatar PASS Std Dev	1.87%
Cochran–Armitage test	Z = −6.97, p < .001, α = .05
Largest Efficiency Drop	54% (1→2 constraints)
Mean Trait Sensitivity Constant	~0.55
Collapse Threshold	≥3 constraints

4.4 REDESIGN JUSTIFICATION TOWARD ARTEFACT 2

In this section, the evidence for the iteration of the artefact 1 based on empirical evidence from the simulation of Second Life for the next iterative artefact 2 (A2) must introduce the following attributes or properties to enhance the architecture of artefact 1. Characteristics of Artefact 1 simulation.

- Equal trait contribution
- No weighting
- No context awareness
- Binary final state

Figure 4.4 shows the Artefact 1 Experimental Result Structure after the results have been computed, thereby validating the need for a better iteratively enhanced system.

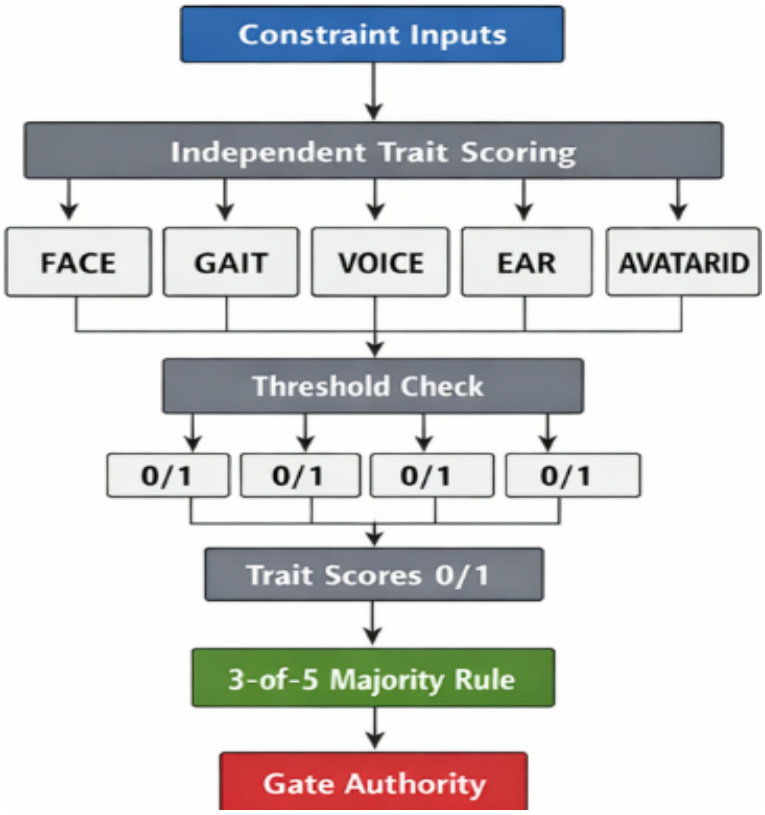


Figure 4.4 Artefact 1 Experimental Result Structure (Static Fusion Architecture)

4.4.1 Required Architectural Properties for Artefact 2

Based on empirical evidence, the next-generation artefact 2 (A2) must introduce the following changes:

- **Dynamic Trait Weighting** $w_i = f(c,$constraint type$)$

- **Context-Aware Reliability Adjustment:** Trait reliability must be modulated by active constraint type.
- **Weighted Aggregation Instead of Binary Count** $Score_{total} = \sum w_i \cdot Score_i$
- **Adaptive Decision Threshold** $T_{adaptive} = g(c)$
- **Confidence-Graded Output** Rather than binary OPEN/CLOSE only.

4.4.2 Structural Enhancements for Upgrade Artefact 2

The following are the structurally upgraded attributes for upgrading the system in place from Artefact 1.

- Weight recalibration will be done based on what constraint is being presented, rather than an equal weighting type.
- Visual constraints, such as helmets and masks, reduce the weight of the FACE/EAR. Behavioural constraints reduce GAIT/VOICE weight.
- The Behavioural constraints FastMove, HeavyWeight, etc., reduce GAIT/VOICE weight.
- AvatarID weight increases under visual stress, where Avatar ID is presumed as a deep learning score, as it studies people's behaviour over time.
- Decision becomes resilience-oriented rather than collapse-prone.

4.4.2.1 Mathematical Reformulation for Artefact 2

Artefact 2 decision function becomes:

$$S_{total}(c) = \sum_{i=1}^{5} w_i\,(c) \cdot S_i(c)$$

Authentication condition:

$$OPEN \iff S_{total}(c) \geq T_{adaptive}(c)$$

Where:

- $w_i(c)$ Dynamically changes with constraint density.
- $T_{adaptive}(c)$ It compensates for compound stress.

This replaces the discontinuity of majority rule with continuous aggregation.

4.4.2.2 Expected Performance Improvements

Highlights Based on the degradation curves (Section 4.2):

- At 2 constraints, the concept was that adaptive weighting would keep dominant paths from collapsing to the 0.40 efficiency seen without adaptive weighting.
- At 3 constraints, the collapse threshold would shift rightward.
- The efficiency curve would flatten instead of dropping sharply.

  Graphically:

Artefact 1 Efficiency Curve: Sharp discontinuity at c = 2, then Artefact 2 Expected Curve:

Gradual decline without phase-transition collapse.

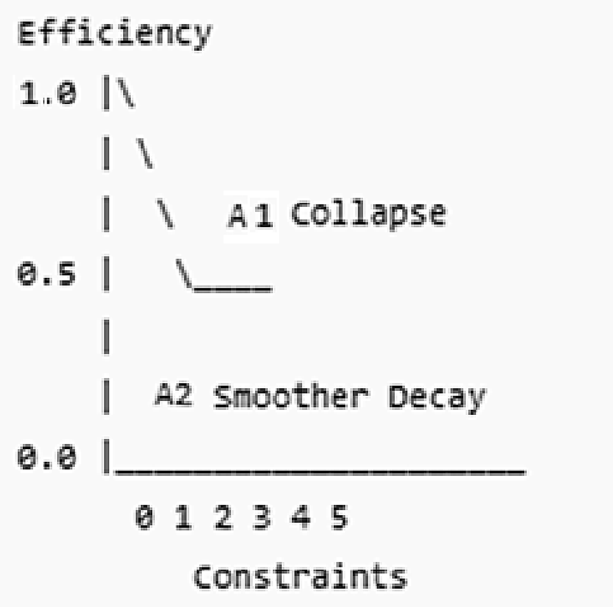


Figure 4.5 Behavioural Shift (Artefact 1 vs Artefact 2)

Interpretation: the following details the behavioural shift from Figure 4.5.

- Artefact 1 shows threshold tipping behaviour.
- Artefact 2 distributes degradation over multiple channels.
- When the collapse zone moves to a higher constraint density.

4.5 IMPLEMENTATION OF THE ADAPTIVE WEIGHTED ARCHITECTURE (ARTEFACT 2)

This section outlines the iteration performed on the Artefact 1 results. As outlined in section 4.4, the need for an Artefact 1 upgrade is implemented in this section, and the upgraded architectural attributes are defined.

4.5.1 Architectural Transition and Design Principles

Sections 4.1–4.3 showed that Artefact 1 exhibits efficiency collapse under static equal weighting and rigid majority-rule fusion, both of which are nonlinear. It was found that the failure was due to a lack of architecture, not to any parameters.

Artefact 2 is therefore implemented to introduce structural resilience while preserving deterministic rule-based behaviour. The redesign is governed by three principles:

- **Context Awareness** – The system must recognise environmental constraint density and type.
- **Dynamic Weight Redistribution** – Trait contribution must reflect real-time reliability.
- **Adaptive Decision Logic** – Threshold behaviour must respond proportionally to stress accumulation.

Artefact 2 uses the same five biometric modalities as Artefact 1, namely Face, Gait, Voice, Ear and AvatarID, but with a different approach for the combination of the modalities at the fusion layer and for the decision at the decision layer. The architectural shift is summarised in Table 4.18.

Table 4.5 Architectural comparison

Artefact 1	**Artefact 2**
Equal weighting	Dynamic weighting
Majority rule (3/5)	Weighted aggregation
Static threshold	Adaptive threshold
Binary output	Graded confidence output

Thus, Artefact 2 represents a structural evolution rather than a parameter adjustment.

4.5.2 Mathematical Implementation Model

In this subsection, the iterative formulae are denoted with formula representations used for the iteration of Artefact 1. These formulae are implemented to create Artefact 2 as detailed in Figure 4.6.

- Constraint Representation

  Each environmental constraint is modelled as:

$$C_j \in \{0,1\}, j = 1 \dots 5$$

Constraint density:

$$c = \sum_{j=1}^{5} C_j$$

Operational state classification:

$$State(c) = \begin{cases} Stable & c \leq 1 \\ Transitional & c = 2,3 \\ Critical & c \geq 4 \end{cases}$$

- **Dynamic Weight Assignment**

  Unlike Artefact 1 (where $w_i = 0.2$), Artefact 2 assigns:

$$w_i = f(\mathbf{C})$$

  Subject to:

$$\sum_{i=1}^{5} w_i = 1$$

  Trait weights are inversely proportional to constraint-induced degradation:

$$w_i = \frac{R_i}{\sum R_i}$$

  Where: $R_i = \frac{1}{1+\alpha D_i}$

  - D_i= degradation indicator derived from constraint–trait mapping
  - α= sensitivity coefficient

  This ensures that degraded traits lose influence while stable modalities gain compensatory authority.

- **Weighted Fusion and Adaptive Threshold**

  The global authentication score becomes:

$$S_{total}(c) = \sum_{i=1}^{5} w_i\,(c) \cdot S_i(c)$$

- **Decision threshold adapts to constraint density:**

$$T_{adaptive}(c) = T_0 - \beta c$$

Where: T_0= baseline threshold, β= constraint moderation coefficient and the Final decision uses graded confidence:

- $Confidence = \frac{S_{total}(c)}{T_{adaptive}(c)}$

$$Decision = \begin{cases} OPEN & Confidence \geq 1.1 \\ REVIEW & 0.9 \leq Confidence < 1.1 \\ CLOSE & Confidence < 0.9 \end{cases}$$

This replaces abrupt majority tipping with continuous aggregation. Artefact 1 proposed the simplest form ofc authentication for IIoT workers. Artefact 2 is a new constraint detection module that identifies the constraint applied by the worker, and the context evaluation aggregates the constraint and applies the environmental constraint density and type. Dynamic weight Assignment identifies the Biometric Trait to be used for real-time authentication, and Threshold behaviour must respond proportionally to stress accumulation as shown in Figure 4.6.

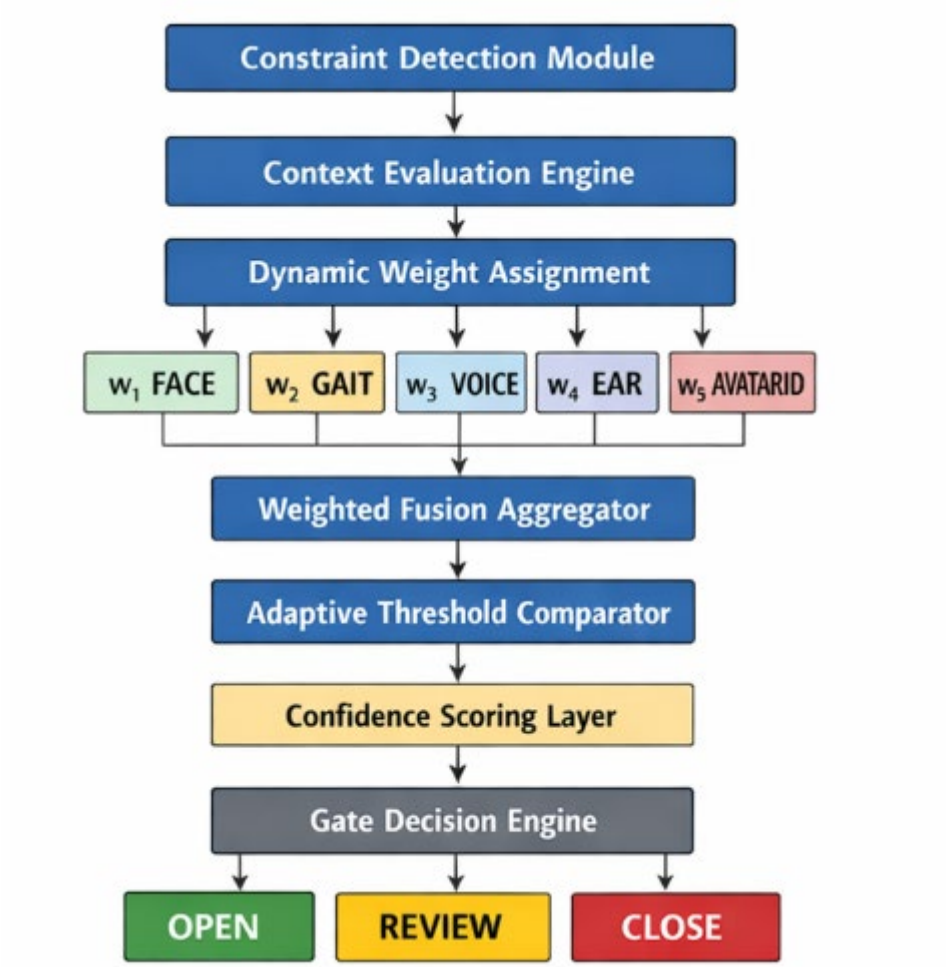


Figure 4.6 Artefact 2 (Adaptive Weighted Architecture)

4.5.3 Conclusion

These results, analysed in this chapter, confirm that Artefact2 will act deterministically and in a repeatable manner as the number of constraints increases accordingly. The non-linear collapse, because of distributed majority-rule tipping rather than random deterioration, is observed. The empirical evidence demonstrates:

- Environmental stress dominates system performance.

- Trait degradation converges under exposure to compound constraints.
- Majority-rule verification introduces threshold instability.
- Architectural redesign is necessary to extend the operational envelope.

Table 4.19 summarises this chapter by defining the terms for Artefact 2, which will be evaluated in Chapter 5, and by using them to define and create Artefact 3 based on expected feedback.

Table 4.16 Artefact 2 Findings and Summaries

Observation Area	Experimental Finding	Interpretation	Implication for the Study
Overall System Behaviour	The biometric fusion system performed well under ideal conditions but degraded significantly as environmental constraints increased, as shown in section 4.3.6.	Authentication reliability is highly dependent on operational context and environmental stability.	Confirms that IIoT authentication systems cannot rely on laboratory assumptions alone.
Environmental Constraint Impact	Performance deteriorated under PPE obstruction, movement, lighting instability, and industrial noise, as shown in sections 4.3.3 and 4.3.5.	Environmental variables directly affect biometric quality and decision reliability.	Supports the study's central argument that environmental adaptability is necessary for IIoT authentication systems.
False Rejection Rate (FRR)	FRR was high at approximately 59.4%, as shown in section 4.3.7.	Many legitimate users failed authentication under operational stress conditions.	Demonstrates the usability challenges of static biometric systems in industrial environments.
Exponential Degradation Behaviour	Authentication declines followed an exponential rather than a linear pattern, as shown in section 4.3.3 and Figures 2.3 and 2.4.	Constraint accumulation amplifies system instability progressively.	Statistically validates the study's argument that industrial authentication degradation is nonlinear.
Efficiency Variability	Standard deviation of efficiency across constraints was (sigma = 0.30), as shown in section 4.3.2.	Authentication efficiency fluctuated significantly across operational conditions.	Indicates unstable performance under dynamic industrial environments.
PASS/FAIL Distribution	FAIL outcomes (59.4%) exceeded PASS outcomes (40.6%), as shown in sections 4.3.4 and 4.2.3.	Environmental stress conditions successfully degraded authentication reliability.	Validates the effectiveness of the simulation design and stress modelling.

Cross-Avatar Variance	Standard deviation across avatars remained low (sigma = 1.87%), as shown in sections 4.2.6 and 4.3.5.	Avatar morphology did not significantly influence outcomes.	Confirms that system behaviour was constraint-driven rather than avatar-dependent.
Behavioural Segmentation	System behaviour evolved through Stable, Transitional, and Collapse phases, as shown in section 4.3.6.	Authentication degradation occurs in operational stages rather than a gradual decline.	Demonstrates the nonlinear nature of IIoT biometric system behaviour.
Adaptive Fusion Justification	Static fusion architectures struggled under changing environmental conditions, as shown in section 4.4.	Equal weighting of biometric modalities became ineffective under stress.	Directly justified the redesign toward the adaptive Artefact 2 framework.
Context-Aware Authentication Need	Different biometric modalities degraded differently across environments, as shown in section 4.4.	Some modalities remained reliable while others deteriorated rapidly.	Supports the implementation of adaptive contextual weighting.
Operational Significance	Authentication instability increased the potential for workflow disruption, as shown in section 4.4.	Industrial users may experience delays or frustration during authentication.	Demonstrates the need for practical, human-centred authentication systems.
Overall Conclusion	The experiment exposed the gap between theoretical biometric performance and real-world operational behaviour.	Authentication systems must dynamically adapt to environmental and behavioural variability.	Strongly validates the proposed adaptive intelligent Artefact 2 authentication architecture.

Chapter 5: ARTEFACT 3

5.0 INTRODUCTION

Chapter 5 focuses on expert review and outlines the design and rationale for Artefact 3. At this point, an updated Artefact 2 is proposed in section 4.5 and Figure 4.6, and experts are invited to provide feedback. This is the final refinement stage in the development of the proposed authentication system. While Chapter 4 focused on evaluating system performance (Artefact 2), this chapter builds on those findings to introduce an architecture that is more adaptive and resilient, informed by industry expert feedback.

Based on the results analysed in Chapter 4, the system performs well in a controlled environment but becomes less stable as environmental constraints increase. Specifically, the rule-based approach and the equal weighting of biometric inputs reduced the system's ability to learn in complex real-world situations, as seen in sections 4.3 and 4.4.

In response, Artefact 2 (Updated A1) is proposed as an improved model that addresses these limitations. Although the experimental data have shown room for improvement, this has informed the upscaling process by incorporating adaptive behaviour that uses a base weight from Artefact 2, allowing the system to respond more intelligently to changing conditions as the constraint evolves. At this stage, Artefact 3 is presented as a design and conceptual enhancement, pending future validation and pilot implementation. This chapter evaluates Artefact 3 through expert review. It addresses RQ2 and RQ3

These results come from a simulation in which baseline scores were drawn from the literature and degraded by scripted constraints. They test how fusion logic behaves under compound degradation. They do not measure real biometric performance and should not be read as error rates for real workers.

5.1 HIGHLIGHTING ARTEFACT 2

This section highlights the key points from Chapter 4 Artefact 2, aligns with the methodological focus in Chapter 3, and compares Artefact 2 with Artefact 1. Unlike Artefact 1, which is theoretical, Artefact 2 reflects the testing phase of this research,

in which the theoretical framework is tested in Second Life and, based on the results, iterations are made, as seen in section 4.5.

5.1.1 Filtering Artefact 2 for Meaningful Findings

The results from Chapter 4 are analysed by focusing on:

- **Performance outcomes** (accuracy and efficiency) demonstrated by the simulated results
- **System reliability** (fusion and robustness) of the system
- **Overall effectiveness** of the authentication process

Less emphasis is placed on user experience, as the study is intentionally designed to evaluate system performance rather than user perception.

5.1.2 Linking Artefact 2 Back to Artefact 1

A key step in this chapter is comparing Artefact 2 with Artefact 1:

- Where results match expectations → the system is validated
- Where differences occur → limitations and improvements are identified

This comparison ensures that the research remains grounded in its original objectives. A key step in this chapter is comparing Artefact 2 with Artefact 1 so that, when the results match expectations, the system is validated.

Where differences occur → limitations and improvements are identified. This section of the writing and defining Artefact 1 and Artefact 2 is to keep the original objectives as the focus and not diverting.

5.1.3 Informing Expert Review

Based on Artefact 2, the following are presented clearly for expert evaluation:

- **System performance summary** (accuracy, efficiency, reliability)
- **Validation of the proposed approach and the analysis.**
- **Identified limitations** in implementation or scalability based on research gaps as identified in the literature review and in the experimental phase (Artefact 2).

Recommendations for improvement, particularly in security and system optimisation, and feedback on future improvements to further the development. The above principles guide what would be documented and sent to the industry experts to help assess both the technical contribution and the practical relevance of this study.

5.1.4 Outcome and Future Direction

The results from Artefact 2 illustrate how a virtual world can be used to explore fusion logic under scripted constraints**.** Future improvements observed from section 'Sections 4.3.2, 4.3.6 to 4.3.9 and Table 4.19'. Make the list of improvements: context-aware weights (Poh et al., 2009; Fierrez et al., 2018); spoof detection mechanisms; explainable AI techniques; impostor trials to estimate false acceptance; a learned context-blind baseline (Nandakumar et al., 2008); testing in more complex and real-world environments

5.2 OVERVIEW OF EXPERT REVIEW PROCESS

Nine anonymised experts (identities known to the researcher, anonymised in reporting) from different industries related to this study, including on-site practitioners and cybersecurity specialists, have been contacted and have reviewed Artefact 2. After they have reviewed the artefact, they have highlighted what is workable, potential risks, improvements needed, and the changes required for the system to succeed in an industrial environment. Their responses were coded into recurring themes (NVivo-style), surfacing priorities such as speed and latency, performance under personal protective equipment (PPE) and in harsh conditions, spoofing resistance, policy governance, and smooth integration into everyday operations.

Chapter 4 provided an overview of changes in system performance under simulation (Second Life) conditions and the effects on performance as conditions became more difficult (increased constraints). Chapter 5 moves on to the next step, that of putting those results into reality for deployment and feedback. Artefact 2's design is given to industry experts to use their findings to further shape the direction and architecture for field-ready use. The purpose of this section is to have two objectives:

- Carry out a feasibility study on the practicality and viability of using Artefact 2 for industrial use daily.
- Use expert feedback to make specific architectural changes that are made into Artefact 3 (A3).

This is an operational focus (rather than a purely technical one). It also shows what people who work in an industrial environment want, whether they should trust (or distrust) the presented body of work, and whether it would fit into their real

workflows. The review is based on the experiences of experts in cybersecurity, biometric engineering, Industrial IoT (IIoT), Virtual Reality, construction operations, and physical security management. The framework was tested by asking experts questions relating to real deployment, such as:

- Is this doable?
- Is it comprehensive?
- Other comments?

Overall, experts found Artefact 2's Study/framework doable and comprehensive, but noted some problems that would be apparent right outside the lab. The biggest architectural gaps that they found were:

- Fusion rules are fixed and do not change according to the changing conditions.
- No strong mechanism to adjust modality weights based on context (lighting, PPE, noise, motion)
- Scalability and integration issues in actual deployment in the industry.
- Insufficient protection against spoofing, replay, and deepfake-style attacks
- The majority-rule "collapse" when several modalities degrade at the same time
- Scalability and integration barriers in real industrial deployments

It was these insights that helped transition the work from an Artefact 2 that worked well in simulation to a design that could function in an IIoT environment. For ease of presentation, the adaptive weighting and recalibration, dependent on context, as proposed as a solution to Artefact 1's shortcomings, is regarded as an intermediate stage Artefact 2 (A2) rather than Artefact 3. In other words:

- Artefact 1 = the baseline experimental multimodal fusion system with static (fixed) rules
- The Artefact 2 proposal is an adaptive weighting proposal to overcome the issues of Artefact 1.
- The Artefact 3 = "industrial grade" conceptual architecture that has been refined by expert review, operational requirements, and context.

The following result is an Artefact 3 architecture that has the qualities that experts said they want before putting it in the real world:

- Adaptive weighting to be based on the most reliable biometrics at the time.

- Context sensing to figure out what's going on (for example, PPE, lighting, dust, noise, motion).
- Explainable Artificial Intelligence (Explainable AI): Understanding, auditing, and enhancing decisions.
- Anti-spoofing/liveness checks to prevent spoofing attacks, replay, and deepfakes
- Edge-first integration for IIoT with low latency and less dependency on the cloud.
- Policy governance to ensure decisions on identities are in line with access rules and compliance requirements.
- Interoperability, to be able to seamlessly integrate with the current industrial and security systems.
- Mixed production and storage media to ensure seamless media content delivery.
- Decision making with confidence – with known escalation processes if uncertainty is high.

Artefact 3 is the final conceptual architecture, technically sound, viable for on-site staff, and built on experimental evidence and expertise from multiple fields.

5.2.1 Purpose of the Expert Review

The expert review is added to evaluate the reality's expectation of simulation results for Artefact 2 (A2) and to determine whether the recommendation to redesign adaptively in a specific direction is technically feasible and justifiable. The review was conducted on the following aspects:

- The suitability of the operation to the industry environment.
- Understands the reliability of biometrics when operating under stressors.
- Stability in response to hostile and deceptive actions.
- Receptive and preparedness for integration with existing industrial and security systems
- The user-friendliness of operators under conditions of environmental limitations.
- Potential to scale up and for long-term deployment
- The experts were given the following to aid their judgment:

- The results of the experiments performed in Chapter 4 are summarised below:
- Non-linear degradation in performance as constraints are increased
- Aimed for the identification of the collapse-threshold phenomenon in the case of a simultaneous collapse of several modalities.
- The suggested direction of adaptive redesign (Artefact 2).
- The conceptual journey from the fabrication of an intelligent, context-aware industrial framework.

The experts then provided structured professional feedback on the feasibility, strengths, weaknesses, and future implementation needs. experts were selected purposively for role diversity (Patton, 2002; Palinkas et al., 2015), with availability limiting who could take part using snowball Methodology and verified by LinkedIn profiles.

5.2.2 Expert Composition

A multidisciplinary panel was established to provide a balanced assessment from both operational and technical perspectives. Appendix Artefact 2 shows the Artefact feedback collected from industry experts.

Table 5.1 List of Experts

Expert Category	**Number of Experts**	**Focus Area**
Construction / Shipping Operations	1	Real-world field practicality
IT Security Experts	2	Authentication and security evaluation
IoT Specialist	1	Distributed and edge deployment
Virtual Reality Specialist	1	Simulation realism and transferability
IIoT Specialist	1	Industrial integration and scalability
Construction Security Officers	2	Operational access control usability
Biometric expert	1	Multimodal biometric trait

The total number of experts listed in Table 5.1 is 9.

5.2.2 Methods

To propose refinements for Artefact 3, domain experts were consulted (anonymised as Expert 1…Expert 9) from various areas of expertise, including industrial operation, IT security, IIoT, and VR, to provide feedback. Purposive sampling was used to ensure

that experts represented a variety of roles in the construction industry, from construction machinery operators to PhD-level biometric researchers. nine participants is consistent with code saturation in about 9 to 12 interviews for fairly homogeneous groups (Guest et al., 2006; Hennink et al., 2017; Hennink & Kaiser, 2022); meaning saturation may need more; information power depends on a narrow aim and specific sample (Malterud et al., 2016); sample sizes in information systems interview studies vary by method and should be justified (Marshall et al., 2013). Participants gave structured feedback on Feasibility (applicable in practice) and Completeness (missing key components) and made open-ended comments. The thematic content analysis of their answers was conducted using NVivo. An NVivo coding method was adopted to identify recurring topics, which were assigned to emergent themes such as performance, security, environmental robustness, policy, and simulation validity, and so on. The author coded it uniformly, and it was checked for clarity. The inter-coder reliability was not calculated due to the small sample size of experts. The themes that arose were directly reflected in the proposal for adaptive weighting (Artefact 1→ Artefact 2) and in the final design changes for Artefact 3.

5.3 EXPERT EVALUATIONS

This section outlines and analyses the expert feedback. It outlines the nine experts' feedback in three main structures, which are important criteria for expert selection, positive and negative concerns from the industrial perspective. The three structures are their role summary in the industry, the positive points, and the concerns/limitations informed by their feedback. The survey was deliberately short, with structured ratings of feasibility and completeness and an open comment item ('Other comments?'), so practitioners from machinery operators to biometric researchers could answer quickly without specialist vocabulary (Dillman et al., 2014; Krosnick, 1999). The study is socio-technical (Bostrom & Heinen, 1977; Sarker et al., 2019). Short questions allowed no follow-up probing and recommend semi-structured follow-up interviews. A summary of the role, key strengths found in the design, main concerns, and implications for the architecture of Artefact 3 (A3) of each expert is summarised below.

5.3.1 Expert 1: Field Operator (Industrial/Construction Worker)

This Subsection presents an industrial expert 1 review and presents its NVivo word focus in Figure 5.1.

- ***Role summary**:* Trained and experienced heavy equipment operator, with a background in logistics and construction (15+ years).
- ***Positive points:*** The design considers the conditions on site, including helmets, masks, lighting conditions, and mobility of the user. The design of the intention to recognise workers on their way to work was considered a useful advantage.
- ***Concerns/limitations:*** Speed is of critical importance: the recognition has to be almost instantaneous, without stopping workers. It was emphasised that they have to be robust to dust, noise, rain, and other "messy" environments, or they will not be used.
- ***Implications for Artefact 3**:* highlighted is the real-time processing, motion-tolerant recognition. Essential to incorporate high-quality pre-processing sensors to minimise environmental noise (e.g., denoising and robust feature extraction) and accommodate PPE-related occlusion. Set explicit latency goals (≤300ms/ per modality at the edge, < 1s/ end-to-end). Use ruggedised sensing and adaptive filtering where possible to deal with weather and dust.



Figure 5.1 NVivo coding word focus for expert 1

5.3.2 Expert 2: IT security (Adaptive Authentication Specialist)

This Subsection presents an industrial expert 2 review and presents its NVivo word focus in Figure 5.2, which focuses on authentication.

- ***Role summary:*** An IT security professional with a PhD speciality in Biometric authentication and Adaptive security.

- ***Positive points****:* The expert agreed with the overall direction of the work that has been created, which is adaptive and context-aware, and commented on the progression from the earlier artefacts Artefact 1 to Artefact 2, that this was coherent. It was determined that one of the key and useful innovations is the adaptive weighting engine.
- ***Concerns/limitations:*** The expert recommended the integration or the use of strict, challenging evaluation, including explicitly anti-spoofing and liveness strategies, before rollout.
- ***Implications for Artefact 3****:* the addition of presentation attack detection (PAD) for different modalities (e.g., face, voice) is necessary in accordance with ISO/IEC 30107. Develop and test against spoofing and deepfake cases, and enhance the trust-validation process, including the use of challenge–response and texture-based methods. Identify low-confidence cases using fusion outputs and initiate more checks if needed.



Figure 5.2 NVivo coding word focus for expert 2

5.3.3 Expert 3: IT Security (IAM Specialist)

This Subsection presents an industrial expert 3 review and presents its NVivo word focus in Figure 5.3, which focuses on policy and access.

- ***Role summary:*** A Security Engineer with 15+ years' experience and a Full Stack Developer specialising in Identity & Access Management (IAM).
- ***Positive points:*** The expert found the approach to be compatible with current IAM practice and highlighted that a policy layer that connects biometric outcomes to access control is important and achievable.
- ***Concerns/limitations:*** The expert suggested the need for a better handling of policy conflict resolution (e.g., if multiple policies conflict, how does it

operate) and recommended aligning with known standards, such as ISO/IEC 27001.

- ***Implications for Artefact 3****:* Create a policy engine that can deal with conflicting policies (e.g., priorities, deny-overrides, or negotiated paths to decisions). Implement audit logging and retention measures consistent with the ISO/IEC 27001 standard and explicitly define access-control policies – including escalation policies – such as when to resort to secondary biometrics. Protect policy data and biometric templates in a secure, encrypted manner that meets privacy expectations.



Figure 5.3 NVivo coding word focus for expert 3

5.3.4 Expert 4: Biometric Systems (Academic)

This Subsection presents an industrial expert 4 review and presents its NVivo word focus in Figure 5.4, which focuses on biometric, adaptation and system.

- ***Role summary****:* Academic researcher/doctor in the field of biometric systems engineering.
- ***Positive points****:* Multimodal biometrics (face, ear, and voice) is a solid approach, and the use of 'context-driven adaptation' is a valuable contribution, according to the feedback from the expert.
- ***Concerns/limitations:*** The expert stated that more transparency with per-modality confidence scores (visibility of the reliability of each modality at decision time) would be helpful.
- ***Implications for Artefact 3:*** Give confidence scoring for each biometric match, instead of just a binary decision (such as saying "Face: 0.87, Voice: 0.65"). These values help guide adaptive weighting, user messaging, and auditing. Keep logs of confidence, include contributions in the logs, and explore ways to explain the decisions, such as which modality led to acceptance or rejection.

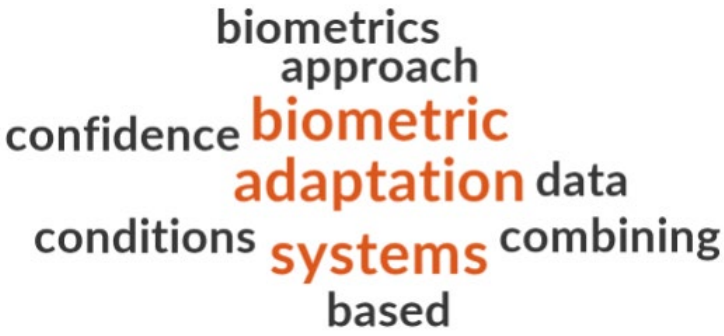


Figure 5.4 NVivo coding word focus for expert 4

5.3.5 Expert 5: Applied IT Security

This Subsection presents an industrial expert 5 review and presents its NVivo word focus in Figure 5.5, which focuses on attacks.

- ***Role summary:*** Security penetration tester specialising in practical attack pathways.
- ***Positive points:*** The expert views that executing the overall artefact is possible if security testing and mitigations were viewed as first-class design requirements and not just an afterthought.
- ***Concerns/limitations:*** the design needs to be more detailed concerning attack resistance, especially spoofing, replay, and deepfakes. The expert added that if there were no specific countermeasures or testing proof, then the authentication surface could still be compromised.
- ***Implications for Artefact 3:*** Concrete defence measures: face liveness check, voice anti-spoofing (to detect synthesised voice/replayed voice), liveness measure of other traits (where applicable). Discuss the hardware-assisted checks (e.g., illumination of IR) and challenge/response mechanisms. Consider anomaly detection of unusual access patterns and design an adversarial test suite as a part of validation.



Figure 5.5 NVivo coding word focus for expert 5

5.3.6 Expert 6: IoT Systems Engineer

This Subsection presents an industrial expert 6 review and presents its NVivo word focus in Figure 5.6, which focuses on IoT.

- ***Role summary:*** IoT and embedded systems engineer with experience in edge deployments.
- ***Positive points:*** The expert agreed that the concept aligns well with IoT constraints and supported explicit context handling for environmental variability.
- ***Concerns/limitations:*** Latency and processing locality were considered a given: the expert warned that IIoT environments aren't going to be able to rely on guaranteed cloud round-trip times, especially in environments where connectivity is not guaranteed.
- ***Implications for Artefact 3:*** Use an edge-first approach to deploy recognition modules in local gateways or on device processors to get sub-300ms latency. Reduce the number of cloud round-trips; use cloud for non-real-time storage and analytics. Optimise for non-constant connectivity with lightweight models, and asynchronous pipelines (sensor → edge AI → central services).



Figure 5.6 NVivo coding word focus for expert 6

5.3.7 Expert 7: Virtual Reality (VR) Specialist

This Subsection presents an industrial expert 7 review and presents its NVivo word focus in Figure 5.7, which focuses on simulation.

- ***Role summary:*** VR systems designer and Game developer.
- ***Positive points:*** The expert agreed/liked the use of Second Life, considering it as an early-stage testbed, and suggested that avatars can be helpful to explore Second Life workflow and fusion behaviour under controlled constraints.

- ***Concerns/limitations**:* The expert highlighted that the validity of the simulation needs to be explicitly validated with real sensing and operational data to ensure that the benefits of the simulation can be transferred beyond VR.
- ***Implications for Artefact 3:*** Use VR to verify fusion logic and user-flow assumptions but introduce real-world trials early. Where possible, calibrate simulation parameters (lighting, motion, occlusion) against sensor measurements from target sites, and document which assumptions remain unvalidated.



Figure 5.7 NVivo coding word focus for expert 7

5.3.8 Expert 8: Industrial IoT Architect

This Subsection presents an industrial expert 8 review and presents its NVivo word focus in Figure 5.8, which focuses on industrial.

- ***Role summary:*** PhD candidate in the field of IIoT specialists in Industry 4.0 architectures.
- ***Positive points:*** The expert stated that there was good relevance with the smart factory environment and endorsed the focus of modelling constraints in the environment.
- ***Concerns/limitations:*** Legacy integration: There are many industrial systems (such as PLCs and SCADA environments) that may not be able to handle modern biometric workflows without the need for intermediate gateways and engineering.
- ***Implications for Artefact 3:*** Add explicit integration patterns (such as gateways, protocol adapters, etc.) to connect to legacy equipment. Ensure the system has a modular interface and configurable options to match the site's policies, constraints, and limitations.



Figure 5.8 NVivo coding word focus for expert 8

5.3.9 Expert 9: Site Security Officer (Construction)

This Subsection presents an industrial expert 9 review and its NVivo word focus in Figure 5.9, which focuses on many words, for example, security, helmet, fast, people, and so on.

- ***Role summary****:* Construction site security supervisor responsible for day-to-day access control.
- ***Positive points****:* The expert saw potential in the approach if it can be maintained to be simple and quick to operate, and added that PPE-aware design would be better than what is currently being done on site.
- ***Concerns/limitations****:* The expert reiterated that it must be fast and simple if it is to be adopted. The system must be reliable when faces are partially obscured, as this is a common occurrence and will likely lead to workarounds during operation.
- ***Implications for Artefact 3:*** Avoid interaction patterns that lead to workers stopping and minimise user extra effort for authentication. Identify step-up pathways for exceptions (e.g., supervised fallback enrolment and verification) and, where possible, prioritise modalities that are not negatively affected by occlusion, such as ear and voice.



Figure 5.9 NVivo coding word focus for expert 9

5.4 THEMATIC ANALYSIS

Expert feedback was thematically coded using NVivo software, and the following areas were highlighted: labelled themes, experts who raised them, frequencies (number of experts), and paraphrased statements as illustrations. The last column of Table 5.2 summarises how each theme influenced the Artefact 3 design to overcome the identified instability zone and transition toward adaptive resilience. Chapter 5 will collect expert reviews to define Artefact 3 (A3) of this study. Table 5.2 below presents the thematic analyses derived from the expert feedback and their implications for the new iteration and redesign of the artefact.

Table 5.2 Thematic review/analysis of the 9 expert reviews using NVivo

Theme	**Experts 1 - 9**	**Illustrative Expert Comment Coded from Expert 1 - 9**	**Artefact 3 Design Implications**
Adaptive Weighting and Context Awareness	2,4,6	2(The architecture aligns well with adaptive authentication frameworks. The integration of context-awareness is particularly strong, your adaptive weighting engine is the strongest contribution),4(Weight adaptation based on environmental conditions is scientifically sound. I would suggest adding confidence scoring transparency), 6(Yes. The system fits well within IoT ecosystems where devices need contextual authentication),	Keep adaptive weight engine. Model constraints quantitatively. Tune weights inversely to modality degradation. Use RL or dynamic selection to adjust modality contributions.
Anti-Spoofing and Attack Resistance	2,5	2(However, I would recommend incorporating adversarial testing—particularly spoofing resistance), 5(How does it handle spoofing? Deepfakes? Replay attacks? If this isn't addressed, attackers will exploit it)	Incorporate PAD modules per ISO/IEC 30107: face liveness CNNs, voice anti-spoof nets, challenge-response. Log confidence to catch anomalies.
Edge vs Cloud Processing	1,6,9	1(but only if it works fast and doesn't slow us down. On-site, we don't have time to stand still for scans.),6(Latency and edge processing need consideration. Industrial IoT systems cannot rely heavily on cloud delays),9(If it's simple and fast, yes.)	Process biometrics at the network edge, where possible. Use cloud for non-real-time tasks (analytics, storage). Optimise task scheduling across edge nodes. This will make it faster
Environmental Robustness & PPE	1,4,6,7,8,9	1(You've thought about helmets, masks, lighting—that's real life for us. Most systems ignore that. And dust, noise, rain. If it fails when things get messy, people won't use it),4(Very strong. Combining ear, speech, and facial data is a robust approach and	Use sensors robust to occlusions (e.g. ears, gait), noise filtering, and adaptive vision algorithms. Include PPE detection sensors. Test in dust/rain conditions.

		Weight adaptation based on environmental conditions is scientifically sound. I would suggest adding confidence scoring transparency),6(particularly in handling environmental constraints),7(Simulation validity is strong, but real-world transferability must be validated beyond VR),8(Yes, and highly relevant for Industry 4.0 environments),9(We deal with people wearing PPE all the time. If your system works with helmets and masks, that's a big win)	
Explainability and Confidence	4 & 5	4(Weight adaptation based on environmental conditions is scientifically sound. I would suggest adding confidence scoring transparency), 5(How does it handle spoofing? Deepfakes? Replay attacks? If this isn't addressed, attackers will exploit it)	Output per-modality confidence and decision reasoning. Provide interpretable scores to meet audit/compliance needs. Use explainable AI techniques for critical decisions
Multimodal Integration	4 & 7	4(Multi-modal biometrics is already proven), 7(Simulation validity is strong, but real-world transferability must be validated beyond VR)	Continue using the four primary modalities (face, gait, voice, ear) plus the fallback modalities (iris, fingerprint, Palmprint). Ensure modality complementarity. The fusion scheme dynamically uses all relevant modalities.
Policy & Compliance	3 & 8	3(The policy layer you included is critical and realistic & though I would like to see more detail on policy conflict resolution),8(However, integration with legacy industrial systems will be a challenge)	Implement a formal policy engine with conflict-resolution rules. Ensure ISO 27001-aligned controls (logging, encryption). Design pluggable modules for legacy protocols.
Real-time Performance and Latency	1,3,6,7,8,9	1(if it works fast and doesn't slow us down. On-site, we don't have time to stand still for scans & If your system can recognise someone even when they're moving or wearing gear, then it fits	Prioritise low-latency edge computing. Set targets (~100–300 ms per recognition). Use lightweight models and asynchronous processing.

		reality), 3(The policy layer you included is critical and realistic), 6(Latency and edge processing need consideration. Industrial IoT systems cannot rely heavily on cloud delays), 7(Simulation validity is strong, but real-world transferability must be validated beyond VR), 8(Yes, particularly the environmental constraint modelling & however, integration with legacy industrial systems will be a challenge), 9(If it's simple and fast, yes)	
Simulation vs Reality	7, 8	7(Yes, especially using platforms like Second Life for simulation), 8(However, integration with legacy industrial systems will be a challenge)	Use VR for initial prototyping only. Plan early, real-world trials. Treat simulation as hypothesis generation; calibrate the system with live data.

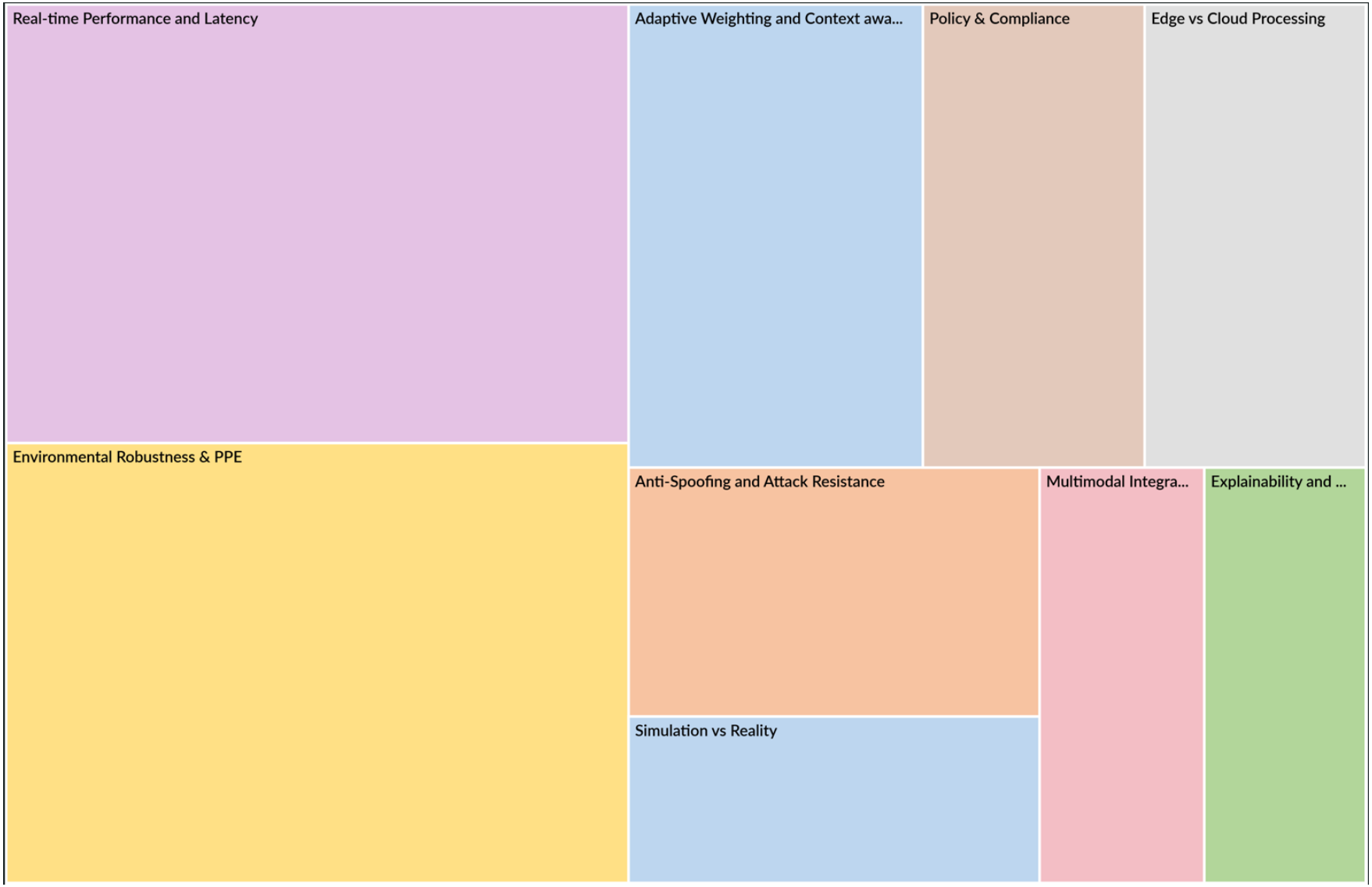


Figure 5.10 NVivo Expert Review Theme context chart showing major theme focus as different size area

5.4.1 Thematic Theme Reviews

This study employed thematic analysis within the framework of qualitative research, using NVivo software and a qualitative coding methodology to analyse the experts' comments, grouping related conceptual themes by frequency of mention, technical significance, and relevance to the proposed development of new Artefact 3 (A3).

The findings of the Expert Review were analysed using a thematic analysis inspired by NVivo's qualitative coding methodology. During analysis, the Reviewers' comments on the proposed framework were grouped into recurring conceptual themes. Based on the findings, the main architectural, operational, security, and usability issues were identified, providing the basis for redesigning the proposed adaptive biometric authentication framework, Artefact 3. The corresponding analysis yielded nine main themes, which the author reviewed.

5.4.1.1 Adaptive Weighting and Context Awareness

Adaptive weighting and context awareness. This was one of the strongest points of the proposed framework for the experts at 2, 4, and 6. The static fusion architecture of the proposed framework, implemented in Artefact 2, is best suited for real-world deployment as an adaptive biometric weighting and fusion system for authentication.

This set of themes relates to the comments of Experts 2, 4, and 6, who emphasised the importance of adaptive biometric weighting. The architecture of the study "aligns well with adaptive authentication frameworks" (Expert 2). The adaptive weighting engine in the proposed framework is the study's strongest contribution. The weight adaptation based on environmental conditions is scientifically sound (Expert 4). There is a growing need for contextual authentication in IoT environments (Expert 6). The thematic interpretation of the findings from Experts 2, 4, and 6 reveals that they consider environmental responsiveness a core aspect of IIoT authentication. The findings of the experts from Experts 2, 4, and 6, therefore, support the analysis of Artefact 2 and the limitations identified.

Future adaptive authentication systems will use reinforcement learning or fully leverage an AI-based decision system to continuously learn and optimise the best combination of biometrics for recognition, thereby enabling the core architecture of the Artefact 3 framework. Figure 5.11 shows the NVivo project map illustrating the relationship between expert interview participants, coded qualitative data, and the

emergence of the central theme "Adaptive Weighting and Context Awareness." The figure demonstrates how three experts, namely experts 2, 4 and 6, gave one contribution each to the subject of focus, Adaptive Weighting and Context Awareness. Multiple expert perspectives converged through thematic coding to inform the design of the proposed adaptive contactless biometric authentication framework.

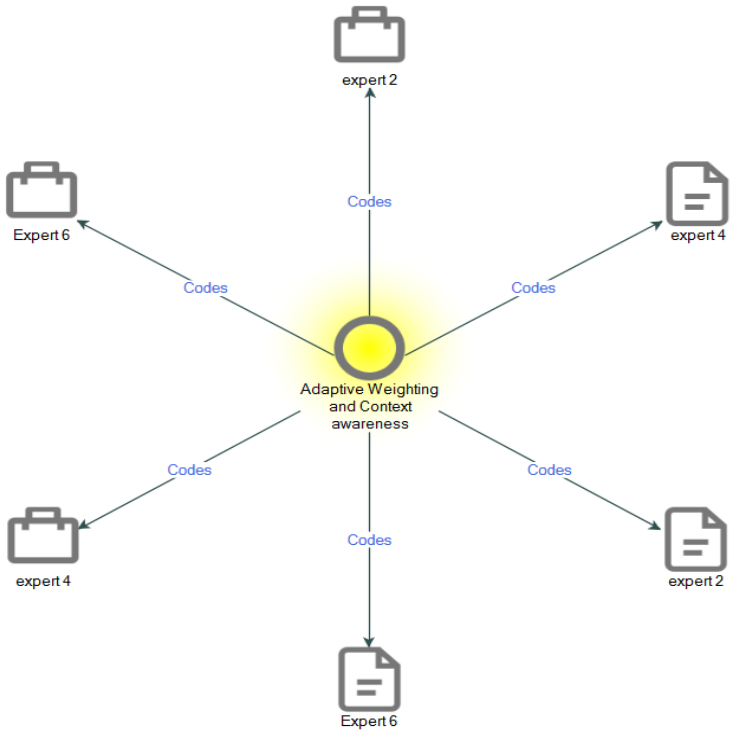


Figure 5.11 Adaptive Weighting and context awareness, NVivo expert coding

5.4.1.2 Anti-Spoofing and Attack Resistance

The second major theme found in the experts' comments was their views on how the Artefact 3 framework for intelligent multimodal biometric authentication, for secure and reliable access control in the industry of the future, could and/or should be improved with respect to biometric anti-spoofing and attack resistance.

Experts 2 and 5 expressed concerns about the security of biometrics, including the potential for fraud, spoofing, and attacks, as well as their possible misuse through so-called deepfakes or replay attacks. Expert 5 pointed out that future developments of the adaptive authentication architecture have to include “mechanisms for adversarial resistance”. Even though the adaptive authentication architecture is technically strong, it lacks practical spoof-resistance.

This theme has exposed a hard truth. Recognition quality alone is not sufficient for industrial biometric systems to function reliably. They must also authenticate the

biometric sample as real (i.e. genuine) or fake (i.e. spoofed). That is, they need to check for liveness. That is what Artefact 3, which forms the third part of the proposed Artefact 3 framework, addresses. Consequently, Artefact 3 evolved to include: Presentation Attack Detection (PAD), face liveness detection, voice anti-spoof neural networks, challenge-response verification, and confidence anomaly monitoring.

The experts' concerns about spoofing highlighted the need for industrial biometric systems to be compliant with the ISO/IEC 30107, which defines behaviours of a spoof attack and an attackable presentation in the context of Presentation Attack Detection. This theme strengthened the security dimension of the Artefact 3 framework, transforming it into a security-aware biometric system for industrial applications (Artefact 3). Figure 5.12 shows that Experts 2 and 5 each contributed one theme to the NVivo thematic coding, illustrating the relationships among expert interview participants, coded qualitative data, and the emergence of the central theme, Anti-Spoofing and Attack Resistance.

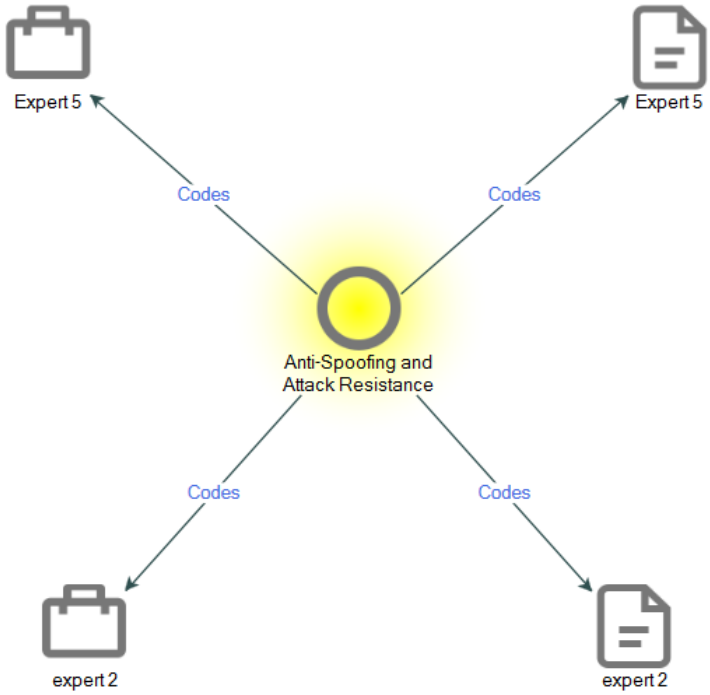


Figure 5.12 Anti-Spoofing and Attack Resistance NVivo expert coding

5.4.1.3 Edge versus Cloud Processing.

Experts 1, 6, and 9 outlined the issues related to the speed, simplicity, and low latency of authentication systems in industrial environments. They could not emphasise enough that any biometric system must be so simple that, even after a scan, employees can continue their work immediately. If not, then other authentication methods are

preferred. Also, the employees should not have to stand still for the scan. In industrial IoT environments, similar constraints must be taken into account; therefore, cloud-based verification processing alone is not suitable, as it introduces excessive latency. The usability and or efficiency of operation of a system has become a critical element of performance or operation of a system for the purpose of industrial authentication.

There was also mention of the potential for low latency to increase worker acceptance of a system, as it would not impact their workflow as much as a system that requires a lot of latency. This theme, therefore, pushed the framework towards A mixture of edge-based and cloud biometric processing, local decision execution, distributed authentication nodes, and cloud-independent verification.

For this theme, within Artefact 3, an edge-computing-based authentication layer is to be created that performs real-time biometric fusion, making the authentication seamless. Cloud systems were repositioned toward analytics, long-term storage, model training, and system auditing, rather than primary authentication execution. Figure 5.13 shows that Experts 1, 6, and 9 each contributed one theme to the NVivo thematic coding, illustrating the relationships among expert interview participants, the coded qualitative data, and the emergence of the central theme Edge versus Cloud Processing.

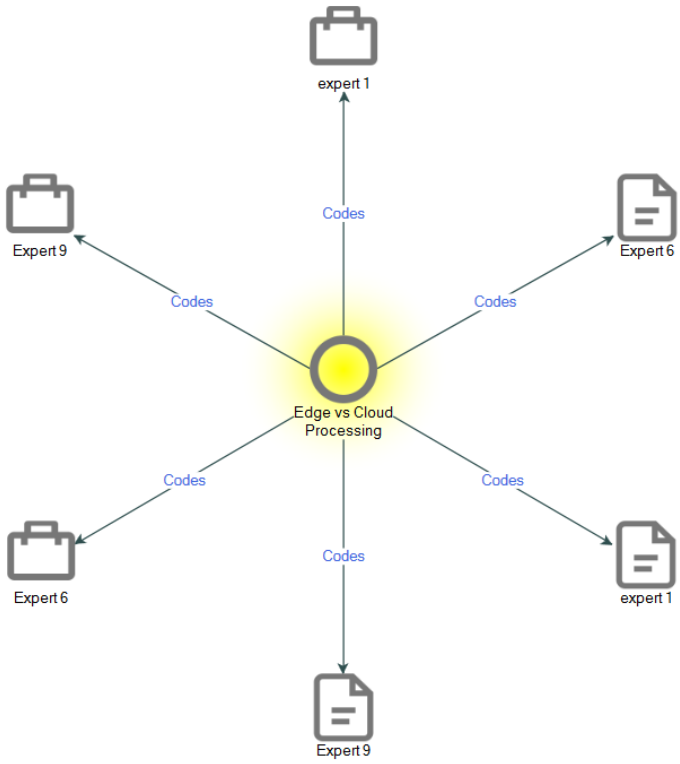


Figure 5.13 Edge versus Cloud Processing NVivo expert coding

5.4.1.4 Environmental Robustness and performance under personal protective equipment (PPE) Constraints

Environmental robustness was one of the major themes to come up in the expert reviews of the artefacts under consideration. The authentication system must function across a range of environmental conditions. Except for Experts 2, 3 and 5, who made no mention of this theme, all the experts agreed that this situation represented an important design situation for the authentication system. The Constraint situations were represented by all the experts to varying degrees as important for the design of the authentication system, and were noted by Experts 1, 4, 6, 7, 8, and 9.

They need to work when things go wrong, and if it fails when things get messy, people won't use it. This is already happening daily on sites Expert 9 travels to when PPE-based obstruction occurs. Thematic analysis of experts' views highlighted that the main challenge for the industrial application of biometric authentication systems is to ensure their environmental adaptability.

This theme is also strongly supported by the report for Artefact 2, the practical investigation of the authentication performance in industrial environments through simulation using Second Life. This report showed that the effect of individual constraints on the system's performance for correctly identifying a user increased exponentially with the number of constraints applied.

The experts therefore supported: robust multimodal sensing, occlusion-resistant biometrics, adaptive computer vision, environmental condition monitoring, and dynamic filtering systems. Consequently, Artefact 3 would incorporate: PPE detection modules, adaptive vision systems, noise filtering, environmental sensing, and fallback modality escalation. This theme also became the core of the Artefact's practical use in industry. Figure 5.14 shows that Experts 1, 4, 6, 7, 8, and 9 each contributed one theme to the NVivo thematic coding, illustrating the relationships among expert interview participants, the coded qualitative data, and the emergence of the Environmental Robustness and PPE Constraints.

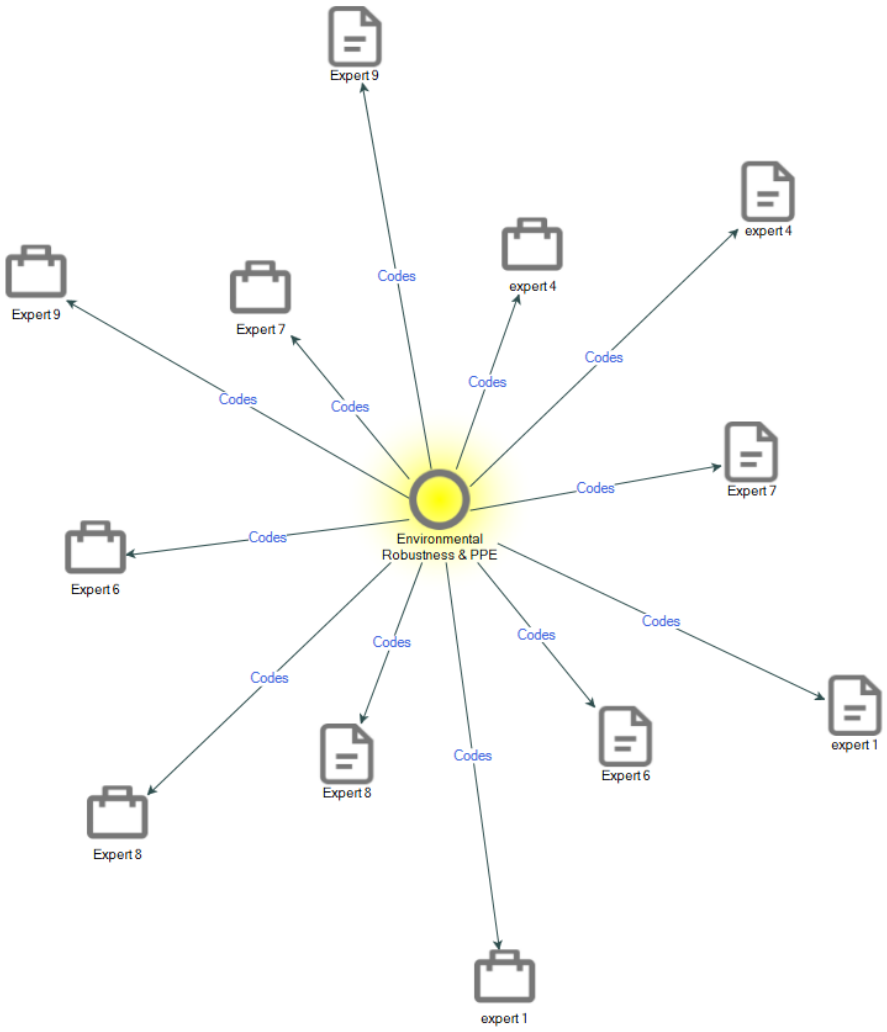


Figure 5.14 Environmental Robustness and PPE Constraints NVivo expert coding

5.4.1.5 Explainability and Confidence Transparency

The fifth theme covers issues of transparency, interpretability and explainable decision-making when implementing an authentication system. Experts 4 and 5 also noted that, when designing highly adaptive systems for AI-based authentication, confidence transparency must be included in the adaptive fusion process. Experts 4 and 5 emphasised the need for confidence and transparency in highly adaptive AI-based systems, such as within the adaptive fusion process. Why was access granted? Why did a modality fail? Or how were weighting decisions made? are questions the system should be able to answer.

The thematic analysis of experts' comments has identified a growing concern about the lack of explainability in new AI-driven security systems. These concerns regarding the explainability of highly adaptive systems, identified in this theme, are also reflected in current discussions on Explainable AI (XAI) in cybersecurity and in

the governance of biometrics. As a result, Artefact 3 is to be introduced: per-modality confidence scoring, explainable fusion reasoning, audit logs, and decision transparency layers.

In summary, these tools will allow an administrator or auditor to gain more insight into a user's authentication behaviour. The inclusion of explainability in authentication mechanisms in an industrial security system helps meet auditing requirements and build trust in the system. Figure 5.15 shows that Experts 4 and 5 each contributed one theme to the NVivo thematic coding, illustrating the relationships among expert interview participants, the coded qualitative data, and the emergence of the Explainability and Confidence Transparency.

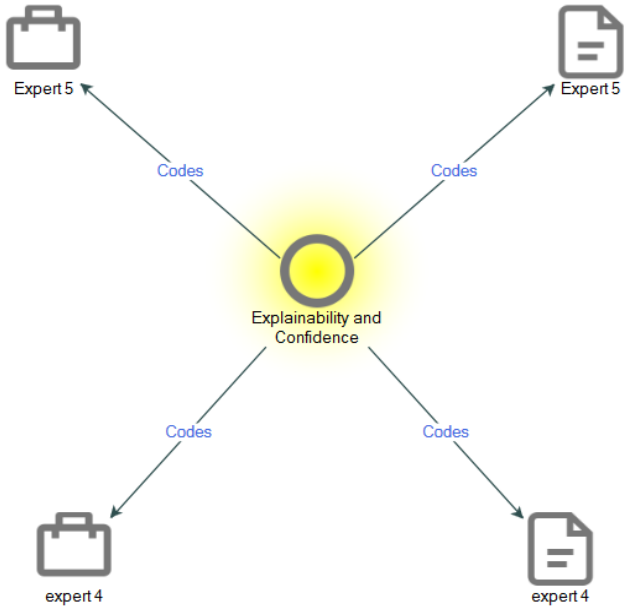


Figure 5.15 Explainability and Confidence Transparency NVivo expert coding

5.4.1.6 Multimodal Integration

Two of the experts (4 and 7) agreed with the current status of multimodal biometric integration in industrial security systems. As previously stated in Theme 5, no single modality is expected to perform perfectly across all possible scenarios in an industrial scenario. Thus, the use of multi-modal biometrics has already been proven by Expert 4 and agreed upon by Expert 7 in simulations performed in virtual environments to analyse different scenarios. Redundancy and Complementarity between different biometric modalities are strengths of multimodal systems (Thematic Interpretation for Theme 6).

The findings from this Theme are used to further validate the work from the previous two Artefacts. That is, to strengthen the architecture and agree on the work from the previous Artefacts, and then to design the system adaptively for the final Artefact. Figure 5.16 shows that Experts 4 and 7 each contributed one theme to the NVivo thematic coding, illustrating the relationships among expert interview participants, the coded qualitative data, and the emergence of the Multimodal Integration.

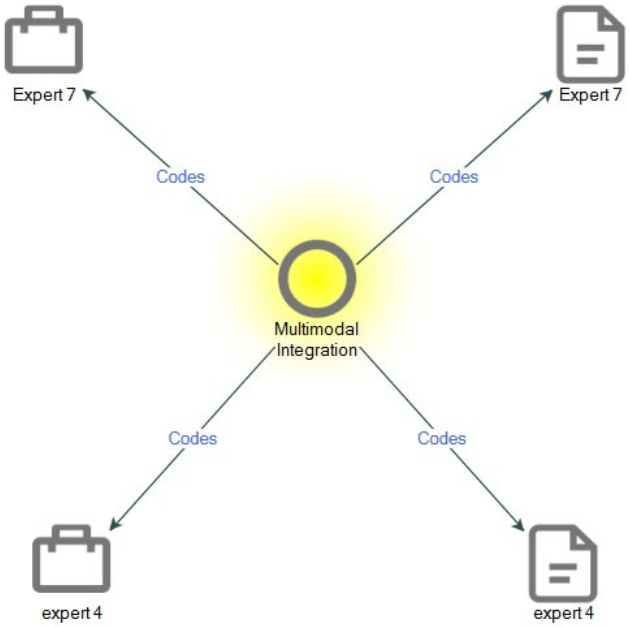


Figure 5.16 Multimodal Integration NVivo expert coding

5.4.1.7 Policy and Compliance Integration

Expert 3 focused on the issues of governance, interoperability and compliance of industrial systems in contrast to the usual biometric authentication systems. Expert 8 also focused on similar issues. Expert 3 (biometric expert, law enforcement) was interested in the governance, policy and compliance aspects for a real-world deployment. In particular, Expert 3 highlighted the importance of the policy layer and required more detail on how conflicts would be solved. Expert 8 (industrial security expert) highlighted the difficulties of integrating modern biometric systems with the legacy industrial security infrastructures.

The analysis of this theme's findings also revealed that experts considered governance integration into the system to be very important to deploy it in real-life

scenarios. Accurate technical output is not enough; the system also has to integrate with organisations' security policies and the operational ecosystem of industries. As a result, Artefact 3 is to be introduced: policy conflict-resolution engines, access governance modules, encryption controls, audit logging, and ISO 27001-aligned authentication policies. The architecture also supports very old industrial systems by adding pluggable integration layers. This theme explores a more enterprise-ready framework. Figure 5.17 shows that Experts 3 and 8 each contributed one theme to the NVivo thematic coding, illustrating the relationships among the expert interview participants, the coded qualitative data, and the emergence of the Policy & Compliance theme.

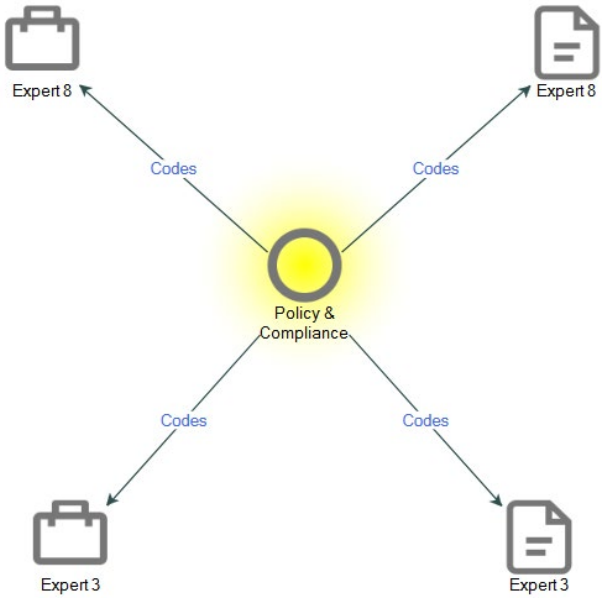


Figure 5.17 Policy & Compliance NVivo expert coding

5.4.1.8 Real-Time Performance and Latency

Real-time authentication performance is another very important operational theme for most of the experts. Experts 1, 3, 6, 7, 8 and 9 described the need for real-time authentication when employees are on the move or working in processes within the industry. Therefore, it is considered a low-latency authentication criterion for IIoT that is easily applicable in practice.

The experts further described the relationship between a system's real-time performance and low latency and workers' acceptance of that system. This connection is described in the next sentence of text in the Experts' Comments column for theme

8 (Table 5.2). Thematic analysis of this Theme for low-latency IIoT authentication for the industrial enterprise also identified the means to achieve it. This has led to the inclusion of Artefact 3: lightweight biometric models, asynchronous processing, edge-based fusion, and low-computation adaptive algorithms. This theme reinforced the study's emphasis on balancing usability, security, and operational continuity. Figure 5.18 shows that Experts 1, 3, 6, 7, 8 and 9 each contributed one theme to the NVivo thematic coding, illustrating the relationships among the expert interview participants, the coded qualitative data, and the Real-time Performance and Latency theme.

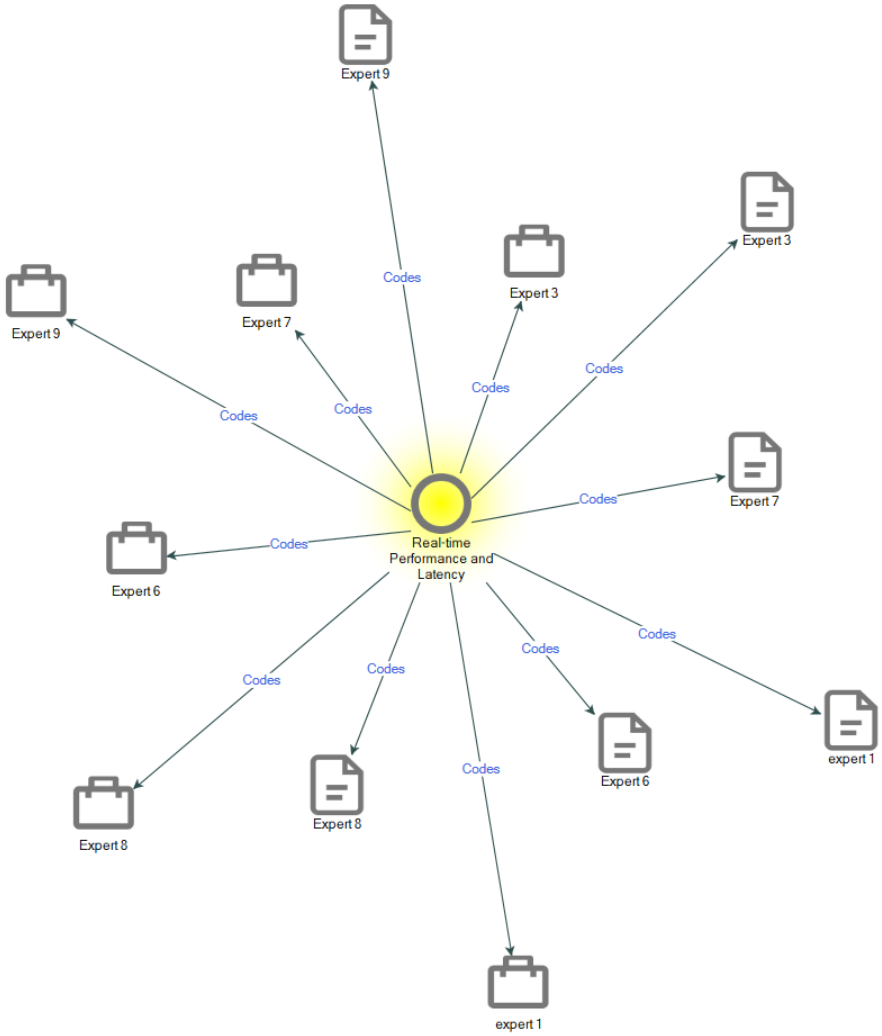


Figure 5.18 Real-time Performance and Latency NVivo expert coding

5.4.1.9 Simulation versus Reality

Experts 7 and 8 agreed that the Second Life simulation was useful for researchers to test hypotheses and that recognition could be tested in a controlled way, however, they agreed that, in the end, testing would have to be conducted in the real industrial

environment. Expert 7 and Expert 8 agreed that simulation of physical environments, such as Second Life, was a useful tool for prototyping, testing hypotheses, and so on, and that these need to be tested in real industrial environments in the end. This theme, therefore, validates the use of Design Science Research in this study while highlighting where further validation is needed. As a result, the study acknowledged that Second Life effectively supported controlled experimentation, behavioural simulation, and environmental modelling.

This confirmed the earlier observations that Second Life supported (live) testing of designs in a virtual environment, but that, in the end, only live testing in the physical industrial environment counted. This theme exposed several of the study's limitations and, as with all the other themes in this thematic analysis, strengthened the study's credibility and transparency. Figure 5.19 shows that Experts 7 and 8 each contributed one theme to the NVivo thematic coding, illustrating the relationships among the expert interview participants, the coded qualitative data, and the Simulation vs Reality theme.

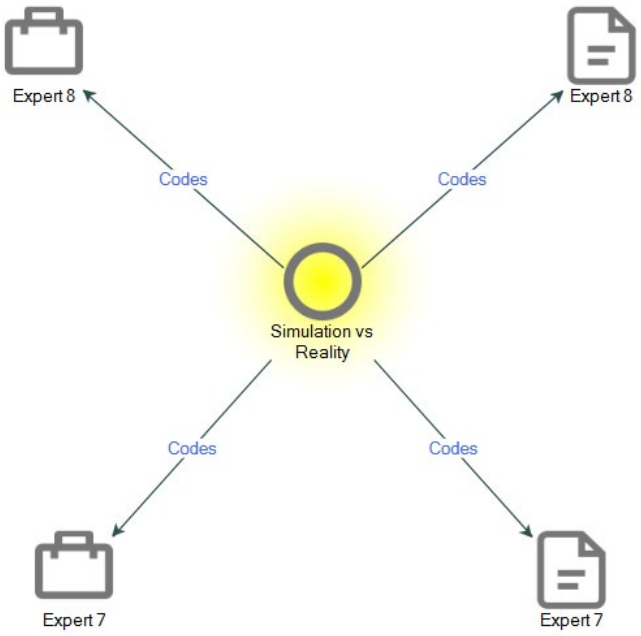


Figure 5.19 Simulation vs Reality from NVivo expert coding

5.4.2 General Conclusion of the Thematic Review

The main finding of this thematic review across all themes is that there is an overwhelming consensus that experts designing biometric systems for the Industrial Internet of Things (IIoT) need to develop adaptive, context-aware, and environmentally resilient authentication systems. All of the points identified in the

thematic review by the experts of this study project pointed in the same direction. The design of adaptive systems adapts to the many constrained situations encountered in real life. Therefore, all the experts in the thematic review rejected the idea of static authentication architectures and instead sought intelligent, adaptive systems. A summary of the key requirements for the future IIoT biometric systems to be effective is adaptive weighting, environmental awareness, multimodal redundancy, spoof resistance, explainability, low-latency edge processing, policy integration, and real-world operational robustness.

The review is intended to significantly influence the major iterative developments between Artefacts 1 and 2, during which the framework for a static biometric fusion-based artefact has matured into an adaptive, intelligent industrial authentication architecture. In addition to conventional security accuracy measures (FAR, FRR, etc.) for industrial biometric systems, a variety of other factors must be addressed, including usability, worker movement, environmental variability, continuity of operation in the event of system failure, and organisational issues.

The findings from the thematic review support the central argument of this thesis: that Biometric authentication for IIoT environments moves beyond traditional static fusion models and needs to be developed into an adaptive, explainable, context-aware, and human-centred authentication ecosystem. Figure 5.20 shows NVivo Word focus for the thematic analysis, which shows the main word Security, and sub focus words like authentication, industrial, IoT and Biometric.



Figure 5.20 word focus for the thematic analysis from NVivo

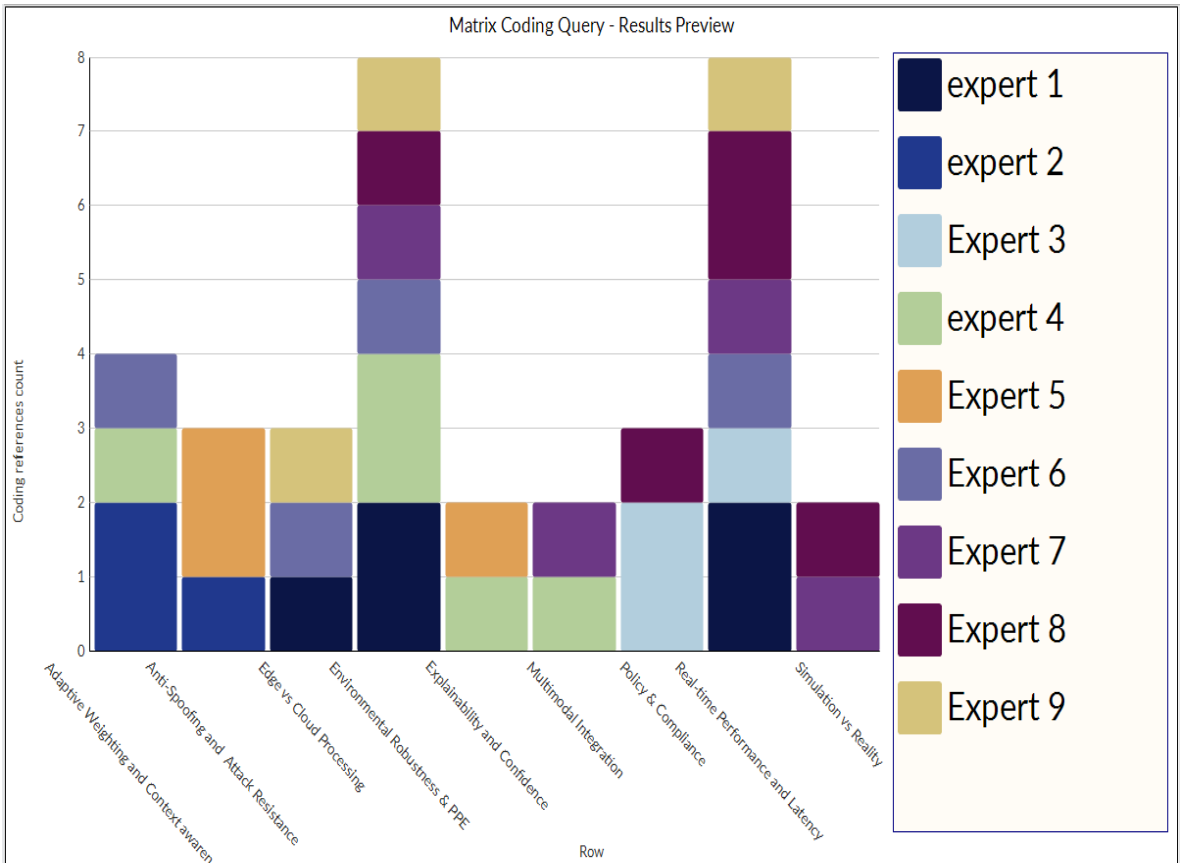


Figure 5.21 Thematic analysis from NVivo Matrix Coding

5.5 ARTEFACT 3 (A3) ARCHITECTURE SPECIFICATION

The expert review and thematic analysis have resulted in Artefact 3 (A3) being identified as a modular layered architecture. The design keeps four main modalities (face, gait, voice, ear) and three fall-back modalities (iris, fingerprint, palm print) and focuses on an adaptive fusion core that adapts decisions according to context and modality confidence.

5.5.1 Sensor/Input layer

There are several sensors that capture raw biometric and contextual data, such as cameras for face recognition, for gait recognition, microphones for voice capture, and ear scanning devices. Context sensors estimate the conditions in the environment (e.g., lighting, dust), and the use of personal protective equipment (PPE) (e.g., detection of the presence of a helmet/mask). Fallback sensors (iris cameras; fingerprint/palm scanners) are used only for step-up authentication in response to policy.

- **Preprocessing modules:** The input is normalised and filtered in the pre-processing modules to minimise the environmental noise. In the case of vision

streams (face, gait, and iris), the pre-processing could involve noise-cancelling, deblurring, and enhancement for low light, even in the presence of multispectral support if available. The noise-cancelled and segmented audio is fed into a feature extractor. If PPE is identified, the input is directed into the appropriate channels (e.g., ear or voice if the face is covered).

- **Recognition Modules:**
    - ***Face Recognition:*** variations are dealt with by a CNN, such as a ResNet-based or lightweight CNN trained on industrial data.
    - ***Voice Recognition****:* Liveness detection (anti-spoof CNN) is parallel to the playback /synthetic voice filter.
    - ***Ear Recognition****:* a CNN model based on ear shape for identification.
    - ***Gait Recognition****:* Pose estimation/silhouette CNN to recognise persons by body movements.
    - ***Fallback Traits:*** Under certain policy conditions (e.g., in a high-risk area, or after multiple mismatches), iris (near-IR camera with liveness checking) and Fingerprint/Palm (scanner + minutiae extractor) are activated

5.5.2 Adaptive Fusion Layer

This is a critical unit which integrates modality scores to obtain an overall decision for authentication. The fusion is context and problem-dependent:

- **Weight Computation:** A dynamic weighting engine is used to give weights to each of the modalities' scores based on current constraints (e.g., face weights are less in low light). The degradation is inversely related to weights, meaning that reliable modalities get more influence.
- **Score Aggregation:** The scores are aggregated (summed and/or passed through a trained fusion network). It is not based on a threshold, but rather graded fusion (continuous confidence) as detailed in the equations adaptations found in artefact 2.
- **Adaptive Threshold**: The threshold for the decision itself adapts to the context (e.g., the threshold for the aggregated score is higher when there is an attack risk).

5.5.3 Decision and policy layer

The access decision generated by the fused score is matched to the rules in the policy. Site-specific requirements (e.g., “Gate entry requires face + voice”) are enforced by a rule-based engine (based on ISO/IEC 27001 principles), and in case of conflicting rules, it resolves the conflict. The results are access granted, access denied, or step up to fall back. A complete record of all decisions, even low-confidence denials, is recorded for traceability. Following IEC 62443 (IEC, 2009; IEC, 2020), the policy layer assigns each zone a target security level, applied here by analogy to physical access areas. The levels are illustrative. Real ones come from a risk assessment.

Table 5.3 Zones and security Levels

Zone	Target level	Authentication required	Fallback or step-up
Site gate	1–2	Unique identification and authentication (face, gait, ear)	Supervised check or badge
Hazardous areas, heavy plant	2–3	Biometric fusion; second factor for permit-to-work entry	Iris, fingerprint or palm print
Control room (SCADA/HMI, PLC engineering)	3	Fusion plus a possession factor	Iris or fingerprint, then supervisor
Safety system zone	3–4	Multifactor, possibly two-person, audited	Break-glass procedure
Remote and vendor access	3–4	Multifactor on untrusted networks	Not applicable

Adaptive weights shift influence between modalities according to context. Adaptive thresholds may tighten or relax with context but never below the minimum for the zone's level. When confidence is too low for a zone, the system steps up by requesting another factor and does not lower the threshold. Two biometric modalities count as one factor type under common definitions (Grassi et al., 2017), so zones at level 3 or 4 combine biometric fusion with a possession factor.

5.5.4 Data and management layer

A secured data store stores biometric templates, policy settings, and audit logs. Access is managed through the use of controls based on ISO/IEC 27001 (e.g., least privilege,

logging, and secure handling). In certain cases, when updates are provided for the model, only authenticated interactions are allowed. Explainability outputs (confidence scores, modality contributions) are kept for auditing and reviews after the incident.

5.5.5 Algorithms and Partitioning

In this subsection, a deep dive into the machine learning and anti-spoofing measures is proposed for Artefact3

- **Machine Learning Models:** Face/ear/gait recognition is done using CNN, voice recognition using LSTM-based or CNN with temporal modelling. Adaptive fusion can be learned via a reinforcement-learning agent (inspired by the Fusion Agent) or via LSTM ensembles, which enable learning optimal fusion weights conditioned on context.
- **Anti-Spoofing Measures:**
  - ***Face Liveness:*** A lightweight CNN (inspired by LwFLNet) to detect print/display attacks with the help of texture and depth cues.
  - ***Voice Spoofing:*** A neural model (complex-valued network) that is based on phase and spectral features for detecting deepfakes/replays.
  - ***Iris/Fingerprint:*** Hardware checks are enabled. (e.g. pupil reaction for iris, sweat pore analysis for finger) are enabled.

5.5.6 Edge vs Cloud

There are critical recognition modules deployed on local edge devices (camera units or gateways) to achieve latency requirements. Non-critical tasks (model retraining, long-term analytics) are carried out in the cloud. A scheduling mechanism distributes the tasks among several edge nodes to distribute the load and keep the response time within a range of about 100–300 ms, as suggested in the research for IIoT. A working combination of edge and cloud is below.

- **Latency Targets:** The targets of under 300 ms at the edge and under 1 s end to end are design goals derived from human response-time limits, under which about 1 s keeps a person's flow uninterrupted (Miller, 1968; Card et al., 1991; Nielsen, 1993), and from walking speed of about 1.3 to 1.4 m/s (Bohannon, 1997), so a decision comes within about a metre and a half of travel. About 700 ms of the 1 s budget remains for sensing, transmission and door actuation.

Edge processing avoids network delay and keeps biometric data on site (Satyanarayanan, 2017; Shi et al., 2016).

- **Data Flows:** (1) Sensors to pre-processing and then to Recognition Modules (in parallel). (2) For each module, a score and confidence are produced. (3) Context analyser (PPE information, weather, network status) provides information to the fusion engine. (4) Fusion engine calls a weighted sum. The policy engine is evaluated for the evaluation of the score and rules. (6) Outputs and logs of decisions are created. Secure channels (e.g., TLS) are used for communicating between layers.

5.5.7 Failure Modes & Mitigation:

Failure scenarios include Sensor Loss, Heavy Occlusion, Spoof Detected, and Policy Rule Problem. The system has the following mitigation:

- **Redundancy:** If one modality fails, then the other modalities with higher weights make it up for this.
- **Fallback:** If the level of confidence is low, or if a denial has been forced, fall back to another type of authentication (e.g., ask for a fingerprint).
- **Manual Override:** Security officer can override as a security measure, if necessary (logged for compliance).
- **Alerting*:*** When sensors fail and/or sensors are detected as attacked, it creates an alert to the admin.
- **Graceful Degradation:** If the pre-processing trait collected is very noisy, relaxed thresholds are implemented, and the use of multi-factor authentication is implemented if not entirely.

Table 5.4 expert feedback impacted on Artefact 3 design elements

Expert	Feedback (Paraphrased)	Artefact 3 Design Change
Field Operator	Must be fast; work in motion with PPE.	Use real-time edge processing, motion-tolerant sensors, and strong PPE handling.
Auth Systems	Include spoofing resistance.	Include one or more modules from each of the ISO/IEC 30107 PAD biometric standards.

IAM Specialist	This module focuses on detailed policy conflict resolution in terms of ISO 27001.	Introduce an in-depth policy engine and conflict rules; synchronise logs with ISO27001.
Biometric Prof	Add confidence and transparency.	Explainability scores (per-modality).
Red Team	Explain deep fakes/replay attacks.	Adversarial test plan on developing/Testing of Liveness/Anti-Spoofing Algorithms.
IoT Engineer	Think about latency, prefer the edge.	Implement biometric processing at the edge devices; optimise for a <300 ms response time.
VR Researcher	Validate beyond VR	Organise field tests; calibration of VR-models with real data.
IIoT Architect	Legacy system integration	Produce API adapters/Protocol Bridges for existing ICS systems
Security Supervisor	Easy to use with PPE.	Simplify UI; allow for multiple sensor fusion, including prioritising unoccluded features.

5.5.8 Artefact 3 Architecture Diagram Plan

Figure 5.22 shows the Proposed Architectural and contextual diagrams for Artefact 3. Where the diagram is put in a pictorial form to explain/incorporate all the described attributes from section 5.5

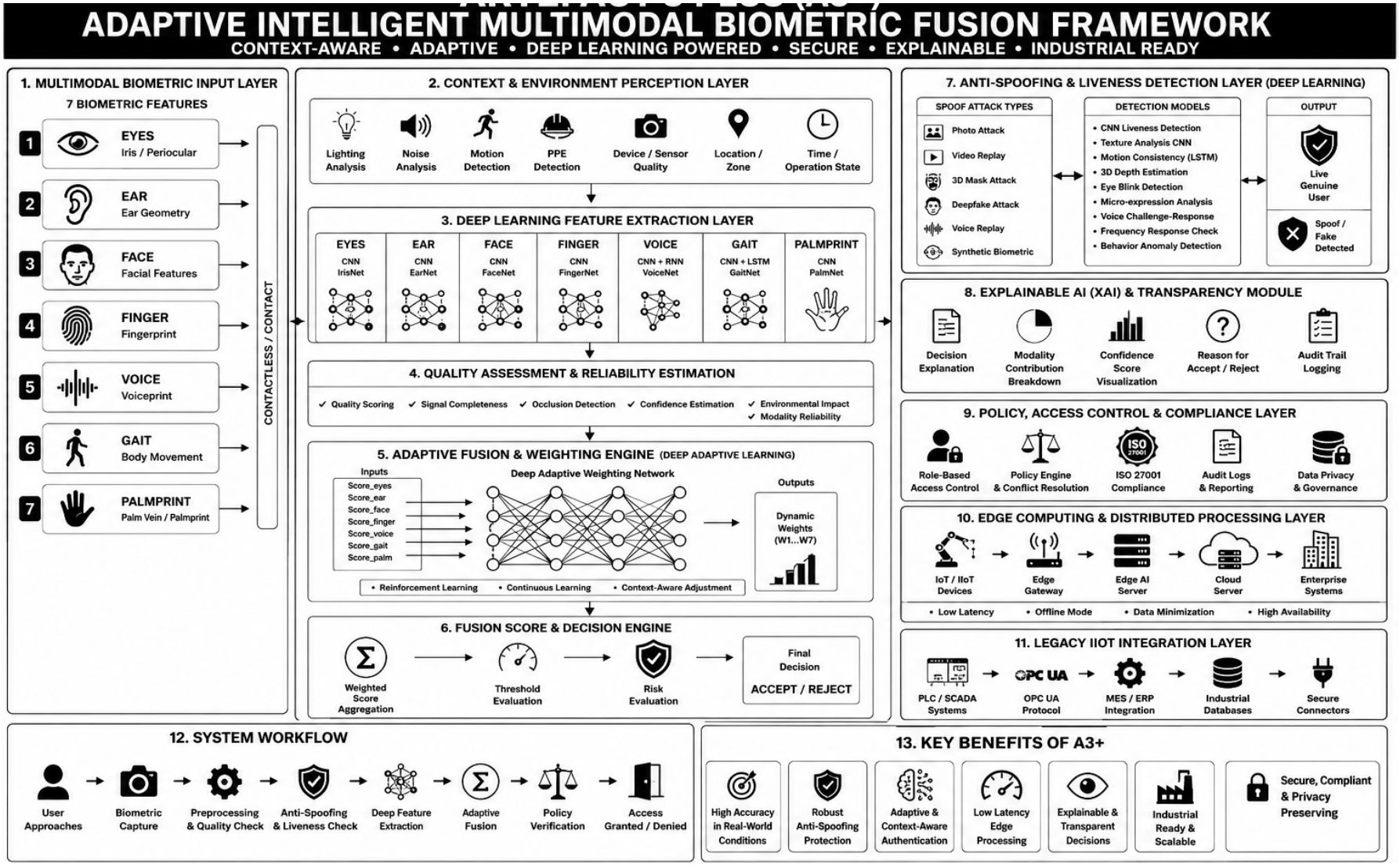


Figure 5.22 Artefact 3 Full framework

5.6 CONCLUSION

This expert review confirmed the overall direction of this research and informed the move from Artefact 2 towards Artefact 3 architecture (Figure 5.23). Three requirements were constantly mentioned, irrespective of experts: Low-latency, Edge-oriented processing (backed by the literature), and Robust policy governance (backed by the principle of ISO 27001). This leads to an Artefact 3 design that combines these requirements in an adaptive multimodal fusion, liveness detection, and logs it for auditing purposes.

- **Limitations:** The analysis is based on experts' views and proof-of-concept-level architecture. Thematic analysis was not quantified, and the findings should be viewed as a qualification rather than a generalisation. Also, it is expected that the real-world validation will be completed across multiple phases, and can be modified if there is a change in technology or threat models. Finally, in this chapter, non-biometric fallback approaches (such as PINs and physical tokens) were not explored.
- **Next steps:** Immediate work will include prototype integration and the development of an adversarial test suite. Recent studies on dynamic fusion mechanisms can be assessed, and on-device models can be optimised for the intended hardware to enhance the fusion mechanism. Further phases should focus on staged field deployment, compliance-oriented auditing (including retention and access control), and user acceptance testing. There is also a need for continuous monitoring of emerging threats, such as generative deepfakes, and for new standards, such as reporting standards (ISO/IEC 30107-3).

Chapter 6: DISCUSSION

6.0 INTRODUCTION

This chapter provides an interpretation of the results from Artefact 2 (A2) and Artefact 3 (A3) of the work to the research questions and hypotheses presented in Chapter 3. It not only presents numerical results but also highlights their implications in the field of biometric fusion authentication in Industrial Internet of Things (IIoT) contexts and their contribution to the research and practice. The four areas of the discussion are:

- Explain the results in relation to the research questions.
- Evaluate the hypotheses in light of the evidence in the experiment.
- Discuss implications of study (theoretical and practical).
- Make suggestions for improvement and/or further studies.

From the Second Life simulation, the results show that biometric fusion can result in strong performance in stable conditions, although as the environmental and operational factors become greater, the performance becomes less reliable. This further solidifies the importance of IIoT authentication that takes a proactive approach with adaptive, context-aware, and usability-focused designs. The direction for redesign identified in Artefact 3 was also confirmed by the expert review, which focused on the need for mechanisms that provide flexibility in response to changes in the environment, variability in behaviour, and stress during operation.

This chapter is designed to align with the research design methodology presented in Chapter 3. Information from the artefacts is used to answer the main research question in section 6.1, and how the socio-technical integration of multiple technologies enables robust biometric user authentication in different situations is demonstrated. Section 6.2 answers the research questions (RQ1–RQ3) and relates the findings obtained from the system performance metrics to their answers. The hypotheses (H1–H3) are examined by evaluating the evidence (based on empirical findings and theory) in section 6.3. The Contribution and impact of this study to the body of knowledge, the future recommendations, and the conclusion of the chapter are discussed in Sections 6.4, 6.5, and 6.6, respectively.

6.1 DISCUSSION OF THE MAIN RESEARCH QUESTION AND SUB-QUESTIONS

This section reviews and answers the main research question along with the research sub-questions.

- **Main Research Question: "How can biometric access control enable industry workers to authenticate seamlessly in various conditions?"**

Overall, the research indicates that the system's architecture is important for enabling seamless authentication for industrial workers, only if it can take advantage of varying conditions. In practice, this means that it is necessary to have a sense of context (e.g., PPE, lighting, motion), dynamic fusion behaviour, and clear escalation pathways when confidence is low, as seen from the analysis in sections 4.5 and subsections 5.4.1.1 and 5.4.1.4.

Under low constraints in Artefact 2 (low PPE obstruction, low lighting, Fast Movement, and industrial noise), the multimodal system achieved good authentication with high efficiency. The more constraints were added, the more unreliable the system became, and the reliability of the system went through three stages of behaviour: Stable phase (up to 1 constraint), Transitional phase (2–3 constraints), and Collapse phase (4, 5 constraints).

The trend suggests that performance in the IIoT environment is not linear, meaning that as additional stressors are combined, the performance of the authentication can drop off sharply. As a result, the above concerns are important in industrial environments because these environments do not necessarily conform to laboratory environments. These conditions are usually: worker motion and task variability, occlusion of safety equipment (PPE), variability in lighting and shadows, Vibration and camera motion of machinery, High ambient noise, and Operator fatigue during long shifts.

The static architecture was unable to maintain usability in the presence of combined stressors. In high constraint situations, the False Rejection Rate (FRR) increased to around 59.4%, which is a high rate of false rejection by legitimate workers from subsection 4.3.7.

These results, combined, raise an old security-usability dilemma where a system is designed with strict security in mind, but may not be fast or continuous enough to be used on an industrial site. In Artefact 3, the expert review was therefore in favour of a redesign towards adaptive fusion with the ability to:

1. Dynamically weight modalities based on reliability.
2. React to surroundings (e.g., PPE, light, movement, sound).
3. Fall back to less effective modalities when necessary, in line with policy and/or low confidence.
4. Minimise the number of legitimate rejections in times of stress.

The results support the case for adaptive, context-aware fusion in IIoT. Artefact 3 is a conceptual design that has not been implemented or tested, so its feasibility remains to be shown.

6.2 DISCUSSION OF RESEARCH QUESTION 1 TO 3 (RQ1–RQ3)

In this section, sub-questions 1 to 3 will be discussed and analysed in the subsections that follow.

6.2.1 Research Question 1

RQ1= **"What are the limitations of using biometric authentication for industry workers?"**

The simulation results are consistent with literature that constraints limit biometric authentication. Because the constraints were scripted, this reflects the modelled degradation. The simulation demonstrated that biometric traits degrade differently depending on the type and intensity of the applied environmental stress from Section 4.3. Visual biometric modalities such as FACE and EAR degraded rapidly under low-light conditions, helmet obstruction, face masks, and visual interference**.** Behavioural modalities such as GAIT and VOICE also deteriorated when workers operated under heavy movement and load conditions from subsection 4.2.8.

The study identified several core limitations:

- **Environmental Sensitivity**

  The operating conditions of industrial processes have a great influence on biometric systems. The compound constraints magnified the instability in authentication in a non-linear fashion.

- **Static Fusion Weakness**

  The system of equal-weight majority rule broke down when more than one biometric modality failed simultaneously. Static weighting was not able to adjust to varying environmental reliability.

- **Human-Computer Interaction Challenges**

  The study confirmed that usability and worker interaction behaviour have significant effects on the authentication performance. Lower authentication consistency was observed when more constraints were applied.

- **Simulation Constraints**

  It also highlighted some of the methodological constraints in using simulation environments. Second Life was able to simulate the decision-support logic and environmental effects but could not duplicate the physiological (biometric) acquisition.

Although these constraints exist, the simulation was still useful because it allowed them to experiment with the fusion logic and the condition-behavioural interaction score in a scalable virtual environment and to handle environmental degradation patterns.

6.2.2 Research Question 2

RQ2= **"What biometric traits can be used to identify and verify workers effectively?"**

The results showed that the multimodal biometric fusion system is a more resilient authentication system than using a single biometric modality. The study tested a number of biometric characteristics: FACE, GAIT, VOICE, and EAR. It was found that none of the biometric data was absolutely consistent in all the environmental conditions. They were, however, observed to be differently sensitive across various operational scenarios. For instance, the FACE and the EAR degraded quickly in conditions with visual obstructions. Heavy movement and load were the cause of deterioration of GAIT and VOICE. Despite various constraints, AVATARID had a slow degradation modality, considered deep learning, indicating the impact and consistency of deep learning in this study.

This is confirmation of the relevance of multimodal fusion for IIoT authentication systems. A combination of multiple biometric traits leads to an increase in redundancy and hence enhances the robustness of authentication. From sections 4.3 and 4.4, the study also showed that alternative biometric systems like IRIS, FINGERPRINT, and PALMPRINT also provide fallback biometric features, offering escalation options when modalities are not working.

The literature, simulation and expert review together suggest that in an IIoT environment, successful authentication of workers needs a mixture of physiological biometrics, behavioural biometrics, contextual know-how of the system, and fallback mechanisms that are adaptive.

6.2.3 Research Question 3

RQ3= **"What biometric mechanisms are required to develop a practical biometric access control framework tailored to IIoT requirements?"**

The results show that the practical IIoT biometric authentication systems must be adaptive and intelligent, instead of deterministic and rule-based systems from section 4.5. From Artefact 2, it was found that fixed-majority-rule verification will become unstable with increasing environmental stresses. The expert review redesign in Artefact 3, therefore, suggested the following mechanisms:

- **Adaptive Fusion Weighting**
  The modalities of biometrics should be dynamically adjusted based on the reliability of the environment.
- **Context-Aware Authentication**
  The authentication engine should be able to analyse several environmental conditions, such as light spectrum, worker motion, the presence of PPE that blocks biometric pathways, and operational stress, to select the optimal biometric pathways.
- **Multi-Level Authentication Escalation**
  The framework should ensure the ability to fall back to authentication using primary biometric traits when the system's authentication score is low or unreliable.
- **Human-Centred Authentication Design**
  However, usability and worker operational efficiency should still be key to the design of authentication in IIoT systems.
- **Intelligent Environmental Responsiveness**
  It would be better if the system could continuously track the degradation in reliability and dynamically adjust authentication thresholds rather than fixed acceptance thresholds.

The proposed Artefact 3 authentication architecture is based on these mechanisms, as shown in Figure 5.23.

6.3 HYPOTHESES TESTING

In this section, all hypotheses formulated in chapters 1 and 3 will be tested using evidence obtained from Artefacts 1, 2 and 3. The hypotheses were tested using a structured evidence-based evaluation approach aligned with the Design Science Research Methodology (DSRM). The testing process followed a logical reasoning approach, in which each hypothesis was evaluated by synthesising evidence from the three research artefacts. Artefact 1 provided theoretical validation through findings from the literature review in Chapter 2. Artefact 2 provided empirical validation through experimental evaluation of the proposed biometric access control framework under simulated IIoT conditions, and Artefact 3 provided practical validation through expert assessment and qualitative feedback. For each hypothesis, supporting evidence and contradictory evidence were critically examined to determine whether the findings confirmed, partially confirmed, or challenged the proposed relationship.

The decision-making process involved comparing the expected outcomes defined by each hypothesis against the observed evidence from the artefact evaluations. The logical testing framework assessed whether the identified relationships between environmental conditions, biometric fusion performance, and adaptive authentication requirements were consistent across theoretical, experimental, and expert perspectives. A hypothesis was accepted when the combined evidence demonstrated sufficient alignment between the expected behaviour and observed findings, while limitations and opposing evidence were used to refine the interpretation. This approach ensured that hypothesis validation was not based on a single source of evidence but represented a comprehensive assessment combining theoretical justification, experimental results, and expert validation to determine the effectiveness and applicability of the proposed adaptive biometric access control framework for IIoT environments.

6.3.1 Hypothesis 1 (H1)

In this subsection, the hypothesis states that “Environmental factors and operational conditions negatively affect biometric authentication reliability**”.**

6.3.1.1 Positive Evidence for H1

Yes, the results are consistent and supports H1 from the literature review, sections 5.4, 4.3 and 4.4, and Evidence from all three artefacts strongly supports this hypothesis.

- **Evidence from Artefact 1 (Literature Review)**

  The literature consistently reports that environmental factors remain a major challenge for contactless biometric authentication systems section 2.9. Previous studies identified illumination changes, occlusion caused by personal protective equipment (PPE), industrial noise, worker movement, dust, and weather conditions as significant causes of degraded biometric quality. Several researchers concluded that facial recognition systems experience considerable performance degradation when users wear masks or safety helmets, while voice recognition is adversely affected by machinery noise and reverberation. The literature, therefore, established the theoretical expectation that biometric reliability decreases as environmental complexity increases.

- **Evidence from Artefact 2 (Experimental Evaluation)**

  The experimental simulation supports the theoretical evidence. As environmental constraints increased from one to five simultaneous conditions, authentication performance deteriorated substantially. The study identified three distinct operational phases:

  - Stable authentication under low environmental constraints;
  - Progressive degradation under moderate constraints;
  - A collapse phase when multiple constraints were combined.

  The False Rejection Rate increased considerably under compound constraints, demonstrating that legitimate workers were increasingly rejected during authentication. These findings suggest that environmental conditions directly influence biometric reliability.

- **Evidence from Artefact 3 (Expert Review)**

  The expert review supports the experimental findings. Expert 1 stated that authentication systems must continue functioning despite helmets, masks, rain, dust, and worker movement, noting that "if it fails when things get messy, people won't use it." Similarly, Experts 4, 6, 8 and 9 all emphasised environmental robustness as a critical requirement for industrial deployment. The thematic analysis identified *Environmental Robustness and PPE*

Constraints as one of the dominant themes emerging from the qualitative evaluation. Collectively, the expert feedback validates the experimental evidence that environmental factors significantly affect authentication reliability.

6.3.1.2 Evidence Against H1

Although substantial evidence supports H1, several findings partially challenge the hypothesis.

- **Evidence from Artefact 1**

  The literature also reported that multimodal biometric systems generally outperform unimodal systems under adverse environmental conditions because degradation rarely affects all biometric modalities simultaneously.

- **Evidence from Artefact 2**

  The experiments showed that authentication performance did not completely collapse under moderate constraints. Some biometric traits remained relatively stable when others deteriorated. For example:

  - Avatar ID maintained consistently high performance.
  - Ear recognition remained usable when facial visibility declined.
  - Gait continued operating when facial features became partially occluded.

  These findings indicate that environmental conditions do not render biometric authentication unusable; instead, they expose weaknesses in static authentication architectures.

- **Evidence from Artefact 3**

  Experts consistently argued that adaptive biometric weighting could mitigate much of the environmental degradation. Expert 2 stated that adaptive weighting was the framework's strongest contribution, while Expert 6 emphasised that context-aware authentication can compensate for changing environmental conditions. Therefore, environmental effects are not irreversible but can be reduced through adaptive biometric fusion.

6.3.1.3 H1 Hypothesis Decision

After considering evidence from all three artefacts, H1 is Supported as constraints increase, the pass rate of the static baseline decreases which is supported, in simulation. The literature established the theoretical relationship between environmental constraints and biometric degradation, the experimental evaluation quantitatively demonstrated this relationship, and the expert review confirmed its operational significance in industrial environments.

However, the findings also demonstrate that the negative effects of environmental conditions can be substantially mitigated through adaptive multimodal biometric fusion, contextual awareness, and intelligent weighting strategies.

6.3.2 Hypothesis 2 (H2)

In this subsection, the hypothesis States that "Multiple biometric traits can effectively identify and verify workers in industrial environments."

6.3.2.1 Positive Evidence for H2

Yes, the results, in part, corroborate H2 from the literature review, sections 4.3 and 4.4, and Artefacts 2 and 3. under the same constraints, fusion achieves a higher pass rate than any single trait partly supported.

- **Evidence from Artefact 1**

  The literature consistently finds that multimodal biometric fusion is more reliable than single-biometric authentication (Section 2.9). Previous studies demonstrated that combining physiological and behavioural biometrics improves recognition accuracy, robustness, and resistance to spoofing attacks, as the weaknesses of one modality are compensated for by the others.

- **Evidence from Artefact 2**

  The experimental evaluation partly supports these findings. The multimodal authentication framework achieves high authentication accuracy under low and moderate environmental stress. The fusion of facial recognition, ear recognition, gait analysis, voice recognition and Avatar ID produced significantly higher authentication reliability than would be expected from individual modalities. The experiments further demonstrated that different

biometric traits degraded independently, creating useful redundancy during authentication.

- **Evidence from Artefact 3**

  Experts 4 and 7 both liked the multimodal authentication. Expert 4 stated that "multi-modal biometrics is already proven," while Expert 7 considered the combination of multiple modalities appropriate for industrial simulation. The thematic analysis further identified *Multimodal Integration* as one of the core design principles incorporated into Artefact 3.

6.3.2.2 Evidence Against H2

Despite these positive findings, important limitations were identified.

- **Evidence from Artefact 1**

  The literature cautioned that multimodal fusion alone does not automatically guarantee improved authentication performance if poor-quality biometric samples are fused without considering environmental context.

- **Evidence from Artefact 2**

  The experimental evaluation suggest that static majority-rule fusion became increasingly unstable under compound environmental constraints. Facial recognition deteriorated significantly under PPE, while voice recognition became unreliable under industrial noise. This showed that merely increasing the number of biometric modalities does not necessarily improve authentication unless modality quality is considered during fusion.

- **Evidence from Artefact 3**

  Experts repeatedly recommend replacing equal-weight fusion with adaptive weighting. Expert 2 identified adaptive weighting as the framework's strongest contribution, while Expert 4 recommended dynamic confidence scoring to account for varying biometric reliability. These findings indicate that multimodal fusion alone is insufficient.

6.3.2.3 Hypothesis 2 Decision

The evidence supports H2 under the same constraints, fusion achieves a higher pass rate than any single trait partly supported.

6.3.3 Hypothesis 3 (H3):

In this subsection, the hypothesis states that "Practical IIoT biometric systems require adaptive fusion mechanisms, contextual responsiveness, and scalable integration."

6.3.3.1 Positive Evidence for H3

The Findings/results corroborate H3 from sections 4.4 and 4.5, and Artefacts 2 and 3. Therefore it is Partly supported adaptive mechanism not tested

- **Evidence from Artefact 1**

  The literature review identified adaptive authentication, context awareness, explainable AI, edge computing, and multimodal fusion as emerging research directions that address the limitations of conventional biometric systems.

- **Evidence from Artefact 2**

  The experimental evaluation demonstrated that equal-weight fusion became increasingly unstable as environmental constraints accumulated. The observed degradation patterns clearly indicated that static authentication architectures lack the flexibility required for IIoT environments.

- **Evidence from Artefact 3**

  The strongest support for H3 emerged from the expert review.

  - Experts consistently recommended:
  - adaptive weighting;
  - edge processing;
  - environmental sensing;
  - anti-spoofing mechanisms;
  - explainable AI;
  - policy integration;
  - low-latency authentication.

  The thematic analysis identified Adaptive Weighting, Edge Computing, Environmental Robustness, Explainability, and Policy Integration as dominant architectural requirements. These findings directly informed the development of Artefact 3.

6.3.3.2 Evidence Against H3

The evidence also revealed several implementation challenges. The literature review acknowledges that adaptive systems require significantly greater computational complexity than traditional biometric architectures. The experimental evaluation was conducted in a controlled virtual environment rather than a live industrial setting. Experts 7 and 8 further noted that simulation validity must eventually be confirmed through real-world deployment and that integration with legacy industrial systems remains challenging. These limitations suggest that although adaptive authentication is desirable, implementation requires additional engineering effort and validation.

6.3.3.3 Hypothesis Decision

H3 is Partly supported adaptive mechanism not tested.

6.3.4 Overall Interpretation of the Hypothesis Testing

The evidence converges across the three artefacts. This is supporting evidence, not validation. **Artefact 1** established the theoretical foundations by identifying the limitations of conventional biometric authentication and highlighting the potential of multimodal, adaptive, and context-aware approaches. **Artefact 2** partly supports these theoretical propositions through controlled experimentation, showing that environmental conditions significantly influence authentication performance and that static fusion strategies are inadequate under compound constraints. **Artefact 3** provided partial validation through expert review, confirming that adaptive weighting, environmental awareness, anti-spoofing mechanisms, edge processing, explainable AI, and policy integration are essential for industrial deployment although its not field tested

Taken together, the evidence supports all three hypotheses while also refining their interpretation. The findings show that multimodal biometric fusion alone is insufficient for reliable IIoT authentication. Instead, robust industrial authentication requires an adaptive, context-aware framework that dynamically adjusts to environmental conditions, biometric quality, operational constraints, and organisational requirements. This integrated conclusion represents the principal contribution of the thesis and provides strong theoretical, empirical, and practical justification for the proposed adaptive contactless biometric access control framework for Industrial Internet of Things environments.

Table 6.1 Evidence matrix

Evidence	H1: constraints reduce reliability	H2: multiple traits identify workers	H3: adaptive, context-aware fusion needed
Literature (2.9)	For: occlusion, noise and light degrade face and voice. Against: multimodal systems are less affected	For: fusion beats single traits. Against: fusing poor samples without context does not help	For: adaptive and context-aware fusion is an emerging direction. Against: more complex
Simulation (Ch. 4)	For: efficiency 1.00 up to one constraint, 0.17 at three, 0.00 from four (Table 4.9); tipping between two and three constraints (p141)	For: fused decisions pass under low and moderate stress. Against: static fusion fails under compound stress; no per-trait comparison yet	Illustrates limits of static fusion; adaptive weighting not tested
Experts (Ch. 5)	For: environmental robustness a dominant theme (Experts 1, 4, 6, 8, 9)	For: multimodal approaches endorsed (Experts 4, 7)	For: adaptive weighting, edge processing, policy integration. Against: simulation validity and legacy integration still to be shown (Experts 7, 8)
Decision	Supported (in simulation)	Partly supported	Partly supported; adaptive mechanism not tested

6.4 CONTRIBUTION OF THE STUDY

This research makes multiple contributions in the field of biometric fusion authentication and in the field of security in IIoT.

- The study presents a simulation-based, structured method for studying the behaviour of the fusion of biometric data in virtual industrial environments with Second Life.
- The research contributes to the current body of HCI to incorporate usability, environmental stress, behavioural variability, and adaptive biometric fusion into a single IIoT authentication framework.
- The proposed Artefact 3 architecture provides a conceptual basis for adaptive biometric authentication systems in the future.

6.4.1 Practical Implications

The implications of this research are meaningful for heavy construction industries with similar constraints / environmental stressors, advising them to upgrade or implement biometric access control systems. The results indicate that environmental variability should be taken into account when designing the system in the deployment sites, such as factories, ports, logistics centres, construction sites, mines, or manufacturing plants.

It shows that, under certain circumstances, it is possible to obtain a high security performance with static biometric systems, but due to excessive legitimate rejection rates, the usability of the system with regard to operational use is reduced. Adaptive authentication, environmental sensing, worker usability, and multimodal redundancy should thus be key concerns for industrial authentication systems.

The face-channel scores declined approximately linearly as the number of environmental constraints increased. The score decreased from 90 under no constraints to 5 under five constraints, representing an average reduction of 17 points per additional constraint, equivalent to approximately 18.9% of the initial score. In contrast, the overall pass rate declined nonlinearly across the constraint levels, with rates of 1.00, 0.93, 0.40, 0.23, 0.20 and 0.00, respectively (Table 4.5 & 4.10). The largest reduction occurred between one and two constraints, where the pass rate decreased from 93.3% to 40.0%. This difference between the approximately linear decline in individual channel scores and the nonlinear decline in overall pass rates reflects the operation of the static fusion rule and its fixed passing threshold of 60. This threshold behaviour is specific to the scripted simulation and the static fusion configuration; it should not be interpreted as evidence of equivalent behaviour in real-world biometric systems.

6.5 ISO STANDARDS ALIGNMENT TO ARTEFACT 3

In this section ISO standards are mapped out to Artefact 3, to help aid its interoperability. Authentication must not obstruct local emergency actions (IEC, 2013). Artefact 3 therefore (1) keeps emergency-stop and other safety functions independent of authentication and hard-wired, (2) gates only access, override, bypass, reset and restart, (3) provides an audited break-glass procedure in every zone, (4) gives a rejected worker a bounded fallback ladder of retry, alternate modality, token and

supervisor, (5) fails egress doors safe and sensitive-zone entry secure, and (6) does not make evacuation tracking depend on a biometric match.

Table 6.2 ISO Mapping to Artefact 3

Artefact 3 element (Section 5.5)	Standard counterpart	How it is addressed
Sensor and recognition modules	IEC 62443-3-3 SR 1.1	Biometric identification of each worker
Enrolment, template store, revocation	SR 1.3, 1.4, 1.5	Account, identifier and authenticator management; template protection
Policy layer with step-up	SR 1.1 enhancements; security levels	Stronger authentication in higher-level zones
Adaptive thresholds	Security level capability	Tightened in higher-level zones, never below the zone minimum
Failed-attempt handling	SR 1.11	Lock-out balanced against emergency access
Explainability output	SR 1.10	Feedback must not leak information to an attacker
Audit and decision log	SR 2.8, 2.12; NIST AU family	Records who were authenticated, when, with what confidence
Remote and vendor access	SR 1.13; IEC 62443-2-4	Multifactor authentication on untrusted networks

The 59.4% false rejection rate under static fusion (Section 4.3.7) shows why authentication must never sit in the path of emergency actions. In line with IEC 62443-3-3 and NIST SP 800-82, Artefact 3 separates safety functions from authentication, uses a bounded fallback ladder and provides an audited break-glass path (Section 5.5.3). The figure comes from a scripted simulation, so it illustrates the risk and is not a field estimate.

6.6 FUTURE RECOMMENDATIONS

The findings of this research and limitations are used to propose several recommendations for future research as follows:

- **Expanded Biometric Modalities**

The study of other biometric characteristics like thermal biometrics, heart rate signatures, behavioural micro-patterns, EEG, and wearable sensor biometrics should be explored in future studies.

- **Longitudinal Human-Centred Studies**

  Future research should explore how well workers will accept and adapt to this unit, worker fatigue and stress behaviour, and the long-term effects on usability, through the application of usability principles.

- **Edge Computing and IIoT Integration**

  For future deployments, the following are potential research areas: edge AI processing, real-time integration of IIoT, distributed biometric gateways, and low-latency authentication architectures.

- **Multi-User and Multi-Site Authentication**

  Multi-worker support, cross-site synchronisation, and enterprise-scale federation should be supported in future systems.

6.7 CHAPTER CONCLUSION

The results of the study were discussed in this chapter, in reference to the research questions and hypotheses. The study showed that, in a stable environment, the biometric fusion authentication systems are effectively used to secure access to IIoT, however, in an environment that is stressful, the system can become more unstable. The results showed that the biometric reliability, usability, and stability of authentication are greatly affected by the environment. Multimodal biometric fusion worked well to make it more resilient, but a static equal-weight design was found to be inadequate for dynamic industrial settings.

Thus, it can be concluded that future IIoT biometric authentication systems need to be adaptive, context-aware, and human-centred, where they will intelligently learn and adapt to the changing conditions of the environment and operational stress. This study combines the concepts of simulation testing, experimental analysis, and expert review-guided redesign to further theory and practice in the design of future adaptive biometric authentication systems in industrial settings.

.

Chapter 7: Conclusion

7.0 INTRODUCTION

In this thesis, the author investigated the feasibility of enabling seamless biometric access control for industrial workers operating under realistic constraints. The issue that needed to be addressed was practical: many biometric systems that operate without problems in controlled environments fail when used in dynamic environments where workers are wearing PPE, lighting changes, noise, and movement cannot be controlled. The thesis, in response, proposed and tested an adaptive multimodal authentication system for IIoT, which considers the security and operational usability. The research questions (RQs) and the hypotheses were:

- **RQ1:** What limitations arise when biometric authentication is used by industrial workers? (H1: The reliability of authentication is influenced by the environment or operation.)
- **RQ2:** Which biometric traits and combinations can identify and verify workers effectively? (H2: multimodal trait makes a trait more reliable.)
- **RQ3:** What mechanisms are required for a practical IIoT biometric access-control framework? Now let's look at the mechanisms required for a feasible IIoT biometric access-control framework: (H3) Adaptive fusion, context awareness, and standards-informed governance are needed.

The DSRM framing was employed in this study. The multimodal fusion system was evaluated in Artefact 2 (A2), which simulated a Second Life application in which a worker avatar was subjected to specific constraints (such as PPE obstruction, movement, and lighting). Artefact 3 (A3) then applied structured feedback from the nine industrial domain specialists to further develop the architecture into an adaptive and context-aware architecture with a specific focus on adversarial testing, standards alignment, edge deployment, and usability within the operational workflows.

7.1 SUMMARISED KEY FINDINGS

There are various key findings of this study:

- **Static fusion collapse:** In Artefact 2, four to five constraints resulted in a sharp drop in the usability. In the worst-case stress, the False Rejection Rate (FRR) was about 59.4%. This helps H1 and shows how stressors can interact

nonlinearly in an industrial environment. In this case, the equal-weight fusion is impractical to run.

- **Multimodal resilience (with limits):** None of the properties was consistent when all constraints occurred together. Face and ear recognition decreased in low lighting and with PPE, while gait and voice recognition decreased in the presence of high movement and noise. Traits (face, gait, voice, and ear) and fall-back iris/fingerprint options had a positive impact on overall resilience and, in part, supported H2. The results, however, demonstrate that multimodality is not enough without adaptive weighting: in compounded stress, even multimodal fusion can yield an unacceptably high number of false rejections.
- **Need for an adaptive framework:** Artefact 3 proposes mechanisms to address RQ3 and H3, such as adaptive weighting (prioritising the most reliable modalities among the ones currently available), context sensing (understanding the context by sensing lighting, motion, and PPE), and escalation pathways (e.g., iris/fingerprint) if primary traits are not reliable. In response to adversarial threats, anti-spoofing and liveness detection (performed according to ISO/IEC 30107) were added, along with policy governance (which was based on ISO 27001) and edge-first processing, which met latency and privacy requirements.
- **Theoretical contributions:** The thesis builds on the field of biometric fusion and IIoT security to show that authentication reliability rather than a gradual degradation when subjected to stressors in the industrial environment. It also proposes adaptive fusion, context sensing, and escalation pathways architecture-level synthesis (Artefact 3) that integrates all these aspects, as well as a means to explore usability-sensitive authentication logic at scale prior to field deployment using simulation.
- **Practical implications:** In terms of experts, this study shows that in many scenarios, the deployment of generic biometric systems is not suitable for an industrial setting without modifications. Systems must be adaptable to changing conditions, and should strike a balance between security and the continuity of the workflow, and minimise unnecessary rejections. The expert panel highlighted the need for standards-aligned governance and explicit

presentation attack detection based on ISO/IEC 30107 principles to access control and auditability. Edge computing was also a recurring theme for minimising latency and avoiding reliance on cloud connectivity in situations with limited bandwidth or where connectivity is not guaranteed.

7.2 KEY RESULTS MAPPED TO RESEARCH QUESTIONS

This section briefly recaps the discussion in Chapter 6.

- **RQ1 (Limitations):** The study is consistent with the findings that environmental and conditional constraints are the main limitations for industrial biometrics. Low light and headgear or PPE resulting in occlusion had a significant impact on visual modalities (e.g., face), and voice and gait were impaired by noise and gait variability. These effects were non-linear, with performance changing abruptly after several constraints were added; the highest-constraint case reached about 59% FRR.
- **RQ2 (Effective traits):** Multimodal fusion (face, voice, gait, ear, with optional iris/fingerprint escalation) proved to be more resilient than any single modality, in that the different traits were more susceptible to different stressors. For instance, masked faces are still informative when discussing their gait, but not when discussing their voice, while masked voices are still informative, but when noise is high, gait is useful. As a result, the evidence supports the refinement of H2: modalities complement each other to enhance robustness, especially when fused with a weight rather than a fixed one.
- **RQ3 (Required mechanisms):** Based on the experimental results and expert review, five mechanisms were found recurring in all the designs proposed for Artefact 3: (1) adaptive fusion and weighting based on reliability, (2) context awareness by using sensor information (lighting, motion), (3) escalation pathway to fallback mechanisms when confidence is low, (4) presentation attack detection and liveness checks that are consistent with the requirements of ISO/IEC 30107, and (5) edge-oriented processing to meet the latency requirements. The ISO/IEC 27001 principles help to implement a policy layer that enables auditability and operational governance.

7.3 THEORETICAL CONTRIBUTIONS

This research makes several contributions to the literature on biometrics and IIoT security:

- It embeds HCI and environmental aspects in the designs of a biometric system, according to the usability principles of ISO standard 9241-11. It takes into account effectiveness, efficiency, and satisfaction within context, which broadens the scope of biometric research into real-world uses.
- It proposes a new **Artefact 3 adaptive architecture** that merges context-awareness, adaptive fusion, escalation, and compliance. This system-level design has not been shown in prior work and can serve as a baseline for future adaptive biometrics research.
- It demonstrates the value of **virtual simulations** (Second Life) for biometric experimentation, offering a method to test user-behaviour interactions and system logic under controlled yet realistic constraints.

7.4 PRACTICAL AND INDUSTRIAL IMPLICATIONS

For practitioners who are thinking about implementing biometric access control at factories, ports, construction sites, and other industrial settings, the results suggest that it is a misconception to think that there is a single "best" biometric they need to choose and that, rather, how the system is engineered to deal with variations is more important. Especially, occlusion, movement, noise, and intermittent connections should be considered in designs as well as continuity of the workflow, with careful attention to strong security measures.

- **Use multimodal, adaptive fusion:** Integrate complementary features and use them in real-time to ensure the most sound and confident signal is used in real time.
- **Design for usability under pressure:** Workers should not have to pause or repeat steps to get authenticated, false rejections will hinder operation, and decrease acceptance.
- **Treat liveness and spoof resistance as mandatory:** Presentational attack detection and evaluate systematically (according to ISO/IEC 30107 expectations).

- **Leverage edge computing:** Use edge computing to reduce latency and dependence on cloud connectivity by performing matching and fusion at the edge.
- **Engineer for harsh conditions:** Ensure proper sensing and filtering of dust, rain, variable lighting, and high noise, and validate under representative site conditions.

7.5 LIMITATIONS

There are several limitations to the study that were partly mitigated by the expert feedback, but they are as follows:

- **Simulation vs. real-world capture:** Artefact 2 used a virtual environment to do the simulation instead of a real-world capture. The evaluation of fusion logic and avatar behaviour was supported by Second Life, but it was unable to capture physiological biometrics, so the results may vary in physical deployments.
- **Simplified user modelling:** Avatar interactions and constraint proxies are good approximations of actual actions, and may not accurately represent all the variability of human action, posture, constraints and fatigue.
- **Scope of conditions and threats:** Conditions and threats simulated were limited to those defined in the simulation (up to five). Real sites bring more dynamics (weather, variety of PPE, changing workflows), and the Artefact 2 threat model was not sophisticated adversaries or insider scenarios.
- **Baseline choice:** Artefact 2 used the equal-weight majority fusion as a baseline. Advanced but non-adaptive baselines (e.g., learned fusion without context) were not tested and could give better results compared to the naive baseline.
- **Prototype maturity:** Artefact 3 is specified as a conceptual architecture. Not yet implemented and validated as a live system, it cannot be assumed to provide benefits until the engineering process and introduction to a field in a staged evaluation are completed.
- The only non-adaptive baseline was equal-weight majority fusion. A learned score-level fusion baseline, such as logistic regression on channel scores without context (Ross & Jain, 2003; Nandakumar et al., 2008), was not

included because the simulation produced only genuine, scripted-degradation attempts and no impostor scores, so a classifier could only learn the scripting rule. This is the first extension recommended.' Optional extension: a Monte Carlo score model comparing equal-weight, learned context-blind and context-weighted fusion at a fixed false acceptance rate, presented as a sensitivity analysis because the context-weighted rule uses the scripted degradation

- The review used short, mostly structured questions with an open comment item, which produced focused judgements but limited explanation of reasons. The panel was selected purposively, coded by one researcher, and saw earlier summary results, so agreement may be partly anchored. Against the principles of Klein and Myers (1999), contextualisation and multiple interpretations were supported, while researcher–subject interaction and critical examination of bias were weak. Nine participants is consistent with code-saturation evidence (Guest et al., 2006; Hennink et al., 2017) but may not reach meaning saturation. Future work should use semi-structured follow-up interviews, a second coder and a wider panel

7.6 RECOMMENDATIONS

Based on the findings, the following actions are recommended:

- **Short-term (Research & Development): Carry** out tests and a prototype of the Artefact 3 architecture, which includes adaptive weighting and context sensors. Start small-scale pilot tests in a controlled industrial environment, gather real data, and improve algorithms. Ensure policy readiness by implementing governance from the beginning that is based on standards (such as access control, logging, handling, and secure handling based on ISO/IEC 27001 principles.
- **Short-term (security validation):** Design and test liveness and anti-spoofing for each modality and implement repeatable PAD testing procedures, based on ISO/IEC 30107.
- **Medium-term (Deployment & Evaluation):** Deploy pilots at one industrial site, or several industrial sites, such as a construction site or port. Take advantage of edge computing hardware to enable low-latency fusion. Collect

quantitative data (authentication success rates, FRR/FAR, time to authenticate) and qualitative feedback (user acceptance, ease of use) during the pilots.

- **Medium-term (adversarial and resilience testing):** Take the evaluation beyond simple spoofing and coordinate the attack (e.g., deepfakes, replay, network-layer disruption). Monitor and record successes, false alarms, and operational effects, then incorporate findings into the improvements of fusion policies, escalation triggers, and monitoring rules.
- **Medium-term (standards and governance):** Ensure that implementation is in accordance with relevant industrial security standards and biometric standards and define appropriate governance for enrolment, retention, access control, and audit logging. In cases of jurisdiction crossovers, ascertain if biometric handling is compliant with relevant privacy and data protection laws.
- **Long-term (Scale & Policy):** Once the pilots are a success, plan for enterprise deployment. Implement biometric and context-aware authentication in the corporations' security policies. Train users to ensure high data quality and data acceptance.
- **Long-term (Continuous Evaluation):** Implement ongoing monitoring of the system in production. Define KPIs (e.g. reduction in tailgating incidents, authentication speed, error rates) and regular audit performance. Solicit user feedback to iterate on usability improvements.
- **Research:** Investigate other modalities (e.g., thermal, heartbeat, or wearable sensors) and AI techniques (e.g., reinforcement learning for fusion optimisation and explainable AI) to enhance adaptability and trust further.

7.7 ARTEFACT 2 VS ARTEFACT 3 COMPARISON

This subsection summarises the conclusions of the Artefact 2-Artefact 3 comparison in the table below.

Table 7.1 Artefact 2 and Artefact 3 comparison table from sections 4.5 and 5.5

ASPECT	ARTEFACT 2 (section 4.5)	ARTEFACT 3 (section 5.5)
Purpose	Test a foundational system that fuses multiple data modalities based on static equal weights in a simulated IIoT setting.	Create a holistic, flexible, context-aware, biometric access model for IIoT.
Strengths	Simple architecture showed the basic viability of the multimodal biometrics concept.	Flexibility in adapting to a changing environment, environmental awareness, usability, and security improvement.
Weaknesses	High False rejection rate with multiple constraints, no Anti-spoofing, Static Policy.	More complex design; not tested in actual deployment; needs to have accurate sensing and model training; overhead of integration.
Key Components	Multimodal sensors (face, gait, voice, ear), equal weight majority fusion, simulated constraint token.	Context sensors (light, motion, and PPE detectors), deep-learning feature extractors, adaptive weighting engines, liveness (anti-spoof) modules, edge computing nodes, and policy/access control layers.
Readiness	The prototype is only validated in simulation, not robust to the variability in the real world.	Concept design, with expert feedback, needs to be validated in the field and in the engineering process before deployment.

7.8 CONCLUSION

Overall, this research shows that to realise seamless biometric authentication in industrial environments, a fixed approach is not sufficient, but an adaptive, context-aware approach is necessary. In contrast to the traditional multimodal fusion method, which is secure, it fails under the variations of real-world conditions. In contrast, the Artefact 3 architecture focuses on adapting security methods to the context of the user and the environment, as well as to escalate to fallback methods, as and when necessary, without detracting from the usability of the operation. The results include a theoretical analysis as well as practical design information, supported by simulations and expert validation.

Going forward, efforts should be made to implement and pilot test Artefact 3 in real IIoT environments and to iteratively improve it through adversarial testing and user feedback. Finally, these findings and standards-based controls (such as ISO 27001/30107) can help to create reliable and usable access using biometrics that can satisfy the requirements of Industry 4.0.

REFERENCES

Abaza, A., Ross, A., Hebert, C., Harrison, M. A. F., & Nixon, M. S. (2013). A survey on ear biometrics. *ACM Computing Surveys, 45*(2), Article 22

Abe, M., Akiyoshi, T., Butaslac, I., Hangyu, Z., & Sawabe, T. (2022, March). Hype Live: Biometric based Sensory Feedback for Improving the Sense of Unity in VR Live Performance. In 2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW) (pp. 836, 837). IEEE.

Abidin, Z. Z., Manaf, M., Shibghatullah, A. S., Yunus, S. M., Anawar, S., & Ayop, Z. (2012). Iris segmentation analysis using integro-differential and hough transform in biometric system. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 4(2), 41-48.

Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A Comprehensive Survey on security, attacks and countermeasures for industrial applications. Sensors, 21(11), 3654.

Adewole, K. S., Abdulsalam, S. O., Babatunde, R. S., Shittu, T. M., & Oloyede, M. O. (2014). Development of fingerprint biometric attendance system for non-academic staff in a tertiary institution. Development, 5(2), 62-70.

Afianian, A., Niksefat, S., Sadeghiyan, B., & Baptiste, D. (2020). Malware Dynamic Analysis Evasion Techniques. ACM Computing Surveys, 52(6), 1–28. https://doi.org/10.1145/3365001

Ahmad, A., Javaid, N., Khan, Z. A., Qasim, U., & Alghamdi, T. A. (2014). $(ACH)^ 2$: Routing Scheme to Maximize Lifetime and Throughput of Wireless Sensor Networks. IEEE Sensors Journal, 14(10), 3516-3532.

Akram, H., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/IJACSA.2018.090349

Al Sibahee, M. A., Lu, S., Masoud, M. Z., Hussien, Z. A., Hussain, M. A., & Abduljabbar, Z. A. (2016, April). LEACH-T: LEACH clustering protocol based on three layers. In 2016 International conference on network and information systems for computers (ICNISC) (pp. 36-40). IEEE.

Alcácer, V., & Cruz-Machado, V. (2019). Scanning the Industry 4.0: A literature review on technologies for manufacturing systems. Engineering Science and Technology an International Journal, 22(3), 899–919.

Alkassar, S., Woo, W. L., Dlay, S. S., & Chambers, J. A. (2015). Robust sclera recognition system with novel sclera segmentation and validation techniques. IEEE transactions on systems, man, and cybernetics: systems, 47(3), 474-486.

Alonso-Fernandez, F., & Bigun, J. (2015). Near-infrared and visible-light periocular recognition with Gabor features using frequency-adaptive automatic eye detection. IET Biometrics, 4(2), 74–89. https://doi.org/10.1049/iet-bmt.2014.0038

Alonso-Fernandez, F., Tome-Gonzalez, P., Ruiz-Albacete, V., & Ortega-Garcia, J. (2009). Iris recognition based on SIFT features. 2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS), 1-8. https://doi.org/10.1109/BIDS.2009.5507529

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F., & Chaudhry, S. R. (2016). IoT architecture challenges and issues: Lack of standardization. 2016 Future

Technologies Conference (FTC), 731–738. https://doi.org/10.1109/FTC.2016.7821686
Al-Rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy and countermeasures: A survey and research directions. Computers & Security, 74, 144–166.
ALSaleem, B. O., & Alshoshan, A. I. (2021). Multi-Factor Authentication to Systems Login. 2021 National Computing Colleges Conference (NCCC), 1–4. https://doi.org/10.1109/NCCC49330.2021.9428806
Alvarez-Betancourt Y, Garcia-Silvente M (2016) A keypoints-based feature extraction method for iris recognition under variable image quality conditions. Knowl-Based Syst 92:169–182
Ambrosin, M., Conti, M., Ibrahim, A., Sadeghi, A.-R., & Schunter, M. (2018). SCIoT: A secure and scalable end-to-end management framework for IoT devices. In Lecture Notes in Computer Science (pp. 595–617). Springer. https://doi.org/10.1007/978-3-319-99073-6_29
Ameer, S., Benson, J., & sandhu, R. (2022). Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT. IEEE Transactions on Dependable and Secure Computing, 118. https://doi.org/10.1109/TDSC.2022.3216297
Anand, S., Kapoor, A., & Jain, A. K. (2020). DeepResPore: A deep residual network for pore detection and fingerprint recognition. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2(3), 235–247. https://doi.org/10.1109/TBIOM.2020.2980394
Armknecht, F., Sadeghi, A.-R., Schulz, S., & Wachsmann, C. (2013). A security framework for the analysis and design of software attestation. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13, 1–12. https://doi.org/10.1145/2508859.2516650
Artabaz, S., Benatchba, K., Koudil, M., Nabil, D. H., & Bouridane, A. (2014). Extraction method of Region of Interest from hand palm: Application with contactless and touchable devices. Proceedings of IAS 2014, IEEE, 77–82. https://doi.org/10.1109/IAS.2014.7004824
Awaysheh, F., Aladwan, M., Alazab, M., & Awajan, A. (2020). Explainable artificial intelligence for cybersecurity applications. IEEE Access, 8, 192418–192431.
Bailenson, J. N., Yee, N., Blascovich, J. (2008). Immersive virtual environments and the experimental study of social interaction. Psychological Science.
Bao, Z., Tan, Z., Wan, J., Ma, X., Guo, G., & Lei, Z. (2023). Divergence-Driven Consistency Training for Semi-Supervised Facial Age Estimation. IEEE Transactions on Information Forensics and Security, 18, 221–232. https://doi.org/10.1109/TIFS.2022.3218431
Barbosa, F. G., & Santos Silva, W. L. (2015). Automatic voice recognition system based on multiple Support Vector Machines and mel-frequency cepstral coefficients. 2015 11th International Conference on Natural Computation (ICNC), 665–670. https://doi.org/10.1109/ICNC.2015.7378069
Battistone, S., & Petrosino, A. (2019). TGLSTM: A time-based graph Long Short-Term Memory model for gait recognition. Pattern Recognition Letters, 126, 35–42. https://doi.org/10.1016/j.patrec.2019.05.003
Behrendt, A., Müller, N., Odenwälder, P., & Schmitz, C. (2017, March 30). Industry 4.0 demystified-lean's next level. McKinsey & Company. https://www.mckinsey.com/business-functions/operations/our-insights/industry-4-0-demystified-leans-next-level

Behutiye, W., Rodriguez, P., & Oivo, M. (2022). Quality Requirement Documentation Guidelines for Agile Software Development. IEEE Access, 10, 70154–70173. https://doi.org/10.1109/ACCESS.2022.3187106
Bengio, Y., Louradour, J., Collobert, R., & Weston, J. (2009). Curriculum learning. Proceedings of the 26th Annual International Conference on Machine Learning (ICML), 41–48. https://doi.org/10.1145/1553374.1553380
Bentahar, A., Meraoumia, A., Bendjenna, H., & Zeroual, A. (2018). IoT Securing System using Fuzzy Commitment for DCT-based Fingerprint Recognition. 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS), 1–5. https://doi.org/10.1109/PAIS.2018.8598511
Berger, S., Klier, J., Klier, M., & Probst, F. (2020). A review of information security management in Industry 4.0. Computers & Security, 89, 101665.
Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Samaka, M., & Khan, K. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89, 101677.
Bhattacharya G, Alam J, Kenny P (2019) Deep speaker recognition: modular or monolithic? Proc Interspeech 2019:1143–1147
Bibri, S. E. (2022). The Social Shaping of the Metaverse as an Alternative to the Imaginaries of DataDriven Smart Cities: A Study in Science, Technology, and Society. Smart Cities, 5(3), 832–874. https://doi.org/10.3390/smartcities5030043
Blanco-Gonzalo, R., Miguel-Hurtado, O., Lunerti, C., Guest, R. M., Corsetti, B., Ellavarason, E., & Sanchez-Reillo, R. (2019). Biometric systems interaction assessment: the state of the art. IEEE Transactions on Human-Machine Systems, 49(5), 397-410.
Bloomfield, R., & Rennekamp, K. (2010). Virtual economies and financial behaviour in online worlds. Journal of Economic Behavior & Organization, 78(2), 159–173.
Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the Internet of Things. Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 13–16.
Bowyer, K. W., Baker, S. E., Hentz, A., Hollingsworth, K., Peters, T., & Flynn, P. J. (2009). Factors that degrade the match distribution in iris biometrics. Identity in the Information Society, 2(3), 327–343. https://doi.org/10.1007/s12394-009-0037-z
Bozomitu, R. G., Păsărică, A., Cehan, V., Rotariu, C., & Barabaşa, C. (2015, May). Pupil centre coordinates detection using the circular Hough transform technique. In 2015 38th International Spring Seminar on Electronics Technology (ISSE) (pp. 462-465). IEEE.
Brown, T. (2008). Design thinking. Harvard Business Review, 86(6), 84–92.
Buchenau, M., & Fulton Suri, J. (2000). Experience prototyping. Proceedings of the Conference on Designing Interactive Systems (DIS). https://doi.org/10.1145/347642.347802
Cai W, Chen J, Li M (2018) Exploring the encoding layer and loss function in end-to-end speaker and language recognition system. arXiv preprint arXiv:1804.05160
Campbell, A. G., Becel, L., & Cornuez, C. (2023). Digital Preservation of Experiences in Virtual Worlds: Using Metaverse Worlds to Preserve VR Research Worlds. 2023 IEEE Gaming, Entertainment, and Media Conference (GEM), 1–4. https://doi.org/10.1109/GEM59776.2023.10390043

Canny, J. (1986). A computational approach to edge detection. IEEE Transactions on pattern analysis and machine intelligence, (6), 679-698.
Chang, C.-C., & Le, H.-D. (2016). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Transactions on Wireless Communications, 15 1), 357–366. https://doi.org/10.1109/TWC.2015.2473165
Ching, H. C., & Eswaran, C. (2009, April). A nature based fusion scheme for multimodal biometric person identity verification at a distance. In Proc. ICSAP (pp. 94-97).
Chung JS, Nagrani A, Zisserman A (2018) Voxceleb2: deep speaker recognition. arXiv preprint arXiv:1806.05622
Cohen, J. (1960). A coefficient of agreement for nominal scales. Educational and Psychological Measurement, 20(1), 37–46.
Collis, J., & Hussey, R. (2021). Business research: A practical guide for undergraduate and postgraduate students (5th ed.). Bloomsbury Publishing.
Coyne, E. J., & Weil, T. R. (2013). ABAC and NGAC: Next generation access control for cyber security. Proceedings of the IEEE International Conference on Technologies for Homeland Security, 236–241.
Cui, J., Wang, Y., Tan, T., Ma, L., & Sun, Z. (2004, August). A fast and robust iris localization method based on texture segmentation. In Biometric Technology for Human Identification (Vol. 5404, pp. 401-408). SPIE.
Cunha, B., & Sousa, C. (2021, June). On the Definition of Intelligible IIoT Architectures. In 2021 16th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.
Da Cruz, M. A. A., Rodrigues, J. J. P. C., Al-Muhtadi, J., Korotaev, V. V., & de Albuquerque, V. H. C. (2018). A reference model for Internet of Things middleware. IEEE Internet of Things Journal, 5(2), 871–883. https://doi.org/10.1109/JIOT.2018.2796561
Daftry, S. (2012). Artificial Neural Networks based Classification Technique for Iris Recognition. International Journal of Computer Applications, 57(4).
Dalka, P., & Czyzewski, A. (2010). Human-computer interface based on visual lip movement and gesture recognition. International Journal of Computer Science and Applications, 7(3), 124–139.
Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management Science, 9(3), 458–467.
Darlow LN, Rosman B (2017) Fingerprint minutiae extraction using deep learning. In: 2017 IEEE International Joint Conference on Biometrics (IJCB), pp 22–30. IEEE
Das, A., Ferryman, J., & Heller, K. (2012). Human gait recognition using silhouette-based biometric techniques. Pattern Recognition Letters, 33(14), 1838–1845.
Daugherty, P., & Berthon, B. (2015). Winning with the industrial internet of things: How to accelerate the journey to productivity and growth. Dublín: Accenture.
Daugman, J. (2003). The importance of being random: statistical principles of iris recognition. Pattern recognition, 36(2), 279-291.
Daugman, J. (2004). How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21–30. https://doi.org/10.1109/TCSVT.2003.818350
Daugman, J. (2006). Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proceedings of the IEEE, 94(11), 1927-1935.

Daugman, J. (2007). New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(5), 1167-1175.
Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. IEEE transactions on pattern analysis and machine intelligence, 15(11), 1148-1161.
Dave, J., Khan, A., Gupta, B., Gangwar, A., & Suman, S. (2021, May). Human-computer interaction methodology to attain face liveness detection. In 2021 2nd international conference for emerging technology (INCET) (pp. 1-4). IEEE. V1.14 October 2023 Page 39 of 47 Confirmation of Candidature
De Angeli, A., Athavankar, U., Joshi, A., Coventry, L., & Johnson, G. I. (2004). Introducing ATMs in India: a contextual inquiry. Interacting with Computers, 16(1), 29-44.
De Diego, I. M., Conde, C., Serrano, Á., & Cabello, E. (2009, November). Combination of kernels applied to face verification. In 2009 16th IEEE International Conference on Image Processing (ICIP) (pp. 1241-1244). IEEE.
Dehak, N., Kenny, P. J., Dehak, R., Dumouchel, P., & Ouellet, P. (2011). Front-end factor analysis for speaker verification. IEEE Transactions on Audio, Speech, and Language Processing, 19(4), 788–798. https://doi.org/10.1109/TASL.2010.2064307
Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. Proceedings of CVPR 2019. https://doi.org/10.1109/CVPR.2019.00482
Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 32–37. https://doi.org/10.1109/I-SMAC.2017.8058363
Derhab, A., Belaoued, M., Guerroumi, M., & Khan, F. A. (2020). Two-Factor Mutual Authentication Offloading for Mobile Cloud Computing. IEEE Access, 8, 28956–28969. https://doi.org/10.1109/ACCESS.2020.2971024
Dickinson, H. W., & Musson, A. E. (2022). A short history of the steam engine. Routledge. https://doi.org/10.4324/9780429423123
Dieter Findling, R., & Mayrhofer, R. (2013). Towards pan shot face unlock. International Journal of Pervasive Computing and Communications, 9(3), 190–208. https://doi.org/10.1108/IJPCC-05-2013-0012
Ding, B., Wang, H., Liang, R., Zhang, Y., & Chen, P. (2023). End-to-End Surface and Internal Fingerprint Reconstruction from Optical Coherence Tomography Based on Contour Regression. IEEE Transactions on Information Forensics and Security, 18, 162–176. https://doi.org/10.1109/TIFS.2022.3219345
Dionisio, J. D. N., Burns, W. G., & Gilbert, R. (2013). 3D virtual worlds and the metaverse: Current status and future possibilities. ACM Computing Surveys, 45(3), 34. https://doi.org/10.1145/2480741.2480751
Drygajlo, A. (2008). Biometrics for identity documents and smart cards: European Perspective. Lecture Notes in Computer Science, 236–244. https://doi.org/10.1007/978-3-540-89991-4_25
Du, R., & Zhen, L. (2022). Multiuser physical layer security mechanism in the wireless communication system of the IIOT. Computers & Security, 113, 102559.
Dubey, R. B., & Madan, A. (2014). Iris localization using Daugman's intero-differential operator. International Journal of Computer Applications, 93(3), 06-12.

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. 44th Annual 2010 IEEE International Carnahan Conference on Security Technology. https://doi.org/10.1109/ccst.2010.5678678
El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. Journal of Systems and Software, 118, 64-84.
Elliot, S. J., & colleagues (2007). Privacy, hygiene, and user concerns in biometric authentication systems. International Journal of Human-Computer Studies, 65(8), 650–660. https://doi.org/10.1016/j.ijhcs.2007.03.004
Emer, J., & others (2018). Impact of ear accessories on biometric recognition performance. IEEE International Conference on Biometrics (ICB). https://doi.org/10.1109/ICB.2018.8411210
Emeršič, Ž., Štruc, V., & Peer, P. (2017). Ear recognition: More than a survey. Neurocomputing, 255, 26–39.
Emerson, G., & Lovell, B. C. (2017). Deep learning-based feature averaging for small biometric datasets. IEEE Access, 5, 23514–23525. https://doi.org/10.1109/ACCESS.2017.2751601
Eugster, P. T., Felber, P. A., Guerraoui, R., & Kermarrec, A. M. (2003). The many faces of publish/subscribe. ACM Computing Surveys, 35(2), 114–131.
Eyiokur FI, Yaman D, Ekenel HK (2017) Domain adaptation for ear recognition using deep convolutional neural networks. IET Biom 7(3):199–206
Fairhurst, M. C. (1997). Signature verification revisited: promoting practical exploitation of biometric technology. Electronics & Communication Engineering Journal, 9(6), 273–280. https://doi.org/10.1049/ecej:19970606
Fan C, Peng Y, Cao C, Liu X, Hou S, Chi J, Huang Y, Li Q, He Z (2020) Gaitpart: temporal part-based model for gait recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp 14225–14233
Fan, C., Peng, Y., Cao, C., Liu, X., Hou, S., Chi, J., Huang, Y., Li, Q., & He, Z. (2020). Gaitpart: Temporal part-based model for gait recognition. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 14225–14233.
Fang M, Damer N, Kirchbuchner F, Kuijper A (2021) Demographic bias in presentation attack detection of iris recognition systems. In 2020 28th European Signal Processing Conference (EUSIPCO), pp 835–839. IEEE
Farouk RM (2011) Iris recognition based on elastic graph matching and gabor wavelets. Comput Vis Image Understand 115(8):1239–1244
Fasel, B., & Luettin, J. (2003). Automatic facial expression analysis: A survey. Pattern Recognition, 36(1), 259–275. https://doi.org/10.1016/S0031-3203(02)00052-3
Ferraiolo, D., Gavrila, S., Hu, V. C., & Kuhn, D. R. (2016). Composing and combining policies under the NGAC functional architecture (NISTIR 8112). National Institute of Standards and Technology.
Flatt, H., Schriegel, S., Jasperneite, J., Trsek, H., & Adamczyk, H. (2016). Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), 1–4. https://doi.org/10.1109/ETFA.2016.7733634

Gagan, S., & Lalitha, Y. (2015). Multimodal biometric authentication systems: A survey. International Journal of Computer Applications, 119(2), 20–26.
Gangwar, A., & Joshi, A. (2016). DeepIrisNet: A deep learning approach for iris recognition. arXiv:1606.04809.
Gartner (2023). Metaverse technologies and immersive platform adoption trends. Gartner Research Report.
Genovese, A., Piuri, V., Plataniotis, K. N., & Scotti, F. (2019). PalmNet: Gabor-PCA Convolutional Networks for Touchless Palmprint Recognition. IEEE Transactions on Information Forensics and Security, 14(12), 3160–3174. https://doi.org/10.1109/TIFS.2019.2911165
George, A., & Marcel, S. (2021). Deep learning for iris presentation attack detection: A survey and benchmarking. Pattern Recognition Letters, 143, 29–36. https://doi.org/10.1016/j.patrec.2020.12.004
Ghate, M. D. J., & Patil, S. B. (2015, September). Robust combination method for privacy protection using fingerprint and face biometrics. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-6). IEEE.
Ghazi Zadeh, E. (2018). Evaluating Identity Theft Protections by Trust-Based Model for Cloud Computing (Doctoral dissertation, Auckland University of Technology).
Gnanasekar, S. T., Shaposhnyk, O., Yankovyi, I., & Yanushkevich, S. (2023). Brief audit of postpandemic biometrics. In Lecture Notes in Computer Science (pp. 610–626). Springer. https://doi.org/10.1007/978-3-031-37731-0_44
Gokulavani, D., & Mohana, J. (2023). A Performance Analysis of Different Detection Techniques of Human Eye Pupils. 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), 824–827. https://doi.org/10.1109/ICSCSS57650.2023.10169155
Grossberg, S. (2020). A path toward explainable AI and autonomous adaptive intelligence: deep learning, adaptive resonance, and models of perception, emotion, and action. Frontiers in neurorobotics, 14, 36.
Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.
Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (2010). Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of web services. IEEE Transactions on Services Computing, 3(3), 223–235.
Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Computers & Security, 30(4), 208-220.
Gupta, P., Mehrotra, H., Rattani, A., Chatterjee, A., & Kaushik, A. K. (2006, July). Iris recognition using corner detection. In Proceedings of the 23rd International Biometric Conference, Montreal, Canada (pp. 1-5).
Hajibabaei M, Dai D (2018) Unified hypersphere embedding for speaker recognition. arXiv preprint arXiv:1807.08312
Han, C., Zhang, X., Wang, Y., & Liu, J. (2018). Secure communication architectures for Industrial Internet of Things environments. IEEE Communications Magazine, 56(2), 26–31.
Hankel, M., & Rexroth, B. (2015). The reference architectural model industrie 4.0 (rami 4.0). Zvei, 2(2), 4-9.

Harakannanavar, S. S., & Puranikmath, V. I. (2017, December). Comparative survey of iris recognition. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 280-283). IEEE.
Hansen, J. H. L., & Hasan, T. (2015). Speaker recognition by machines and humans: A tutorial review. IEEE Signal Processing Magazine, 32(6), 74–99.
Haryanti, T., et al. (2022). Design science research approaches in information systems: A review. International Journal of Information Systems and Project Management, 10(2), 45–61.
He, K., Zhang, X., Ren, S., & Sun, J. (2015). Deep residual learning for image recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
He, L., Li, S., & Zhang, Y. (2018). FingerNet: An unified deep network for fingerprint minutiae extraction. IEEE Transactions on Pattern Analysis and Machine Intelligence, 40(12), 2946–2958. https://doi.org/10.1109/TPAMI.2017.2778462
Hehn, J., & Uebernickel, F. (2018). The Use of Design Thinking for Requirements Engineering: An Ongoing Case Study in the Field of Innovative Software-Intensive Systems. 2018 IEEE 26th International Requirements Engineering Conference (RE), 400–405. https://doi.org/10.1109/RE.2018.00-18
Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.
Ho, K. (2018). Virtual worlds and social VR evolution: From MMORPGs to immersive social systems. Journal of Virtual Worlds Research, 11(2), 1–18.
Hofmann, E., & Rüsch, M. (2017). Industry 4.0 and the current status as well as future prospects on logistics. Computers in Industry, 89, 23–34. https://doi.org/10.1016/J.COMPIND.2017.04.002
Holsapple, C. W., & Joshi, K. D. (2002). A collaborative approach to ontology design. Communications of the ACM, 45(2), 42–47. https://doi.org/10.1145/564376.564401
Holsapple, C. W., & Joshi, K. D. (2002). Knowledge manipulation activities: results of a Delphi study. Information & Management, 39(6), 477-490.
Hongye, X., & Zhuoya, H. (2015). Gait recognition based on gait energy image and linear discriminant analysis. 2015 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 1–4. https://doi.org/10.1109/ICSPCC.2015.7338934
Hou, X., Ren, Z., Yang, K., Chen, C., Zhang, H., & Xiao, Y. (2019). IIoT-MEC: A Novel Mobile Edge Computing Framework for 5G-enabled IIoT. 2019 IEEE Wireless Communications and Networking Conference (WCNC), 1–7. https://doi.org/10.1109/WCNC.2019.8885703
Hough, P. V. (1962). U.S. Patent No. 3,069,654. Washington, DC: U.S. Patent and Trademark Office.
Hu VC, Kuhn DR, Ferraiolo DF, Voas J (2015) Attribute-based access control. Computer 48(2):85–88
International Organization for Standardization. (2016). Biometric presentation attack detection (ISO/IEC 30107).
International Organization for Standardization. (2018). Ergonomics of human-system interaction — Usability (ISO 9241-11).

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022).
Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2019). The Internet of Things for health care: A comprehensive survey. IEEE Access, 3, 678–708. https://doi.org/10.1109/ACCESS.2019.2936067
Isnanto, R. R., Zahra, A. A., & Widianto, E. D. (2015). Palmprint recognition system based on principle-lines feature using Euclidean Distance and neural network. 2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), 153–158. https://doi.org/10.1109/ICITACEE.2015.7437789
Israr, N., & Awan, I. U. (2007). Multihop clustering algorithm for load balancing in wireless sensor networks.
Iwama, H., Okumura, M., Makihara, Y., & Yagi, Y. (2012). The OU-ISIR gait database comprising the largest population dataset with age and gender information. IEEE International Conference on Biometrics (ICB). https://doi.org/10.1109/ICB.2012.6199818
Jain, A. K., Dass, S. C., & Nandakumar, K. (2004). Soft biometric traits for personal recognition systems. In Lecture Notes in Computer Science (pp. 731–738). Springer. https://doi.org/10.1007/978-3-540-25948-0_99
Jain, A. K., Dass, S. C., & Nandakumar, K. (2009). Soft biometric traits for personal recognition systems. In Handbook of Multibiometrics. Springer.
Jain, A. K., Deb, D., & Engelsma, J. J. (2022). Biometrics: Trust, But Verify. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(3), 303–323. https://doi.org/10.1109/TBIOM.2021.3115465
Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). Handbook of biometrics. Springer Science & Business Media.
Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80–105.
Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to biometrics. Springer.
Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. https://doi.org/10.1109/tcsvt.2003.818349
Jalali A, Mallipeddi R, Lee M (2015) Deformation invariant and contactless palmprint recognition using convolutional neural network. In: Conference on Human-Agent Interaction. ACM
Jalilian, E., & Uhl, A. (2017). Iris segmentation using fully convolutional encoder–decoder networks. Deep Learning for Biometrics, 133-155.
Jalilian, E., Karakaya, M., & Uhl, A. (2021). CNN-based off-angle iris segmentation and recognition. IET Biometrics, 10(5), 518-535.
Jalilian, E., Wimmer, G., Uhl, A., & Karakaya, M. (2022, May). Deep Learning Based Off-Angle Iris Recognition. In ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4048-4052). IEEE.
Javaid, M., Haleem, A., Singh, R. P., Rab, S., & Suman, R. (2021). Upgrading the manufacturing sector via applications of industrial internet of things (IIoT). Sensors International, 2, 100129.

Javidnia, H., Ungureanu, A., Costache, C., & Corcoran, P. (2016). Palmprint as a smartphone biometric. 2016 IEEE International Conference on Consumer Electronics (ICCE), 463–466. https://doi.org/10.1109/ICCE.2016.7430692
Jerbi, W., Guermazi, A., & Trabelsi, H. (2016, March). O-LEACH of routing protocol for wireless sensor networks. In 2016 13th international conference on computer graphics, imaging and visualization (CGiV) (pp. 399-404). IEEE.
Ji, W., Wang, J., Fang, X., & Gu, S. (2013, June). Improved Delphi method with weighted factor and its application. In 2013 9th Asian Control Conference (ASCC) (pp. 1-5). IEEE.
Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2015). An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-Peer Networking and Applications, 8(6), 1070–1081. https://doi.org/10.1007/s12083-014-0285-z
Jiang, X., Ser, W., Liu, J., & Yan, S. (2016). Iris recognition using deep learning approaches. IEEE Transactions on Information Forensics and Security, 11(4), 879–892.
Johannesson, P., & Perjons, E. (2014). An introduction to design science. Springer. https://doi.org/10.1007/978-3-319-10632-8
Jones, L. A., Antón, A. I., & Earp, J. B. (2007). Towards understanding user perceptions of authentication technologies. Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, 91–98. https://doi.org/10.1145/1314333.1314352 V1.14 October 2023 Page 40 of 47 Confirmation of Candidature
Jones, M. J., & Viola, P. (2006). U.S. Patent No. 7,099,510. Washington, DC: U.S. Patent and Trademark Office.
K, S. K., Sahoo, S., Mahapatra, A., Swain, A. K., & Mahapatra, K. K. (2017). Security Enhancements to System on Chip Devices for IoT Perception Layer. 2017 IEEE International Symposium on Nanoelectronic and Information Systems (INIS), 151–156. https://doi.org/10.1109/iNIS.2017.39
Kang, J. S., Lawryshyn, Y., & Hatzinakos, D. (2020). Neural Network Architecture and Transient Evoked Otoacoustic Emission (TEOAE) Biometrics for Identification and Verification. IEEE Transactions on Information Forensics and Security, 15, 1858–1867. https://doi.org/10.1109/TIFS.2019.2951310
Kantonen, T., Woodward, C., & Katz, N. (2010). Mixed reality in virtual world teleconferencing. 2010 IEEE Virtual Reality Conference (VR), 179–182. https://doi.org/10.1109/VR.2010.5444792
Katal, A., Gupta, P., Wazid, M., Goudar, R. H., Mittal, A., Panwar, S., & Joshi, S. (2013). Authentication and authorization: Domain specific Role Based Access Control using Ontology. 2013 7th International Conference on Intelligent Systems and Control (ISCO), 439–444. https://doi.org/10.1109/ISCO.2013.6481195
Kathiriya, H., Pandya, A., Dubay, V., & Bavarva, A. (2020, June). State of art: energy efficient protocols for self-powered wireless sensor network in IIoT to support industry 4.0. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 1311-1314). IEEE.
Kaudki, O., & Bhurchandi, K. (2018). A Robust Iris Recognition Approach Using Fuzzy Edge Processing Technique. 2018 9th International Conference on

Computing, Communication and Networking Technologies (ICCCNT), 1–6. https://doi.org/10.1109/ICCCNT.2018.8493855
Kaur, G., Yadav, A. K., & Chaudhary, S. (2014). An improved approach to multibiometrics security. Int J Comput Sci Commun, 5(1), 181-187.
Kawulok, M., & Szymanek, J. (2012). Precise multi-level face detector for advanced analysis of facial images. IET image processing, 6(2), 95-103
Kedia, A., Gupta, A., Saha, S., & Shukla, P. K. (2020). Security and privacy issues in Industrial Internet of Things (IIoT): A comprehensive survey. International Journal of Information Security and Privacy, 14(4), 1–21.
Kedia, M., Sekhani, R., & Katiyar, T. (2020). The role of standards in diffusion of emerging technologies Internet of Things (IoT).
Khobragade, S., Mor, D. D., & Chhabra, A. (2015). A method of ear feature extraction for ear biometrics using MATLAB. 2015 Annual IEEE India Conference (INDICON), 1–5. https://doi.org/10.1109/INDICON.2015.7443344
Kim, J., Cho, S., Choi, J., & Marks, R. J. (2004). Iris recognition using wavelet features. Journal of VLSI signal processing systems for signal, image and video technology, 38, 147-156.
Kim, S., Ahn, J., Kim, H., & Park, J. (2016). Fingerprint liveness detection using deep belief networks. Pattern Recognition Letters, 83, 329–336. https://doi.org/10.1016/j.patrec.2016.06.004
Kiran, M. A., Yogeshwari, P., Bhavani, K. V., & Ramya, T. (2018). Biometric Authentication: A Holistic Review. 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference On, 428–433. https://doi.org/10.1109/I-SMAC.2018.8653751
Kissel, R. (2013). Glossary of key information security terms. https://doi.org/10.6028/NIST.IR.7298r2
Kittler, J., et al. (2016). Ear recognition using deep convolutional networks. Pattern Recognition Letters, 74, 1–8. https://doi.org/10.1016/j.patrec.2016.01.009
Kong, A., Zhang, D., & Kamel, M. (2009). A survey of palmprint recognition. Pattern Recognition, 42(7), 1408–1418.
Kosta, B. P., & Sanyasi, P. (2021). Design and Implementation of a Strong and Secure Lightweight Cryptographic Hash Algorithm using Elliptic Curve Concept: SSLHA-160. International Journal of Advanced Computer Science and Applications, 12(2). https://doi.org/10.14569/IJACSA.2021.0120279
Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. Computer Networks, 141, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012
Kowtko, M. A. (2014). Biometric authentication for older adults. IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014. https://doi.org/10.1109/lisat.2014.6845213
Krivokuća Hahn, J., Roos, S., & Busch, C. (2023). Face image protection: A survey on privacy-preserving biometric template protection and face de-identification techniques. ACM Computing Surveys, 55(10), 1–38. https://doi.org/10.1145/3565010
kumar Dewangan, A., & Siddhiqui, M. A. (2012). Human identification and verification using iris recognition by calculating hamming distance. International Journal of Soft Computing and Engineering(IJSCE), 2(2).

Kumar, A., & Kanhangad, V. (2015). Human identification using palm vein images. IEEE Transactions on Information Forensics and Security, 10(4), 847–859.
Kumar, P., & Lee, H.-J. (2011). Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors, 12(1), 55–91. https://doi.org/10.3390/s120100055
Kumar, S., Chandra, S. K., Shukla, R. N., & Panigrahi, L. (2023). Industry 4.0 based Machine Learning Models for Anomalous Product Detection and Classification. 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), 1–6.
Kusakunniran W, Qiang W, Zhang J, Li H, Wang L (2013) Recognizing gaits across views through correlated motion co-clustering. IEEE Trans Image Process 23(2):696–709
Kwon, J., & Hudson-Smith, A. (2018). Social VR and immersive communication systems. Computers in Human Behavior, 85, 123–134.
Lee, C. J., & Wang, S. D. (1999). Fingerprint feature extraction using Gabor filters. Proceedings of the 1999 International Conference on Image Processing (ICIP). IEEE.
Lee, M. J., Jin, Z., Liang, S.-N., & Tistarelli, M. (2022). Alignment-robust cancelable biometric scheme for iris verification. IEEE Transactions on Information Forensics and Security, 17, 3449–3464. https://doi.org/10.1109/TIFS.2022.3208812
Lei Y, Scheffer N, Ferrer L, McLaren M (2014) A novel scheme for speaker recognition using a phonetically-aware deep neural network. In International Conference on Acoustics, Speech and Signal Processing, pp 1695–1699. IEEE
Li, G., Busch, C., & Yang, B. (2014a). A novel approach used for measuring fingerprint orientation of arch fingerprint. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1309–1314. https://doi.org/10.1109/MIPRO.2014.6859770
Li, G., Busch, C., & Yang, B. (2014b). A novel approach used for measuring fingerprint orientation of arch fingerprint. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1309–1314. https://doi.org/10.1109/MIPRO.2014.6859770
Li, W., Cheng, H., Wang, P., & Liang, K. (2021). Practical Threshold Multi-Factor Authentication. IEEE Transactions on Information Forensics and Security, 16, 3573–3588. https://doi.org/10.1109/TIFS.2021.3081263
Li, X., Makihara, Y., Xu, C., Yagi, Y., & Ren, M. (2020). Gait recognition via disentangled representation learning. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42(10), 2723–2737. https://doi.org/10.1109/TPAMI.2019.2937229
Li, X., Peng, J., Niu, J., Wu, F., Liao, J., & Choo, K.-K. R. (2018). A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. IEEE Internet of Things Journal, 5(3), 1606–1615. https://doi.org/10.1109/JIOT.2017.2787800
Liao R, Shiqi Y, An W, Huang Y (2020) A model-based gait recognition method with body pose and human prior knowledge. Pattern Recognit 98:107069
Likert, R. (1932). A technique for the measurement of attitudes. Archives of Psychology, 22(140), 1–55.

Lin C, Kumar A (2017) Multi-siamese networks to accurately match contactless to contact-based fingerprint images. In: International Joint Conference on Biometrics (IJCB), pp 277–285. IEEE
Lin C, Kumar A (2018) Contactless and partial 3d fingerprint recognition using multi-view deep representation. Pattern Recognit 83:314–327
Lin, H.-I., & Ho, Y.-C. (2019). Adaptive Gain Control for a Steady Human-Robot Cooperation. 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), 325–330. https://doi.org/10.1109/ICPHYS.2019.8780293
Lin, S. W., Miller, B., Durand, J., Joshi, R., Didier, P., Chigani, A., ... & Witten, B. (2015). Industrial internet reference architecture. Industrial Internet Consortium (IIC), Tech. Rep.
Linstone, H. A., & Turoff, M. (Eds.). (1975). The Delphi method: Techniques and applications. Addison-Wesley.
Lipps, C., Herbst, J., & Schotten, H. D. (2021, February). How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments. In ICCWS 2021 16th International Conference on Cyber Warfare and Security (p. 168). Academic Conferences Limited.
Liu W, Wen Y, Yu Z, Li M, Raj B, Song L (2017) Sphereface: Deep hypersphere embedding for face recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 212–220
Liu, M., Li, X., Li, J., Liu, Y., Zhou, B., & Bao, J. (2022). A knowledge graph-based data representation approach for IIoT-enabled cognitive manufacturing. Advanced Engineering Informatics, 51, 101515.
Liu, Y., & Long, Y. (2016, May). Image edge extraction based on fuzzy theory and Sobel operator. In 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 373-378). IEEE.
Lu, H. K., & Ali, A. (2008). Communication Security between a Computer and a Hardware Token. Third International Conference on Systems (Icons 2008), 220–225. https://doi.org/10.1109/ICONS.2008.36
Lu, X., Pan, Z., & Xian, H. (2020). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. Computers & Security, 92, 101686. https://doi.org/10.1016/j.cose.2019.101686
Lu, Y., Xu, X., & Wang, L. (2020). Smart manufacturing process and system automation–a critical review of the standards and envisioned scenarios. Journal of Manufacturing Systems, 56, 312325.
Lucia, C., Zhiwei, G., & Michele, N. (2023). Biometrics for Industry 4.0: a survey of recent applications. Journal of Ambient Intelligence and Humanized Computing, 1-23.
Luckham, D. C. (2011). Event processing for business: Organizing the real-time enterprise. Wiley.
Ma, L., Tan, T., Wang, Y., & Zhang, D. (2004). Efficient iris recognition by characterizing key local variations. IEEE Transactions on Image processing, 13(6), 739-750.
Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (2nd ed.). Springer.
Mahmud, R., Kotagiri, R., & Buyya, R. (2020). Fog computing: A taxonomy, survey and future directions. In Internet of Everything (pp. 103–130). Springer.

Maity, S., & Abdel-Mottaleb, M. (2015). 3D Ear Segmentation and Classification Through Indexing. IEEE Transactions on Information Forensics and Security, 10(2), 423–435. https://doi.org/10.1109/TIFS.2014.2379437

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Industrial and critical infrastructure security: Technical analysis of real-life security incidents. IEEE Access, 9, 165295–165325. https://doi.org/10.1109/ACCESS.2021.3133348

Manjeshwar, A., & Agrawal, D. P. (2001, April). TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks. In ipdps (Vol. 1, No. 2001, p. 189).

Manjunathswamy B E, Thriveni J, & Venugopal K R. (2015). Bimodal biometric verification mechanism using fingerprint and face images(bbvmff). 2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS). https://doi.org/10.1109/iciinfs.2015.7399040 V1.14 October 2023 Page 41 of 47 Confirmation of Candidature

Mantravadi, S., Møller, C., LI, C., & Schnyder, R. (2022). Design choices for next-generation IIoT connected MES/MOM: An empirical study on smart factories. Robotics and Computer-Integrated Manufacturing, 73, 102225. https://doi.org/10.1016/j.rcim.2021.102225

Mao, K., et al. (2023). Design science research in information systems: A systematic review. Information & Management, 60(4), 103741. https://doi.org/10.1016/j.im.2023.103741

Marin-Jimenez, M. J., Castro, F. M., Guil, N., de la Torre, F., & Medina-Carnicer, R. (2017). Deep multitask learning for gait-based biometrics. 2017 IEEE International Conference on Image Processing (ICIP), 106–110. https://doi.org/10.1109/ICIP.2017.8296252

Marr, B. (2021, December 10). 8 Industrial IoT (IIoT) Security Risks & Solutions. Forbes. https://www.forbes.com/sites/bernardmarr/2020/01/27/8-industrial-iot-iiot-security-risks--solutions/?sh=1561a1415cda

Marras, F., Fenu, G., & Roli, F. (2023). Adversarial vector-dictionary attacks against speaker recognition systems. IEEE Transactions on Information Forensics and Security, 18, 3456–3470. https://doi.org/10.1109/TIFS.2023.3245678

Masek, L. (2003). *Recognition of human iris patterns for biometric identification* (BEng thesis). University of Western Australia.

Matey, J. R., Naroditsky, O., Hanna, K., Kolczynski, R., LoIacono, D. J., Mangru, S., et al. (2006). Iris on the move: Acquisition of images for iris recognition in less constrained environments. *Proceedings of the IEEE, 94*(11), 1936–1947

Mathur, S., & Arora, A. (2020). Internet of things (IoT) and PKI-based security architecture. In Industrial internet of things and cyber-physical systems: transforming the conventional to digital (pp. 25-46). IGI Global.

Mcginthy, J. M., & Michaels, A. J. (2019). Secure Industrial Internet of Things Critical Infrastructure Node Design. IEEE Internet of Things Journal, 6(5), 8021–8037. https://doi.org/10.1109/JIOT.2019.2903242

McKenna H.P. (1994) The Delphi technique: a worthwhile approach for nursing? Journal of Advanced Nursing 19, 1221– 1225.

McVeigh-Schultz, J., et al. (2018). Social presence in virtual reality: Design implications. Proceedings of CHI 2018.

Menon H, Mukherjee A (2018) Iris biometrics using deep convolutional networks. In: 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), pp 1–5. IEEE

Michele, A., Colin, V., & Santika, D. D. (2019). Mobilenet convolutional neural networks and support vector machines for palmprint recognition. Procedia Computer Science, 157, 110–117.

Mihailescu, M. I., & Loredana Nita, S. (2020). Three-factor authentication scheme based on searchable encryption and biometric fingerprint. 2020 13th International Conference on Communications (COMM), 139–144. https://doi.org/10.1109/COMM48946.2020.9141956

Mikaelyan, A., Alonso-Fernandez, F., & Bigun, J. (2014). Periocular Recognition by Detection of Local Symmetry Patterns. 2014 Tenth International Conference on Signal-Image Technology and Internet-Based Systems, 584–591. https://doi.org/10.1109/SITIS.2014.105

Miller, R., Banerjee, N. K., & Banerjee, S. (2020, March). Within-system and cross-system behaviorbased biometric authentication in virtual reality. In 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW) (pp. 311-316). IEEE.

Miller, R., Banerjee, N. K., & Banerjee, S. (2021, March). Using siamese neural networks to perform cross-system behavioral authentication in virtual reality. In 2021 IEEE Virtual Reality and 3D User Interfaces (VR) (pp. 140-149). IEEE.

Miller, R., Banerjee, N. K., & Banerjee, S. (2022, March). Combining real-world constraints on user behavior with deep neural networks for virtual reality (vr) biometrics. In 2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR) (pp. 409-418). IEEE.

Minaee S, Abdolrashidi A (2019) Deepiris: Iris recognition using a deep learning approach. arXiv preprint arXiv:1907.09380

Minaee S, Abdolrashidi AA, Wang Y (2015) Iris recognition using scattering transform and textural features. In: Signal processing and signal processing education workshop, pp 37–42. IEEE

Minaee S, Abdolrashidiy A, Wang Y (2016) An experimental study of deep convolutional features for iris recognition. In: Signal processing in medicine and biology symposium, pp 1–6. IEEE

Minaee S, Azimi E, Abdolrashidi A (2019) Fingernet: pushing the limits of fingerprint recognition using convolutional neural network. arXiv preprint arXiv:1907.12956

Minaee S, Wang Y (2017) Palmprint recognition using deep scattering network. In: International Symposium on Circuits and Systems (ISCAS). IEEE

Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: a survey. Artificial Intelligence Review, 56(8), 8647–8695. https://doi.org/10.1007/s10462-022-10237-x

Mohammed, R. A., Nabi, R. M., Mahmood, S. M.-R., & Nabi, R. M. (2015). State-of-the-Art in Handwritten Signature Verification System. 2015 International Conference on Computational Science and Computational Intelligence (CSCI), 519–525. https://doi.org/10.1109/CSCI.2015.180

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Muramatsu, D., Makihara, Y., & Yagi, Y. (2015). View transformation model incorporating quality measures for cross-view gait recognition. IEEE Transactions on Cybernetics, 46(7), 1602–1615.
Nakamura, E. T., & Ribeiro, S. L. (2018). A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems. 2018 Global Internet of Things Summit (GIoTS), 1–6. https://doi.org/10.1109/GIOTS.2018.8534521
Nalla, P. R., & Kumar, A. (2017). Toward More Accurate Iris Recognition Using Cross-Spectral Matching. IEEE Transactions on Image Processing, 26(1), 208–221. https://doi.org/10.1109/TIP.2016.2616281
Navarro-Ortiz, J., Sendra, S., Ameigeiras, P., & Lopez-Soler, J. M. (2018). Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things. IEEE Communications Magazine, 56(2), 60-67.
Nesa, N., & Banerjee, I. (2020). A lightweight security protocol for IoT using Merkle hash tree and chaotic cryptography. In Lecture Notes in Networks and Systems (pp. 3–16). Springer. https://doi.org/10.1007/978-981-13-8969-6_1
Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, April). The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268).
Nguyen, K., Fookes, C., & Sridharan, S. (2020). Constrained Design of Deep Iris Networks. IEEE Transactions on Image Processing, 29, 7166–7175. https://doi.org/10.1109/TIP.2020.2999211
Nguyen, K., Fookes, C., Ross, A., & Sridharan, S. (2017). Iris recognition with CNNs under unconstrained conditions. IEEE Access, 5, 14314–14325. https://doi.org/10.1109/ACCESS.2017.2722002
Nogueira, R. F., de Alencar Lotufo, R., & Machado, R. C. (2016). Fingerprint liveness detection using convolutional neural networks. IEEE Transactions on Information Forensics and Security, 11(6), 1201–1213. https://doi.org/10.1109/TIFS.2016.2520889
Okabe K, Koshinaka T, Shinoda K (2018) Attentive statistics pooling for deep speaker embedding. arXiv preprint arXiv:1803.10963
Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. Information & management, 42(1), 15-29.
Oloyede, M. O., & Hancke, G. P. (2016). Unimodal and multimodal biometric sensing systems: a review. IEEE access, 4, 7532-7555.
Omara I, Xiaohe W, Zhang H, Yong D, Zuo W (2018) Learning pairwise SVM on hierarchical deep features for ear recognition. IET Biom 7(6):557–566
Ondrejka, C. (2008). Education unleashed: Participatory culture, education, and Second Life. The International Journal of Learning, 14(12), 1–9.
Oravec, M. (2014, September). Feature extraction and classification by machine learning methods for biometric recognition of face and iris. In Proceedings ELMAR-2014 (pp. 1-4). IEEE.
Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. EURASIP Journal on Wireless Communications and Networking, 2016(1), 130. https://doi.org/10.1186/s13638-016-0623-3

Padma, P., & Srinivasan, S. (2016). A survey on biometric based authentication in cloud computing. 2016 International Conference on Inventive Computation Technologies (ICICT), 1–5. https://doi.org/10.1109/INVENTIVE.2016.7823273

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. International Journal of Surgery, 88, Article 105906. https://doi.org/10.1186/s13643-021-01626-4

Pandya B, Cosma G, Alani AA, Taherkhani A, Bharadi V, McGinnity TM (2018) Fingerprint classification using a deep convolutional neural network. In: 2018 4th International Conference on Information Management (ICIM), pp 86–91. IEEE

Pandya, B., Cosma, G., Alani, A. A., Taherkhani, A., Bharadi, V., & McGinnity, T. M. (2018). Fingerprint classification using a deep convolutional neural network. 2018 4th International Conference on Information Management (ICIM), 86–91. IEEE.

Panetto, H., & Cecil, J. (2013). Information systems for enterprise integration, interoperability and networking: Theory and applications. Enterprise Information Systems, 7(1), 1–6.

Park, U., Jillela, R. R., Ross, A., & Jain, A. K. (2011). Periocular biometrics in the visible spectrum. IEEE Transactions on Information Forensics and Security, 6(1), 96–106. https://doi.org/10.1109/TIFS.2010.2096810

Parkhi OM, Vedaldi A, Zisserman A et al. (2015) Deep face recognition. In: bmvc, volume 1,

Parkhi, O. M., Vedaldi, A., Zisserman, A., et al. (2015). Deep face recognition. BMVC, Volume 1.

Paulraj, D., Swamynathan, S., & Madhaiyan, M. (2023). Deep learning enabled authentication frameworks for Industry 4.0 systems. Future Generation Computer Systems, 141, 109–124.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology. Journal of Management Information Systems, 24(3), 45–77.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pesonen LI, Eyers DM, Bacon J (2006) A capability-based access control architecture for multi-domain publish/subscribe systems. In: International Symposium on Applications and the Internet, SAINT 2006, 7 pp

Petrenko, A. S., Makoveichuk, K. A., & Chetyrbok, P. V. (2018). The IIoT/IoT device control model based on narrow-band IoT (NB-IoT). 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 950–953. https://doi.org/10.1109/EIConRus.2018.8317246

Plattner, H., Meinel, C., & Leifer, L. (2009). Design thinking: Understand – improve – apply. Springer.

Podder, P., Parvez, A. H. M. S., Yeasmin, Most. N., & Khalil, Md. I. (2018). Relative Performance Analysis of Edge Detection Techniques in Iris Recognition System. 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), 1–6. https://doi.org/10.1109/ICCTCT.2018.8551023

Prakash, J., Yu, C. C. Q., Thombre, T. R., Bytes, A., Jubur, M., Saxena, N., Blessing, L., Zhou, J., & Quek, T. Q. S. (2021). Countering Concurrent Login Attacks in "Just Tap" Push-based Authentication: A Redesign and Usability Evaluations. 2021 IEEE European Symposium on Security and Privacy (EuroS&P), 21–36. https://doi.org/10.1109/EuroSP51992.2021.00013

Pramana, M. D., Lestyea, A., & Amiruddin, A. (2020). Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token. 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 52–57. https://doi.org/10.1109/ICIMCIS51567.2020.9354328

Purnamasari, A. I., & Setiawan, A. (2019). Pengembangan Passive Infrared Sensor (PIR) HC-SR501 dengan Microcontrollers ESP32-CAM Berbasiskan Internet of Things (IoT) dan Smart Home sebagai Deteksi Gerak untuk Keamanan Perumahan. Prosiding SISFOTEK, 3(1), 148 - 154. Retrieved from http://seminar.iaii.or.id/index.php/SISFOTEK/article/view/118

Qin, J., Liu, Y., & Grosvenor, R. (2016). A Categorical Framework of Manufacturing for Industry 4.0 and beyond. Procedia CIRP, 52, 173–178. https://doi.org/10.1016/J.PROCIR.2016.08.005 V1.14 October 2023 Page 42 of 47 Confirmation of Candidature

Qin, X., Huang, Y., Yang, Z., & Li, X. (2019). An access control scheme with fine-grained time constrained attributes based on smart contract and trapdoor. 2019 26th International Conference on Telecommunications (ICT), 249–253. https://doi.org/10.1109/ICT.2019.8798859

Qing, L., Zhu, Q., & Wang, M. (2006). Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Computer Communications, 29(12), 2230-2237.

Qu, Y., Pokhrel, S. R., Garg, S., Gao, L., & Xiang, Y. (2020). A blockchain federated learning framework for cognitive computing in industry 4.0 networks. IEEE Transactions on Industrial Informatics, 17(4), 2964-2973.

Rafik, H. D., & Boubaker, M. (2020). Application of metaheuristic for optimization of iris Image segmentation by using evaluation Hough Transform and methods Daugman. 020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP), 142–150. https://doi.org/10.1109/CCSSP49278.2020.9151617

Raghavender Jillela, Arun Ross, Vishnu Naresh Boddeti, B. V. K. Vijaya Kumar, Xiaofei Hu, Robert Plemmons, Paul Pauca (2002). "An Evaluation of Iris Segmentation Algorithms in Challenging Periocular Images".

Ramesh, Kumar. P., & Rao, K. N. (2009). Pattern extraction methods for ear biometrics - A survey. 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), 1657–1660. https://doi.org/10.1109/NABIC.2009.5393639

Rasco, A. J. A. O., Chan, J., Peko, G. M., & Sundaram, D. (2020). Serious Financial Games for Youth: An Evolutionary Action Design Science Approach. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3675287

Rasheed, M. B., Javaid, N., Khan, Z. A., Qasim, U., & Ishfaq, M. (2013, May). E-HORM: An energy-efficient hole removing mechanism in Wireless Sensor Networks. In 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1-4). IEEE.

Ravanelli M, Bengio Y (2018) Learning speaker representations with mutual information. arXiv preprint arXiv:1812.00271

Razzak, M. I., Yusof, R., & Khalid, M. (2010). Multimodal face and finger veins biometric authentication. Scientific Research and Essays, 5(17), 2529-2534.

Rehman, A., & Saba, T. (2014). Evaluation of biometric systems based on fingerprint and palmprint recognition. Neural Computing and Applications, 25(2), 349–360.

Ren, M., Wang, Y., Sun, Z., & Tan, T. (2020). Dynamic Graph Representation for Occlusion Handling in Biometrics. Proceedings of the AAAI Conference on Artificial Intelligence, 34(07), 11940–11947. https://doi.org/10.1609/aaai.v34i07.6869

Ren, M., Zhu, Y., Wang, Y., & Sun, Z. (2022). Perturbation Inactivation Based Adversarial Defense for Face Recognition. IEEE Transactions on Information Forensics and Security, 17, 2947–2962. https://doi.org/10.1109/TIFS.2022.3195384

Rida I, Herault R, Marcialis GL, Gasso G (2019) Palmprint recognition with an efficient data driven ensemble classifier. Pattern Recognit Lett 126:21–30

Ross, A., & Jain, A. K. (2003). Information fusion in biometrics. Pattern Recognition Letters, 24(13), 2115–2125.

Rowe, G., & Wright, G. (2001). Expert opinions in forecasting: The role of the Delphi technique. In J. S. Armstrong (Ed.), Principles of forecasting (pp. 125–144). Springer. https://doi.org/10.1007/978-0-306-47630-3_7

Rudrapal, D., Das, S., Debbarma, S., Kar, N., & Debbarma, N. (2012). Voice recognition and authentication as a proficient biometric tool and its application in online exam for PH people. International Journal of Computer Applications, 39(12), 6-12.

Saaty, T. L. (1980). The analytic hierarchy process. McGraw-Hill.

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. Proceedings of the 52nd Design Automation Conference (DAC), 1–12. ACM. https://doi.org/10.1145/2744769.2747942

Saffie, N. A. M., & Rasmani, K. A. (2016, July). Fuzzy delphi method: Issues and challenges. In 2016 International Conference on Logistics, Informatics and Service Sciences (LISS) (pp. 1-7). IEEE.

Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Lecture Notes in Computer Science (pp. 457–473). Springer. https://doi.org/10.1007/11426639_27

Salonikias S, Mavridis I, Gritzalis D (2015) Access control issues in utilizing fog computing for transport infrastructure. In: International Conference on Critical Information Infrastructures Security. Springer, pp 15–26

Salonikias, S., Gouglidis, A., Mavridis, I., & Gritzalis, D. (2019). Access control in the industrial internet of things. Security and privacy trends in the industrial internet of things, 95-114.

Sammoud, A., Chalouf, M. A., Hamdi, O., Montavont, N., & Bouallegue, A. (2020). A secure and lightweight three-factor authentication and key generation scheme for direct communication between healthcare professionals and

patient's WMSN. Proceedings of the IEEE Symposium on Computers and Communications (ISCC), 1–7.
Saqib, M., & Moon, A. H. (2023). A systematic security assessment and review of Internet of Things in the context of authentication. Computers & Security, 125, 103053. https://doi.org/10.1016/j.cose.2022.103053
Sarkar, S., Phillips, P. J., Liu, Z., Vega, I. R., Grother, P., & Bowyer, K. W. (2005). The humanID gait challenge problem: Data sets, performance, and analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(2), 162–177.
Sardar, A., Umer, S., Rout, R. K., & Khan, M. K. (2022). A Secure and Efficient Biometric Template Protection Scheme for Palmprint Recognition System. IEEE Transactions on Artificial Intelligence, 1–13. https://doi.org/10.1109/TAI.2022.3188596
Sarjan, H., Ameli, A., & Ghafouri, M. (2022). Cyber-Security of Industrial Internet of Things in Electric Power Systems. IEEE Access, 10, 92390–92409. https://doi.org/10.1109/ACCESS.2022.3202914
Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30–39.
Scavarelli, A., Arya, A., & Teather, R. J. (2021). Virtual reality and augmented reality in social learning spaces: a literature review. Virtual Reality, 25(1), 257–277. https://doi.org/10.1007/s10055-02000444-8
Schmidt, C. (2004). The analysis of semi-structured interviews. In E. v. Uwe Flick, A companion to qualitative research (pp. 253-258). Sage Publications, Inc.
Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques. Decision Sciences, 28(3), 763–774. https://doi.org/10.1111/j.1540-5915.1997.tb01330.x
Schroff F, Kalenichenko D, Philbin J (2015) Facenet: a unified embedding for face recognition and clustering. In: IEEE conference on computer vision and pattern recognition, pp 815–823
Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. IEEE Conference on Computer Vision and Pattern Recognition, 815–823.
Sequeira, A., Chen, L., Wild, P., Ferryman, J., Alonso-Fernandez, F., Raja, K. B., Raghavendra, R., Busch, C., & Bigun, J. (2016). Cross-Eyed - Cross-Spectral Iris/Periocular Recognition Database and Competition. 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), 1–5. https://doi.org/10.1109/BIOSIG.2016.7736915
Sezer, O. B., Dogdu, E., & Ozbayoglu, A. M. (2018). Context-aware computing, learning, and big data in Internet of Things: A survey. IEEE Internet of Things Journal, 5(1), 1–27. https://doi.org/10.1109/JIOT.2017.2773600
Shah, S., & Ross, A. (2009). Iris segmentation using geodesic active contours. IEEE Transactions on Information Forensics and Security, 4(4), 824-836.
Shao H, Zhong D (2019) Few-shot palmprint recognition via graph neural networks. Electron Lett 55(16):890–892
Shao H, Zhong D, Du X (2019) Efficient deep palmprint recognition via distilled hashing coding. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops
Shao, H., & Zhong, D. (2019). Few-shot palmprint recognition via graph neural networks. Electronics Letters, 55(16), 890–892.

Shao, H., Zhong, D., Du, X., Du, S., & Veldhuis, R. N. J. (2021). Few-Shot Learning for Palmprint Recognition via Meta-Siamese Network. IEEE Transactions on Instrumentation and Measurement, 70, 1–12. https://doi.org/10.1109/TIM.2021.3076850

Shao, Y. Zou, C. Liu, Q. Guo and D. Zhong, "Learning to Generalize Unseen Dataset for Cross-Dataset Palmprint Recognition," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3788-3799, 2024, doi: 10.1109/TIFS.2024.3371257.

Shekhar, S., Kumar, B. S., & Ramesh, S. (2012). Robust approach for palm (ROI) extraction in palmprint recognition system. 2012 IEEE International Conference on Engineering Education: Innovative Practices and Future Trends (AICERA), 1–6. https://doi.org/10.1109/AICERA.2012.6306747

Shen, L., Bai, L., & Ji, Z. (2011). FPCODE: An efficient approach for multi-modal biometrics. International Journal of Pattern Recognition and Artificial Intelligence, 25(02), 273-286.

Shen, M., Yu, H., Zhu, L., Xu, K., Li, Q., & Hu, J. (2021). Effective and Robust Physical-World Attacks on Deep Learning Face Recognition Systems. IEEE Transactions on Information Forensics and Security, 16, 4063–4077. https://doi.org/10.1109/TIFS.2021.3102492

Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C. M. (2015). Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT. IEEE Access, 3, 622–637. https://doi.org/10.1109/ACCESS.2015.2435000

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.

Shon S, Tang H, Glass J (2018) Frame-level speaker embeddings for text-independent speaker recognition and analysis of end-to-end model. In: Spoken Language Technology Workshop (SLT). IEEE

Shrestha, B., Mohamed, M., & Saxena, N. (2019). ZEMFA: Zero-Effort Multi-Factor Authentication based on Multi-Modal Gait Biometrics. 2019 17th International Conference on Privacy, Security and Trust (PST), 1–10. https://doi.org/10.1109/PST47121.2019.8949032

Singhal, A., Mishra, A., & Singh, P. (2014). Iris recognition system using improved normalization and feature matching techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 122–128.

Sinha H, Manekar R, Sinha Y, Ajmera PK (2019) Convolutional neural network-based human identification using outer ear images. In: Soft Computing for Problem Solving, pp 707–719. Springer

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Transactions on Industrial Informatics, 14(11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

Slater, M., & Sanchez-Vives, M. V. (2016). Enhancing our lives with immersive virtual reality. Frontiers in Robotics and AI, 3, 74. https://doi.org/10.3389/frobt.2016.00074

Snyder, D., Garcia-Romero, D., McCree, A., Sell, G., Povey, D., & Khudanpur, S. (2018). X-vectors: Robust DNN embeddings for speaker recognition. IEEE ICASSP. https://doi.org/10.1109/ICASSP.2018.8461375

Soltane, M., Doghmane, N., & Guersi, N. (2010). Face and speech based multi-modal biometric authentication. International Journal of Advanced Science and Technology, 21(6), 41–56.
Srikrishna M, & Nirmala G. (2023). Realization of Human Eye Pupil Detection System using Canny Edge Detector and Circular Hough Transform Technique.
Srinivasan, A., & Balamurugan, V. (2014). Occlusion detection and image restoration in 3D face image. TENCON 2014 - 2014 IEEE Region 10 Conference, 1–6. https://doi.org/10.1109/TENCON.2014.7022477
Štepec D, Emeršič Ž, Peer P, Štruc V (2020) Constellation-based deep ear recognition. In Deep Biometrics, pp 161–190. Springer
Stevens, S. S. (1946). On the theory of scales of measurement. Science, 103(2684), 677–680.
Sun Y, Chen Y, Wang X, Tang X (2014) Deep learning face representation by joint identification verification. In: Advances in neural information processing systems, pp 1988–1996
Sun Y, Liang D, Wang X, Tang X (2015) Deepid3: face recognition with very deep neural networks. arXiv preprint arXiv:1502.00873 V1.14 October 2023 Page 43 of 47 Confirmation of Candidature
Sun Y, Wang X, Tang X (2014) Deep learning face representation from predicting 10,000 classes. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 1891–1898
Sun Y, Wang X, Tang X, (2016) Sparsifying neural network connections for face recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 4856–4864
Sung, H., Lim, J., Park, J. H., & Lee, Y. (2004, August). Iris recognition using collarette boundary localization. In Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004. (Vol. 4, pp. 857-860). IEEE.
Taigman Y, Yang M, Ranzato M, Wolf L (2014) Deepface: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 1701–1708
Tang Y, Gao F, Feng J, Liu Y (2017) Fingernet: an unified deep network for fingerprint minutiae extraction. In: 2017 IEEE International Joint Conference on Biometrics (IJCB), pp 108–116. IEEE
Tang, Y., et al. (2019). MENet: Mobile deep fingerprint recognition network. Pattern Recognition, 90 221–233. https://doi.org/10.1016/j.patcog.2019.01.019
Tange, K., De Donno, M., Fafoutis, X., & Dragoni, N. (2020). A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. IEEE Communications Surveys & Tutorials, 22(4), 2489-2520.
Tassabehji, R., & Kamala, M. A. (2009). Improving E-Banking Security with Biometrics: Modelling User Attitudes and Acceptance. 2009 3rd International Conference on New Technologies, Mobility and Security, 1–6. https://doi.org/10.1109/NTMS.2009.5384806
Thakur, S., Gupta, B., Mathur, U., & Bansal, D. (2023). Ultimate Usability and User Experience in Electronic Health Records: Designing User-Friendly Features for EHRs. 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), 1726–1731. https://doi.org/10.1109/ICAISS58487.2023.10250723

Tian L, Mu Z (2016) Ear recognition based on deep convolutional network. In: International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, pp 437–441. IEEE

Tico, M., Kuosmanen, P., & Saarinen, J. (2001). Fingerprint feature extraction using Gabor filters. Proceedings of the IEEE International Conference on Image Processing (ICIP).

Tisse, C. L., Martin, L., Torres, L., & Robert, M. (2002, May). Person identification technique using human iris recognition. In Proc. Vision Interface (Vol. 294, No. 299, pp. 294-299).

Triantaphyllou, E. (2000). Multi-criteria decision-making methods: A comparative study. Kluwer Academic

Turkanović, M., Brumen, B., & Heričko, M. (2014). Secure authentication model using biometrics and smart cards. Journal of Network and Computer Applications, 44, 89–101.

V. Alcácer and V. Cruz-Machado. (2019). Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems. Engineering Science and Technology an International Journal, 22(3), 99–8919.

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A glimpse. Procedia Manufacturing, 20, 233–238. https://doi.org/10.1016/J.PROMFG.2018.02.034

Van Hamme, H., Marcel, S., & others (2021). Security analysis of IMU-based biometric gait authentication systems. Pattern Recognition Letters, 145, 75–82. https://doi.org/10.1016/j.patrec.2021.01.018

Variani E, Lei X, McDermott E, Moreno IL, Gonzalez-Dominguez J (2014) Deep neural networks for small footprint text-dependent speaker verification. In: International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE

Vatsa, M., Singh, R., & Noore, A. (2008). Reducing the false rejection rate of iris recognition using textural and topological features. International Journal of Computer and Information Engineering, 2(7), 2533-2539.

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. Information Management & Computer Security, 16(4), 415–430. https://doi.org/10.1108/09685220810908813

Vhaduri, Sudip & Poellabauer, Christian. (2017). Wearable device user authentication using physiological and behavioral metrics. 1-6. 10.1109/PIMRC.2017.8292272. M, S., & G, N. (2023). Realization of Human Eye Pupil Detection System using Canny Edge Detector and Circular Hough Transform Technique. 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 861–865. https://doi.org/10.1109/ICAAIC56838.2023.10140671

Verma, O. P., Jain, V., & Gumber, R. (2013). Simple fuzzy rule based edge detection. Journal of Information Processing Systems, 9(4), 575-591.

W. Gong, X. Zhang, B. Deng and X. Xu, "Palmprint Recognition Based on Convolutional Neural Network-Alexnet," *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Leipzig, Germany, 2019, pp. 313-316, doi: 10.15439/2019F248

Wan, C., Wang, L., & Phoha, V. V. (2018). A survey on gait recognition. ACM Computing Surveys, 51(5), Article 89.

Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M., & Vasilakos, A. V. (2018). Software-defined industrial Internet of Things in the context of Industry 4.0. IEEE Sensors Journal, 16(20), 7373–7380.

Wang X, Zhang S, Wang S, Tianyu F, Shi H, Mei T (2020) Mis-classified vector guided softmax loss for face recognition. Proc AAAI Conf Artif Intell 34:12241–12248

Wang, C., Wang, Y., Zhang, K., Muhammad, J., Lu, T., Zhang, Q., Tian, Q., He, Z., Sun, Z., Zhang, Y., Liu, T., Yang, W., Wu, D., Liu, Y., Zhou, R., Wu, H., Zhang, H., Wang, J., Wang, J., … Noshad, M. (2021). NIR Iris Challenge Evaluation in Non-cooperative Environments: Segmentation and Localization. 2021 IEEE International Joint Conference on Biometrics (IJCB), 1–10. https://doi.org/10.1109/IJCB52358.2021.9484336

Wang, D., & Wang, P. (2014). Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. Ad Hoc Networks, 20, 1–15. https://doi.org/10.1016/j.adhoc.2014.03.003

Wang, H., Zhou, B., & Zhang, X. (2018). Research on the Remote Maintenance System Architecture for the Rapid Development of Smart Substation in China. IEEE Transactions on Power Delivery, 33(4), 1845–1852. https://doi.org/10.1109/TPWRD.2017.2757939

Wang, K., & Kumar, A. (2019). Cross-spectral iris recognition using CNN and supervised discrete hashing. Pattern Recognition, 86, 85–98. https://doi.org/10.1016/j.patcog.2018.08.010

Wang, S., Kinnunen, T., & Lee, K. A. (2023). Domain adaptation for speaker recognition using PLDA and correlation alignment. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 31, 1120–1134. https://doi.org/10.1109/TASLP.2023.3256789

Wang, X., Zhang, S., Wang, S., Tianyu, F., Shi, H., & Mei, T. (2020). Mis-classified vector guided softmax loss for face recognition. Proceedings of the AAAI Conference on Artificial Intelligence, 34, 12241–12248.

Wang, Y. N., & Su, J. B. (2013, July). Symmetry description and face recognition using face symmetry based on local binary pattern feature. In Proceedings of the 32nd Chinese Control Conference (pp. 3955-3960). IEEE.

Warp, T., et al. (2022). Spatial audio and emotional response in immersive virtual environments. Frontiers in Virtual Reality, 3, 1–14.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Springer.

Wei, J., Huang, H., Wang, Y., He, R., & Sun, Z. (2022). Towards more discriminative and robust iris recognition by learning uncertain factors. IEEE Transactions on Information Forensics and Security, 17, 865–879. https://doi.org/10.1109/TIFS.2022.3154240

Wei, J., Wang, Y., Huang, H., He, R., Sun, Z., & Gao, X. (2023). Contextual Measures for Iris Recognition. IEEE Transactions on Information Forensics and Security, 18, 57–70. https://doi.org/10.1109/TIFS.2022.3221897

Wei, J., Wang, Y., Li, Y., He, R., & Sun, Z. (2022). Cross-Spectral Iris Recognition by Learning Device-Specific Band. IEEE Transactions on Circuits and Systems for Video Technology, 32(6), 3810–3824. https://doi.org/10.1109/TCSVT.2021.3117291

Wei, Z., Qinghui, W., Muqing, D., & Yiqi, L. (2015). A new inertial sensor-based gait recognition method via deterministic learning. 2015 34th Chinese

Control Conference (CCC), 3908–3913. https://doi.org/10.1109/ChiCC.2015.7260243
Weyrich, M., & Ebert, C. (2016). Reference Architectures for the Internet of Things. IEEE Software, 33(1), 112–116. https://doi.org/10.1109/MS.2016.20
Wicaksono, M. F., & Rahmatya, M. D. (2020). Implementasi Arduino dan ESP32 CAM untuk Smart Home. Jurnal Teknologi Dan Informasi, 10(1), 40-51.
Wicha, S., Temdee, P., Kamyod, C., Chaisricharoen, R., Thiriet, J.-M., & Yahoui, H. (2023). Industrial requirements analysis for Excellence Center setting-up and curriculum design in Industry 4.0 context. 2023 Joint International Conference on Digital Arts, Media, and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), 423–426. https://doi.org/10.1109/ECTIDAMTNCON57770.2023.10139488
Wieringa, R. J. (2014). Design science methodology for information systems and software engineering. Springer. https://doi.org/10.1007/978-3-662-43839-8
Wildes, R. P. (1997). Iris recognition: an emerging biometric technology. Proceedings of the IEEE, 85(9), 1348-1363.
Wilkes MV, Needham RM (1979) In: Denning PJ (ed) The Cambridge CAP computer and its operating system, Operating and programming systems series. North Holland, New York City
Wolf T, Babaee M, Rigoll G (2016) Multi-view gait recognition using 3d convolutional neural networks. In: International Conference on Image Processing, pp 4165–4169. IEEE
Wu Z, Huang Y, Wang L, Wang X, Tan T (2016) A comprehensive study on cross-view gait based human identification with deep CNNS. IEEE Trans Pattern Anal Mach Intell 39(2):209–226
Xie W, Nagrani A, Chung JS, Zisserman A (2019) Utterance-level aggregation for speaker recognition in the wild. In: International Conference on Acoustics, Speech and Signal Processing. IEEE
Xinrong, P., Yangmeng, T., & Jiaqiang, W. (2013). A survey of palmprint feature extraction algorithms. 2013 Fourth International Conference on Intelligent Systems Design and Engineering Applications, 57–63. https://doi.org/10.1109/ISDEA.2013.420
Xu X, Xu N, Li H, Zhu Q (2019) Multi-spectral palmprint recognition with deep multi-view representation learning. In: International Conference on Machine Learning and Intelligent Communications, pp 748–758. Springer
Xu, C., Makihara, Y., Li, X., & Yagi, Y. (2023). Occlusion-Aware Human Mesh Model-Based Gait Recognition. IEEE Transactions on Information Forensics and Security, 18, 1309–1321. https://doi.org/10.1109/TIFS.2023.3236181
Xu, L. D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243. https://doi.org/10.1109/TII.2014.2300753
Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the art and future trends. International Journal of Production Research, 56(8), 2941–2962.
Xu, Y., Zhang, Z., Lu, G., & Yang, J. (2016). Approximately symmetrical face images for image preprocessing in face recognition and sparse representation based classification. Pattern Recognition, 54, 68–82. https://doi.org/10.1016/j.patcog.2015.12.017
Xue, Z., Zhou, Y., & Du, Y. (2013). Ear biometric recognition based on local feature descriptors. Pattern Recognition, 46(3), 1035–1045.

Yadav, D., Kohli, N., Vatsa, M., & Singh, R. (2020). LivDet-Iris 2020: Iris presentation attack detection competition. Proceedings of the IEEE International Joint Conference on Biometrics (IJCB). https://doi.org/10.1109/IJCB48548.2020.9304880

Yahya, A. E., & Nordin, M. J. (2008). A new technique for iris localization in iris recognition systems. Information Technology Journal, 7(6), 924-929.

Yan C, Zhang B, Coenen F (2015) Multi-attributes gait identification by convolutional neural networks. In: International Congress on Image and Signal Processing (CISP), pp 642–647. IEEE

Yan, P., & Bowyer, K. W. (2007). Biometric Recognition Using 3D Ear Shape. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(8), 1297–1308. https://doi.org/10.1109/TPAMI.2007.1067

Yang, D., Xu, L. D., Zhang, H., & Metawa, N. (2017). An overview of Internet of Things technologies and applications. Enterprise Information Systems, 11(6), 824–847.

Yang, J., Li, H., Zhang, J., & Liu, W. (2022). Face synthesis with identity-attribute separation for heterogeneous face recognition. Pattern Recognition, 125, 108515. https://doi.org/10.1016/j.patcog.2021.108515

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet of-things security: A review. Sensors, 21(18), 6163.

Yang, Y., Sun, J., Liu, Z., & Qiao, Y. (2022). Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing. Journal of Information Security and Applications, 65, 103108. https://doi.org/10.1016/j.jisa.2022.103108 V1.14 October 2023 Page 44 of 47 Confirmation of Candidature

Yang, Z., Huangfu, H., Leng, L., Zhang, B., Teoh, A. B. J., & Zhang, Y. (2023). Comprehensive competition mechanism in palmprint recognition. IEEE Transactions on Information Forensics and Security, 18, 5160–5170. https://doi.org/10.1109/TIFS.2023.3306104

Yi, S., Li, C., & Li, Q. (2015). A survey of fog computing: Concepts, applications and issues. Proceedings of the 2015 Workshop on Mobile Big Data, 37–42.

Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on mobile computing, 3(4), 366-379.

Yu, M., Bai, Y., & Li, Y. (2023). Emo-regulator: An emotion-regulation training system fusing virtual reality and EEG-based neurofeedback. 2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 1–4. https://doi.org/10.1109/EMBC40787.2023.10340975

Yu, S., Tan, D., & Tan, T. (2017). GaitGAN: Invariant gait feature extraction using generative adversarial networks. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). https://doi.org/10.1109/CVPRW.2017.173

Yu, X., & Guo, H. (2019). A survey on IIoT security. 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), 1–5. https://doi.org/10.1109/VTSAPWCS.2019.8851679

Yuqing He, Jiali Cui, Tieniu Tan, & Yangsheng Wang. (2006). Key Techniques and Methods for Imaging Iris in Focus. 18th International Conference on Pattern Recognition (ICPR'06), 557–561. https://doi.org/10.1109/ICPR.2006.739

Zalozhnev, A. Yu., & Ginz, V. N. (2023). Industry 4.0: Underlying Technologies. Industry 5.0: HumanComputer Interaction as a Tech Bridge from Industry 4.0 to Industry 5.0. 2023 9th International Conference on Web Research (ICWR), 232–236. https://doi.org/10.1109/ICWR57742.2023.10139166

Zhang J, Yu W, Yang X, Deng F (2019) Few-shot learning for ear recognition. In: Proceedings of the 2019 International Conference on Image, Video and Signal Processing, pp 50–54. ACM ·

Zhang X, Zhao R, Qiao Y, Wang X, Li H (2019) Adacos: Adaptively scaling cosine logits for effectively learning deep face representations. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 10823–10832

Zhang X, Zhao R, Yan J, Gao M, Qiao Y, Wang X, Li H (2019) P2sgrad: Refined gradients for optimizing deep face models. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 9906–9914

Zhang Z, Tran L, Yin X, Atoum Y, Liu X, Wan J, Wang N (2019) Gait recognition via disentangled representation learning. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 4710–4719

Zhang, C., Patras, P., & Haddadi, H. (2020). Deep learning in mobile and wireless networking: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2224–2287.

Zhang, Q., Cui, J., Zhong, H., & Liu, L. (2022). Toward data transmission security based on proxy broadcast re-encryption in edge collaboration. ACM Transactions on Sensor Networks (TOSN), 18(3), 1-27.

Zhang, X., Zhao, Z., Dong, F., & Su, H. (2019). AdaCos: Adaptively scaling cosine logits for effectively learning deep face representations. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. https://doi.org/10.1109/CVPR.2019.00451

Zhang, Y., Mu, Z., & Yuan, Z. (2018). Ear recognition using convolutional neural networks in unconstrained environments. Pattern Recognition Letters, 110, 41–47. https://doi.org/10.1016/j.patrec.2018.03.004

Zhang, Y., Sun, J., Wang, H., & Xu, L. D. (2023). Artificial intelligence enabled Industrial Internet of Things security framework. IEEE Internet of Things Journal, 10(7), 5660–5674.

Zhang, Y., Xiang, Y., & Huang, X. (2017). A Cross-Layer Key Establishment Model for Wireless Devices in Cyber-Physical Systems. Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, 43–53. https://doi.org/10.1145/3055186.3055187

Zhao Z, Kumar A (2017) Towards more accurate iris recognition using deeply learned spatially corresponding features. In: IEEE International Conference on Computer Vision, pp 3809–3818

Zhao, L., & Kumar, A. (2017). Siamese CNN for palmprint recognition. IEEE Transactions on Information Forensics and Security, 12(11), 2570–2581. https://doi.org/10.1109/TIFS.2017.2718482

Zhao, W., & Kumar, A. (2017). Accurate periocular recognition under less constrained conditions. IEEE Transactions on Image Processing, 26(5), 2263–2276. https://doi.org/10.1109/TIP.2017.2656946

Zhao, Z., & Kumar, A. (2017). Towards more accurate iris recognition using deeply learned spatially corresponding features. IEEE International Conference on Computer Vision, 3809–3818.

Zhao, Z., & Kumar, A. (2019). A deep learning based unified framework to detect, segment and recognize irises using spatially corresponding features. Pattern Recognition, 93, 546–557. https://doi.org/10.1016/j.patcog.2019.04.010

Zhao Dandan Pan Xin , Pan Xin , Luo Xiaoling , & Gao Xiaojing (2015). Palmprint Recognition Based on Deep Learning 6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN 2015) https://doi.org/10.1049/cp.2015.0942

Zheng, Z., Li, Y., & Xu, L. D. (2022). Deep learning for Industrial Internet of Things security: A survey. IEEE Internet of Things Journal, 9(12), 9565–9583.

Zhou, X., & Bhanu, B. (2006, August). Feature fusion of face and gait for human recognition at a distance in video. In 18th International conference on pattern recognition (ICPR'06) (Vol. 4, pp. 529-532). IEEE.

Zhu, Y., Tan, T., & Wang, Y. (2000). Biometric personal identification based on iris patterns. Pattern Recognition, 33(2), 289–303. https://doi.org/10.1016/S0031-3203(99)00074-5

Zia, T., Anwar, M., & Khan, M. K. (2019). Machine learning techniques for secure Industrial Internet of Things systems. IEEE Access, 7, 146824–146839.

Zimmermann, V., & Gerber, N. (2017). "If it wasn't secure, they would not use it in the movies" – Security perceptions and user acceptance of authentication technologies. In Lecture Notes in Computer Science (pp. 265–283). Springer. https://doi.org/10.1007/978-3-319-58460-7_18

Zou Q, Wang Y, Zhao Y, Wang Q, Shen C, Li Q (2018) Deep learning-based gait recognition using smartphones in the wild. arXiv preprint arXiv:1811.00338

Appendix Artefact 1 –Experts Participation

This Appendix presents the expert's review document, which includes a detailed description of the study, as well as the questions and answers sent and received from various experts.

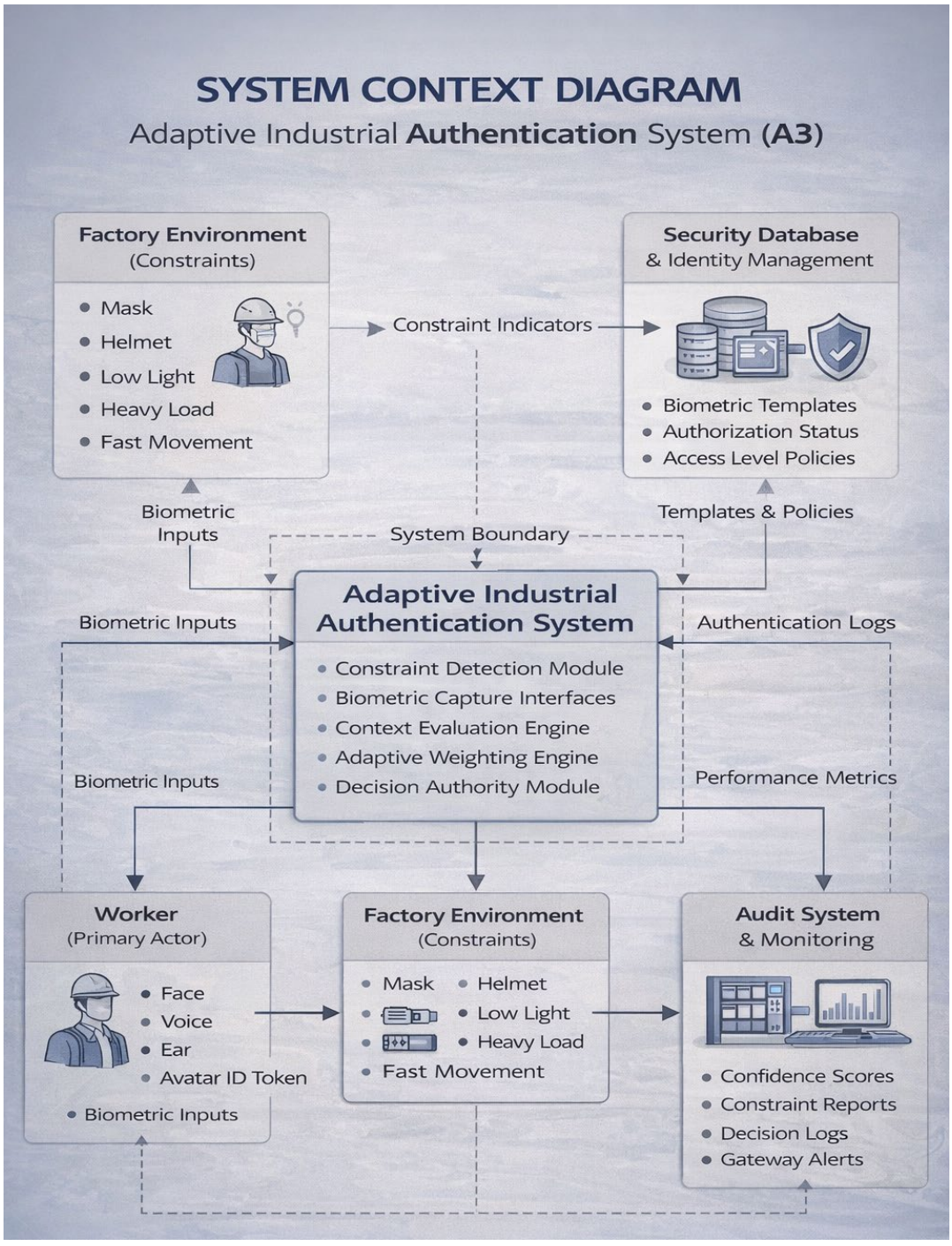


Figure 7.1 Industrial Expert study.

Overview of the Proposed System and Experimental Study

Introduction:

The adaptive industrial authentication system is designed to operate and function effectively under real-world constraints. The study is founded on the theoretical construct (Artefact 1), evaluated through experimental results (Artefact 2) using Second Life virtual reality software, and then presents a functionally upgraded system architecture (Artefact 3). Together, these elements provide a complete view of how biometric authentication can be improved within constrained industrial environments.

The core of this research is to address a key limitation in traditional authentication systems: their inability to adapt to environmental conditions. Drawing from the literature, the study assumes that authentication should not be static, but context-aware and responsive. This principle (Artefact 1) is implemented in the system (Artefact 3) through modules such as the constraint detection and context evaluation components, which allow the system to interpret environmental factors such as low lighting, movement, or protective equipment. The experimental findings (Artefact 2) demonstrate that incorporating contextual awareness improves the overall effectiveness of authentication decisions.

To strengthen reliability, the system integrates multi-modal biometric inputs, including facial features, voice, ear characteristics, and avatar-based identity tokens. This approach is informed by theoretical work suggesting that combining multiple biometric sources increases accuracy and robustness. Within the implemented system, these inputs are processed through biometric capture interfaces and evaluated collectively. The experimental results confirm that this multi-modal approach enhances authentication performance, particularly in constrained scenarios where individual biometric signals may be degraded.

A significant contribution of this research lies in its ability to handle environmental constraints typical of industrial settings. Factors such as masks, helmets, and fast movement are explicitly modelled within the system. These constraints are not treated as external limitations but as integral inputs that shape the authentication process. The results show that the system maintains effectiveness even with such constraints, demonstrating its practical applicability.

Central to the system is an adaptive decision-making mechanism, which dynamically adjusts the importance (weighting) of different biometric inputs based on context. This reflects the theoretical expectation that not all biometric signals are equally reliable in all situations. The implemented adaptive weighting engine and

decision module ensure that the system prioritises the most reliable inputs at any given time. Experimentally, this leads to more consistent and efficient authentication outcomes.

The system also incorporates a secure identity and policy management layer, ensuring that authentication decisions are aligned with predefined access control rules. Biometric templates and authorisation policies are stored and retrieved as part of the decision process. This integration ensures that the system is not only accurate but also secure and compliant with access requirements.

To support evaluation, the research includes a monitoring and audit component that records performance metrics such as confidence scores, authentication outcomes, and decision logs. These outputs form the basis of Artefact 2, enabling a clear assessment of system effectiveness. Rather than focusing heavily on user perception, the study prioritises technical performance, particularly efficiency and effectiveness, as the primary indicators of success.

Overall, the research demonstrates that an adaptive, context-aware biometric system can operate efficiently within a simulated industrial environment. The system design (Artefact 3) successfully implements the theoretical expectations (Artefact 1), and the experimental results (Artefact 2) confirm its effectiveness. This alignment provides strong evidence that the proposed approach is both technically sound and practically relevant.

Closing Statement for Expert Readers

This study establishes a clear link between theory (Artefact 1), system implementation (Artefact 3), and experimental validation (Artefact 2), demonstrating that adaptive, multi-modal biometric authentication can achieve efficient and effective performance in constrained industrial environments.

Questions

- Is this solution doable?
- Is it comprehensive?
- Other comments?

Appendix A2 – Expert Feedback

Expert 1 Feedback

Shipping / Construction Worker (Field Operator Perspective)

Experience: 15+ years on industrial sites, MSC cybersecurity

1. Is this solution doable?

Yeah, it's doable—but only if it works fast and doesn't slow us down. On-site, we don't have time to stand still for scans. If your system can recognise someone even when they're moving or wearing gear, then it fits reality.

2. Is it comprehensive?

From what I see, yes. You've thought about helmets, masks, and lighting—that's real life for us. Most systems ignore that.

3. Other comments

Just make sure it works in rough conditions—dust, noise, rain. If it fails when things get messy, people won't use it.

4. Qualifications and role

Heavy machinery operator, logistics and port construction environments.

Expert 2 Feedback

Job: IT security, Authentication Systems

1. Doable?

Yes. The architecture aligns well with adaptive authentication frameworks. The integration of context-awareness is particularly strong.

2. Comprehensive?

Highly. The linkage between Artefact 1, Artefact 2, and Artefact 3 demonstrates theoretical, experimental, and architectural completeness.

3. Other comments

Your adaptive weighting engine is the strongest contribution. However, I would recommend incorporating adversarial testing—particularly spoofing resistance.

4. Role

PhD in IT security, specialised in biometric authentication systems/lecturer university of Enugu 10+ years.

Expert 3 Feedback

1. Doable?

Yes, especially with current IAM systems. The policy layer you included is critical and realistic.

2. Comprehensive?

Yes, though I would like to see more detail on policy conflict resolution.

3. Other comments

Your integration of biometric templates with access control policies is solid.

Consider compliance frameworks like ISO 27001.

4. Role

Full stack and security developer +15 years / **Identity & Access Management, BSC Information Technology**

Expert 4 Feedback

1. Doable?

Yes. Multi-modal biometrics is already proven; your novelty lies in adaptation.

2. Comprehensive?

Very strong. Combining ear, speech, and facial data is a robust approach.

3. Other comments

Weight adaptation based on environmental conditions is scientifically sound. I would suggest adding confidence scoring transparency.

4. Role

Professor in Biometric Systems Engineering, **Biometric Systems Designer 7years**

Expert 5 Feedback

1. Doable?

Yes—but only if tested against attacks.

2. Comprehensive?

Technically yes, but offensively incomplete.

3. Other comments

How does it handle spoofing? Deepfakes? Replay attacks? If this isn't addressed, attackers will exploit it.

4. Role

Red Team Specialist, **Applied Security 6+, MSc Computer Science**

Expert 6 Feedback

1. Doable?

Yes. The system fits well within IoT ecosystems where devices need contextual authentication.

2. Comprehensive?

Yes, particularly in handling environmental constraints.

3. Other comments

Latency and edge processing need consideration. Industrial IoT systems cannot rely heavily on cloud delays.

4. Role

IoT Systems Engineer, 6years

Expert 7 Feedback

1. Doable?

Yes, especially using platforms like Second Life for simulation.

2. Comprehensive?

Yes, the use of avatars as proxies is clever and appropriate.

3. Other comments

Simulation validity is strong, but real-world transferability must be validated beyond VR.

4. Role

VR Systems Designer and Game designer 10+ years

Expert 8 Feedback

1. Doable?

Yes, and highly relevant for Industry 4.0 environments.

2. Comprehensive?

Yes, particularly the environmental constraint modelling.

3. Other comments

Your system aligns with smart factory needs. However, integration with legacy industrial systems will be a challenge.

4. Role

Industrial IoT Architect 15years +. BSc Computer Science

Expert 9 Feedback

1. Doable?

If it’s simple and fast, yes.

2. Comprehensive?

Better than most systems we use.

3. Other comments

We deal with people wearing PPE all the time. If your system works with helmets and masks, that’s a big win.

4. Role

Site Security Supervisor +20years.

Appendix B1- Second Life Test result table

Table 7.2 Experimental Result

TRIAL	AVATAR	MASK	HELMET	HEAVYLOAD	LOWLIGHT	FASTMOVE	FACE	GAIT	VOICE	EAR	AVATARID	FUSION_SCORE	DECISION
1	A1	0	0	0	0	0	82	84	86	88	96	87.67	PASS
2	A1	0	0	0	0	1	67.2	70.6	74	77.4	92.2	77.07	PASS
3	A1	0	0	0	1	0	67.2	70.6	74	77.4	92.2	77.07	PASS
4	A1	0	0	0	1	1	52.5	57.1	61.9	66.9	88.3	66.45	PASS
5	A1	0	0	1	0	0	67.2	70.6	74	77.4	92.2	77.07	PASS
6	A1	0	0	1	0	1	52.5	57.1	61.9	66.9	88.3	66.45	PASS
7	A1	0	0	1	1	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS
8	A1	0	0	1	1	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
9	A1	0	1	0	0	0	67.2	70.6	74	77.4	92.2	77.07	PASS
10	A1	0	1	0	0	1	52.5	57.1	61.9	66.9	88.3	66.45	PASS
11	A1	0	1	0	1	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS
12	A1	0	1	0	1	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
13	A1	0	1	1	0	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS
14	A1	0	1	1	0	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
15	A1	0	1	1	1	0	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
16	A1	0	1	1	1	1	23	30.2	37.8	45.8	80.6	45.23	FAIL
17	A1	1	0	0	0	0	67.2	70.6	74	77.4	92.2	77.07	PASS
18	A1	1	0	0	0	1	52.5	57.1	61.9	66.9	88.3	66.45	PASS
19	A1	1	0	0	1	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS
20	A1	1	0	0	1	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
21	A1	1	0	1	0	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS
22	A1	1	0	1	0	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
23	A1	1	0	1	1	0	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
24	A1	1	0	1	1	1	23	30.2	37.8	45.8	80.6	45.23	FAIL
25	A1	1	1	0	0	0	52.5	57.1	61.9	66.9	88.3	66.45	PASS

26	A1	1	1	0	0	1	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
27	A1	1	1	0	1	0	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
28	A1	1	1	0	1	1	23	30.2	37.8	45.8	80.6	45.23	FAIL
29	A1	1	1	1	0	0	37.7	43.7	49.9	56.3	84.5	55.85	FAIL
30	A1	1	1	1	0	1	23	30.2	37.8	45.8	80.6	45.23	FAIL
31	A1	1	1	1	1	0	23	30.2	37.8	45.8	80.6	45.23	FAIL
32	A1	1	1	1	1	1	8.2	16.8	25.8	35.2	76.8	34.63	FAIL
33	A2	0	0	0	0	0	77.9	79.8	81.7	83.6	91.2	83.28	PASS
34	A2	0	0	0	0	1	63.1	66.4	69.7	73	87.4	72.68	PASS
35	A2	0	0	0	1	0	63.1	66.4	69.7	73	87.4	72.68	PASS
36	A2	0	0	0	1	1	48.4	52.9	57.6	62.5	83.5	62.07	PASS
37	A2	0	0	1	0	0	63.1	66.4	69.7	73	87.4	72.68	PASS
38	A2	0	0	1	0	1	48.4	52.9	57.6	62.5	83.5	62.07	PASS
39	A2	0	0	1	1	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
40	A2	0	0	1	1	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
41	A2	0	1	0	0	0	63.1	66.4	69.7	73	87.4	72.68	PASS
42	A2	0	1	0	0	1	48.4	52.9	57.6	62.5	83.5	62.07	PASS
43	A2	0	1	0	1	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
44	A2	0	1	0	1	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
45	A2	0	1	1	0	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
46	A2	0	1	1	0	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
47	A2	0	1	1	1	0	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
48	A2	0	1	1	1	1	18.9	26	33.5	41.4	75.8	40.85	FAIL
49	A2	1	0	0	0	0	63.1	66.4	69.7	73	87.4	72.68	PASS
50	A2	1	0	0	0	1	48.4	52.9	57.6	62.5	83.5	62.07	PASS
51	A2	1	0	0	1	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
52	A2	1	0	0	1	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
53	A2	1	0	1	0	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
54	A2	1	0	1	0	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
55	A2	1	0	1	1	0	33.6	39.5	45.6	51.9	79.7	51.47	FAIL

56	A2	1	0	1	1	1	18.9	26	33.5	41.4	75.8	40.85	FAIL
57	A2	1	1	0	0	0	48.4	52.9	57.6	62.5	83.5	62.07	PASS
58	A2	1	1	0	0	1	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
59	A2	1	1	0	1	0	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
60	A2	1	1	0	1	1	18.9	26	33.5	41.4	75.8	40.85	FAIL
61	A2	1	1	1	0	0	33.6	39.5	45.6	51.9	79.7	51.47	FAIL
62	A2	1	1	1	0	1	18.9	26	33.5	41.4	75.8	40.85	FAIL
63	A2	1	1	1	1	0	18.9	26	33.5	41.4	75.8	40.85	FAIL
64	A2	1	1	1	1	1	4.1	12.6	21.5	30.8	72	30.25	FAIL
65	A3	0	0	0	0	0	86.1	88.2	90.3	92.4	100	91.92	PASS
66	A3	0	0	0	0	1	71.3	74.8	78.3	81.8	97	81.45	PASS
67	A3	0	0	0	1	0	71.3	74.8	78.3	81.8	97	81.45	PASS
68	A3	0	0	0	1	1	56.6	61.3	66.2	71.3	93.1	70.83	PASS
69	A3	0	0	1	0	0	71.3	74.8	78.3	81.8	97	81.45	PASS
70	A3	0	0	1	0	1	56.6	61.3	66.2	71.3	93.1	70.83	PASS
71	A3	0	0	1	1	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS
72	A3	0	0	1	1	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
73	A3	0	1	0	0	0	71.3	74.8	78.3	81.8	97	81.45	PASS
74	A3	0	1	0	0	1	56.6	61.3	66.2	71.3	93.1	70.83	PASS
75	A3	0	1	0	1	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS
76	A3	0	1	0	1	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
77	A3	0	1	1	0	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS
78	A3	0	1	1	0	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
79	A3	0	1	1	1	0	41.8	47.9	54.2	60.7	89.3	60.23	PASS
80	A3	0	1	1	1	1	27.1	34.4	42.1	50.2	85.4	49.62	FAIL
81	A3	1	0	0	0	0	71.3	74.8	78.3	81.8	97	81.45	PASS
82	A3	1	0	0	0	1	56.6	61.3	66.2	71.3	93.1	70.83	PASS
83	A3	1	0	0	1	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS
84	A3	1	0	0	1	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
85	A3	1	0	1	0	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS

86	A3	1	0	1	0	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
87	A3	1	0	1	1	0	41.8	47.9	54.2	60.7	89.3	60.23	PASS
88	A3	1	0	1	1	1	27.1	34.4	42.1	50.2	85.4	49.62	FAIL
89	A3	1	1	0	0	0	56.6	61.3	66.2	71.3	93.1	70.83	PASS
90	A3	1	1	0	0	1	41.8	47.9	54.2	60.7	89.3	60.23	PASS
91	A3	1	1	0	1	0	41.8	47.9	54.2	60.7	89.3	60.23	PASS
92	A3	1	1	0	1	1	27.1	34.4	42.1	50.2	85.4	49.62	FAIL
93	A3	1	1	1	0	0	41.8	47.9	54.2	60.7	89.3	60.23	PASS
94	A3	1	1	1	0	1	27.1	34.4	42.1	50.2	85.4	49.62	FAIL
95	A3	1	1	1	1	0	27.1	34.4	42.1	50.2	85.4	49.62	FAIL
96	A3	1	1	1	1	1	12.3	21	30.1	39.6	81.6	39.02	FAIL
97	A4	0	0	0	0	0	73.8	75.6	77.4	79.2	86.4	78.9	PASS
98	A4	0	0	0	0	1	59	62.2	65.4	68.6	82.6	68.3	PASS
99	A4	0	0	0	1	0	59	62.2	65.4	68.6	82.6	68.3	PASS
100	A4	0	0	0	1	1	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
101	A4	0	0	1	0	0	59	62.2	65.4	68.6	82.6	68.3	PASS
102	A4	0	0	1	0	1	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
103	A4	0	0	1	1	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
104	A4	0	0	1	1	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
105	A4	0	1	0	0	0	59	62.2	65.4	68.6	82.6	68.3	PASS
106	A4	0	1	0	0	1	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
107	A4	0	1	0	1	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
108	A4	0	1	0	1	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
109	A4	0	1	1	0	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
110	A4	0	1	1	0	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
111	A4	0	1	1	1	0	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
112	A4	0	1	1	1	1	14.8	21.8	29.2	37	71	36.47	FAIL
113	A4	1	0	0	0	0	59	62.2	65.4	68.6	82.6	68.3	PASS
114	A4	1	0	0	0	1	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
115	A4	1	0	0	1	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL

116	A4	1	0	0	1	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
117	A4	1	0	1	0	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
118	A4	1	0	1	0	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
119	A4	1	0	1	1	0	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
120	A4	1	0	1	1	1	14.8	21.8	29.2	37	71	36.47	FAIL
121	A4	1	1	0	0	0	44.3	48.7	53.3	58.1	78.7	57.68	FAIL
122	A4	1	1	0	0	1	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
123	A4	1	1	0	1	0	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
124	A4	1	1	0	1	1	14.8	21.8	29.2	37	71	36.47	FAIL
125	A4	1	1	1	0	0	29.5	35.3	41.3	47.5	74.9	47.08	FAIL
126	A4	1	1	1	0	1	14.8	21.8	29.2	37	71	36.47	FAIL
127	A4	1	1	1	1	0	14.8	21.8	29.2	37	71	36.47	FAIL
128	A4	1	1	1	1	1	0	8.4	17.2	26.4	67.2	25.87	FAIL
129	A5	0	0	0	0	0	88.6	90.7	92.9	95	100	94.07	PASS
130	A5	0	0	0	0	1	73.8	77.3	80.8	84.5	99.8	84.07	PASS
131	A5	0	0	0	1	0	73.8	77.3	80.8	84.5	99.8	84.07	PASS
132	A5	0	0	0	1	1	59	63.8	68.8	73.9	96	73.45	PASS
133	A5	0	0	1	0	0	73.8	77.3	80.8	84.5	99.8	84.07	PASS
134	A5	0	0	1	0	1	59	63.8	68.8	73.9	96	73.45	PASS
135	A5	0	0	1	1	0	59	63.8	68.8	73.9	96	73.45	PASS
136	A5	0	0	1	1	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
137	A5	0	1	0	0	0	73.8	77.3	80.8	84.5	99.8	84.07	PASS
138	A5	0	1	0	0	1	59	63.8	68.8	73.9	96	73.45	PASS
139	A5	0	1	0	1	0	59	63.8	68.8	73.9	96	73.45	PASS
140	A5	0	1	0	1	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
141	A5	0	1	1	0	0	59	63.8	68.8	73.9	96	73.45	PASS
142	A5	0	1	1	0	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
143	A5	0	1	1	1	0	44.3	50.4	56.8	63.4	92.2	62.88	PASS
144	A5	0	1	1	1	1	29.5	37	44.7	52.8	88.3	52.25	FAIL
145	A5	1	0	0	0	0	73.8	77.3	80.8	84.5	99.8	84.07	PASS

146	A5	1	0	0	0	1	59	63.8	68.8	73.9	96	73.45	PASS
147	A5	1	0	0	1	0	59	63.8	68.8	73.9	96	73.45	PASS
148	A5	1	0	0	1	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
149	A5	1	0	1	0	0	59	63.8	68.8	73.9	96	73.45	PASS
150	A5	1	0	1	0	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
151	A5	1	0	1	1	0	44.3	50.4	56.8	63.4	92.2	62.88	PASS
152	A5	1	0	1	1	1	29.5	37	44.7	52.8	88.3	52.25	FAIL
153	A5	1	1	0	0	0	59	63.8	68.8	73.9	96	73.45	PASS
154	A5	1	1	0	0	1	44.3	50.4	56.8	63.4	92.2	62.88	PASS
155	A5	1	1	0	1	0	44.3	50.4	56.8	63.4	92.2	62.88	PASS
156	A5	1	1	0	1	1	29.5	37	44.7	52.8	88.3	52.25	FAIL
157	A5	1	1	1	0	0	44.3	50.4	56.8	63.4	92.2	62.88	PASS
158	A5	1	1	1	0	1	29.5	37	44.7	52.8	88.3	52.25	FAIL
159	A5	1	1	1	1	0	29.5	37	44.7	52.8	88.3	52.25	FAIL
160	A5	1	1	1	1	1	14.8	23.5	32.7	42.2	84.5	41.65	FAIL
161	A6	0	0	0	0	0	91.8	94.1	96.3	98.6	100	96.8	PASS
162	A6	0	0	0	0	1	77.1	80.6	84.3	88	100	86.97	PASS
163	A6	0	0	0	1	0	77.1	80.6	84.3	88	100	86.97	PASS
164	A6	0	0	0	1	1	62.3	67.2	72.2	77.4	99.8	76.95	PASS
165	A6	0	0	1	0	0	77.1	80.6	84.3	88	100	86.97	PASS
166	A6	0	0	1	0	1	62.3	67.2	72.2	77.4	99.8	76.95	PASS
167	A6	0	0	1	1	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
168	A6	0	0	1	1	1	47.6	53.8	60.2	66.9	96	66.38	PASS
169	A6	0	1	0	0	0	77.1	80.6	84.3	88	100	86.97	PASS
170	A6	0	1	0	0	1	62.3	67.2	72.2	77.4	99.8	76.95	PASS
171	A6	0	1	0	1	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
172	A6	0	1	0	1	1	47.6	53.8	60.2	66.9	96	66.38	PASS
173	A6	0	1	1	0	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
174	A6	0	1	1	0	1	47.6	53.8	60.2	66.9	96	66.38	PASS
175	A6	0	1	1	1	0	47.6	53.8	60.2	66.9	96	66.38	PASS

176	A6	0	1	1	1	1	32.8	40.3	48.2	56.3	92.2	55.77	FAIL
177	A6	1	0	0	0	0	77.1	80.6	84.3	88	100	86.97	PASS
178	A6	1	0	0	0	1	62.3	67.2	72.2	77.4	99.8	76.95	PASS
179	A6	1	0	0	1	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
180	A6	1	0	0	1	1	47.6	53.8	60.2	66.9	96	66.38	PASS
181	A6	1	0	1	0	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
182	A6	1	0	1	0	1	47.6	53.8	60.2	66.9	96	66.38	PASS
183	A6	1	0	1	1	0	47.6	53.8	60.2	66.9	96	66.38	PASS
184	A6	1	0	1	1	1	32.8	40.3	48.2	56.3	92.2	55.77	FAIL
185	A6	1	1	0	0	0	62.3	67.2	72.2	77.4	99.8	76.95	PASS
186	A6	1	1	0	0	1	47.6	53.8	60.2	66.9	96	66.38	PASS
187	A6	1	1	0	1	0	47.6	53.8	60.2	66.9	96	66.38	PASS
188	A6	1	1	0	1	1	32.8	40.3	48.2	56.3	92.2	55.77	FAIL
189	A6	1	1	1	0	0	47.6	53.8	60.2	66.9	96	66.38	PASS
190	A6	1	1	1	0	1	32.8	40.3	48.2	56.3	92.2	55.77	FAIL
191	A6	1	1	1	1	0	32.8	40.3	48.2	56.3	92.2	55.77	FAIL
192	A6	1	1	1	1	1	18	26.9	36.1	45.8	88.3	45.15	FAIL

Appendix B2- Second Life Implementation Code

Gate_Scanner.Lsl — Land Scanner

Place inside the Gate_Scanner prim on the land near the gate.
// gate_scanner.lsl
// Listens for PROBE messages, logs locally (object description), forwards to server or computes local fusion,
// returns RESULT to HUD and instructs gate prim (GATE_CHANNEL).

- Place gate_scanner.lsl in the Gate_Scanner prim content. Set SERVER_URL (ngrok https) when server is live.

```
// ========================================================
//  GATE-SIDE BIOMETRIC SCANNER (MANUAL TOUCH VERSION)
//  LSL-SAFE — NO SCOPE ERRORS — MATCHES HUD FORMAT
// ========================================================

integer GATE_CH = -9001;
integer LOG_CH  = -9002;

// Biometrics
list TRAITS = ["FACE","GAIT",”VOICE","EAR"," AVATARID"];

// Constraints
list CONSTRAINTS =
["MASK","HELMET","HEAVYLOAD","LOWLIGHT","FASTMOVE"];

// Detected constraints
list DETECTED = [];

// ---------- BASE SCORES ----------
integer getBase(string t)
{
   if (t == "FACE") return 90;
   if (t == "GAIT") return 85;
   if (t == "VOICE") return 80;
   if (t == "EAR")  return 75;
   if (t == "AVATARID") return 100;
   return 0;
}

// ---------- PENALTIES ----------
integer getPenalty(string c)
{
   if (c == "MASK") return 25;
   if (c == "HELMET") return 20;
   if (c == "HEAVYLOAD") return 30;
```

```
    if (c == "LOWLIGHT") return 10;
    if (c == "FASTMOVE") return 15;
    return 0;
}

// ---------- DETECT CONSTRAINTS ----------
detectConstraints(key agent)
{
    DETECTED = [];

    list worn = llGetAttachedList(agent);
    integer n = llGetListLength(worn);

    integer i;
    for (i = 0; i < n; i++)
    {
        key itemKey = llList2Key(worn, i);
        string name = llToUpper(llKey2Name(itemKey));

        integer x;
        for (x = 0; x < llGetListLength(CONSTRAINTS); x++)
        {
            string c = llList2String(CONSTRAINTS, x);
            if (llSubStringIndex(name, c) != -1)
            {
                if (llListFindList(DETECTED, [c]) == -1)
                    DETECTED += [c];
            }
        }
    }
}

// ---------- SUM PENALTIES ----------
integer sumPenalties()
{
    integer total = 0;
    integer i;
    for (i = 0; i < llGetListLength(DETECTED); i++)
    {
        string c = llList2String(DETECTED, i);
        total += getPenalty(c);
    }
    return total;
}

// ---------- BUILD REPORT ----------
string buildReport()
{
    string r = "=== GATE-SIDE BIOMETRIC REPORT ===\n";
```

```
    integer totalPenalty = sumPenalties();
    integer passCount = 0;

    integer i;
    for (i = 0; i < llGetListLength(TRAITS); i++)
    {
        string t = llList2String(TRAITS, i);
        integer base = getBase(t);

        integer s = base - totalPenalty;
        if (s < 0) s = 0;

        string st = "FAIL";
        if (s >= 60)
        {
            st = "PASS";
            passCount++;
        }

        r += t + ": " + (string)s + " (" + st + ")\n";
    }

    string final = "FAIL";
    if (passCount >= 4) final = "PASS";

    r += "FINAL DECISION: " + final + "\n";

    if (llGetListLength(DETECTED) > 0)
        r += "CONSTRAINTS: " + llDumpList2String(DETECTED, ", ") + "\n";
    else
        r += "CONSTRAINTS: NONE\n";

    return r;
}

// ---------- MAIN ----------
default
{
    touch_start(integer total)
    {
        key avatar = llDetectedKey(0);

        // detect constraints from attachments
        detectConstraints(avatar);

        // build report
        string rep = buildReport();

        // print to local owner / avatar
        llRegionSayTo(avatar, 0, rep);
```

```
        // send to logger
        llShout(LOG_CH, rep);

        // gate command
        if (llSubStringIndex(rep, "FINAL DECISION: PASS") != -1)
            llShout(GATE_CH, "OPEN");
        else
            llShout(GATE_CH, "CLOSE");
    }
}
```

Avatar_Hud.Lsl — Wearable Hud (Per Avatar)

Place into a small prim, attach as HUD (center). Each test avatar must wear this.

```
// avatar_hud.lsl
// Wear this as HUD. It constructs a deterministic probe vector, detects constraints
```

- Attach to HUD slot.
- Set SERVER_URL to your server before deploying server. When SERVER_URL=="", HUD still sends region message to scanner for local decisions.

```
// ============================================================
// HUD BIOMETRIC SCORING SYSTEM (STRICT LSL-SAFE VERSION)
// ============================================================

integer GATE_CH = -9001;
integer LOG_CH  = -9002;

// Simple trait list
list TRAITS = ["FACE","GAIT", "VOICE","EAR", "AVATARID"];
list CONSTRAINTS =
["MASK","HELMET","HEAVYLOAD","LOWLIGHT","FASTMOVE"];

// Base scores
integer getBase(string t)
{
    if (t == "FACE") return 90;
    if (t == "GAIT") return 85;
    if (t == "VOICE") return 80;
    if (t == "EAR") return 75;
    if (t == "AVATARID") return 100;
    return 0;
}

// penalties
integer getPenalty(string c)
{
```

```
    if (c == "MASK") return 25;
    if (c == "HELMET") return 20;
    if (c == "HEAVYLOAD") return 30;
    if (c == "LOWLIGHT") return 10;
    if (c == "FASTMOVE") return 15;
    return 0;
}

// detected constraints
list DETECTED = [];

// scans worn attachments for names containing keywords
detectConstraints()
{
    DETECTED = [];
    integer invCount = llGetInventoryNumber(INVENTORY_OBJECT);
    integer i;
    for (i = 0; i < invCount; i++)
    {
        string item = llToUpper(llGetInventoryName(INVENTORY_OBJECT, i));

        integer x;
        for (x = 0; x < llGetListLength(CONSTRAINTS); x++)
        {
            string c = llList2String(CONSTRAINTS, x);

            if (llSubStringIndex(item, c) != -1)
            {
                if (llListFindList(DETECTED, [c]) == -1)
                {
                    DETECTED += [c];
                }
            }
        }
    }
}

// sums all penalties
integer sumPenalties()
{
    integer total = 0;
    integer i;
    for (i = 0; i < llGetListLength(DETECTED); i++)
    {
        string c = llList2String(DETECTED, i);
        total += getPenalty(c);
    }
    return total;
}
```

```
// compute final report string
string buildReport()
{
    integer totalPenalty = sumPenalties();
    string r = "=== BIOMETRIC REPORT ===\n";

    integer passCount = 0;

    integer i;
    for (i = 0; i < llGetListLength(TRAITS); i++)
    {
        string t = llList2String(TRAITS, i);
        integer base = getBase(t);

        integer score = base - totalPenalty;
        if (score < 0) score = 0;

        string status = "FAIL";
        if (score >= 60)
        {
            status = "PASS";
            passCount++;
        }

        r += t + ": " + (string)score + " (" + status + ")\n";
    }

    string final = "FAIL";
    if (passCount >= 4) final = "PASS";

    r += "FINAL DECISION: " + final + "\n";

    // Add constraints list
    if (llGetListLength(DETECTED) > 0)
        r += "CONSTRAINTS: " + llDumpList2String(DETECTED, ", ") + "\n";
    else
        r += "CONSTRAINTS: NONE\n";

    return r;
}

// When HUD is touched, run the analysis
default
{
    touch_start(integer n)
    {
        detectConstraints();
        string report = buildReport();

        llOwnerSay(report);
```

```
        // send to gate
        if (llSubStringIndex(report, "FINAL DECISION: PASS") != -1)
            llShout(GATE_CH, "OPEN");
        else
            llShout(GATE_CH, "CLOSE");

        // send to logger
        llShout(LOG_CH, report);
    }
}
```

Logger

Put to store result in any prim provide

```
integer LOG_CH = -9002;

list ENTRIES = [];

default
{
    state_entry()
    {
        llListen(LOG_CH, "", NULL_KEY, "");
        llOwnerSay("LOGGER ACTIVE");
    }

    listen(integer c, string nm, key id, string msg)
    {
        ENTRIES += [msg];
        llOwnerSay("LOG ENTRY RECORDED");
    }

    touch_start(integer n)
    {
        integer i;
        string out = "=== STORED LOGS ===\n";

        for (i = 0; i < llGetListLength(ENTRIES); i++)
        {
            out += "\n--- ENTRY " + (string)i + " ---\n";
            out += llList2String(ENTRIES, i) + "\n";
        }

        llOwnerSay(out);
    }
}
```

Gate Control

gate_controller.lsl — Sliding gate prim
Put this into the physical gate prim (sliding door) and set its local position/slide distance if needed.

```
// gate_controller.lsl
// Sliding gate: opens when receives GATE_OPEN|uuid on GATE_CHANNEL, closes automatically after timeout.

integer GATE_CH = -9001;

rotation ROT_CLOSED;
rotation ROT_OPEN;

default
{
   state_entry()
   {
      ROT_CLOSED = llGetLocalRot();
      ROT_OPEN = ROT_CLOSED * llEuler2Rot(<0,0,90> * DEG_TO_RAD);

      llListen(GATE_CH, "", NULL_KEY, "");
   }

   listen(integer ch, string nm, key id, string msg)
   {
      if (msg == "OPEN")
      {
         llSetLocalRot(ROT_OPEN);
         llSleep(5.0);
         llSetLocalRot(ROT_CLOSED);
      }
      else if (msg == "CLOSE")
      {
         llSetLocalRot(ROT_CLOSED);
      }
   }
}
```

Appendix B3- Second Life Avatar Snapshot Scenario.

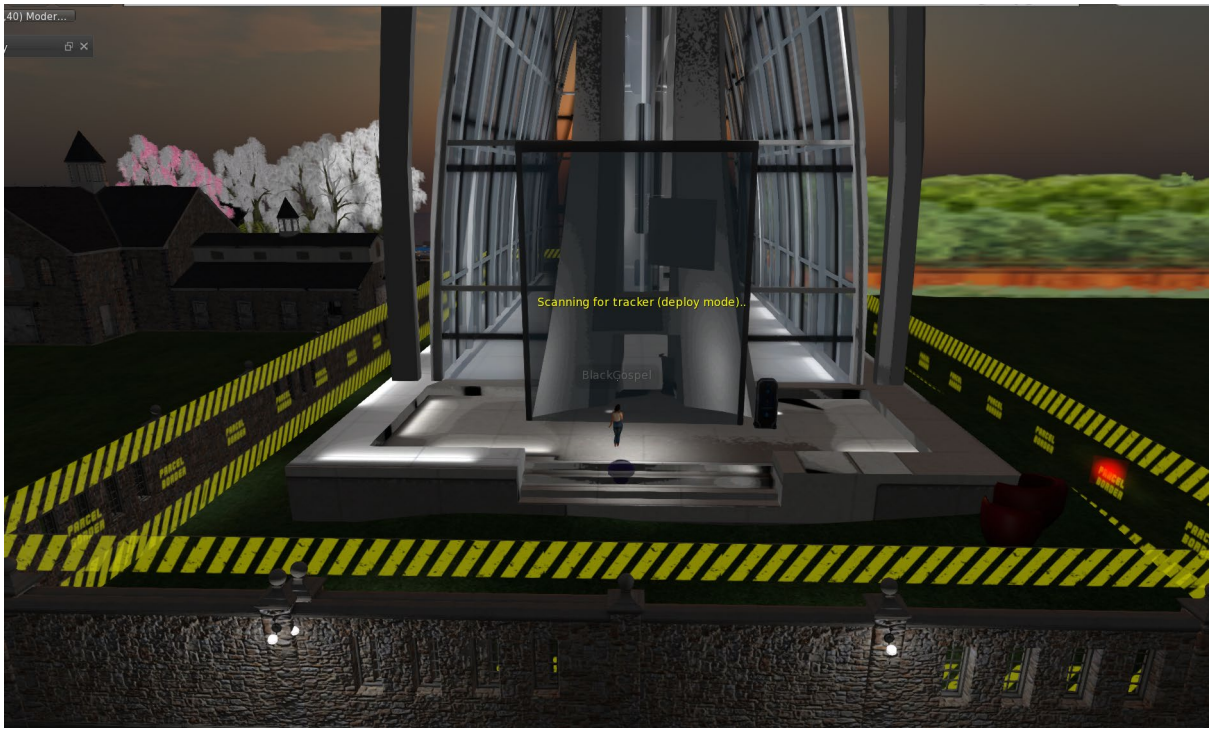


Figure 7.2 Second life experimental scenario

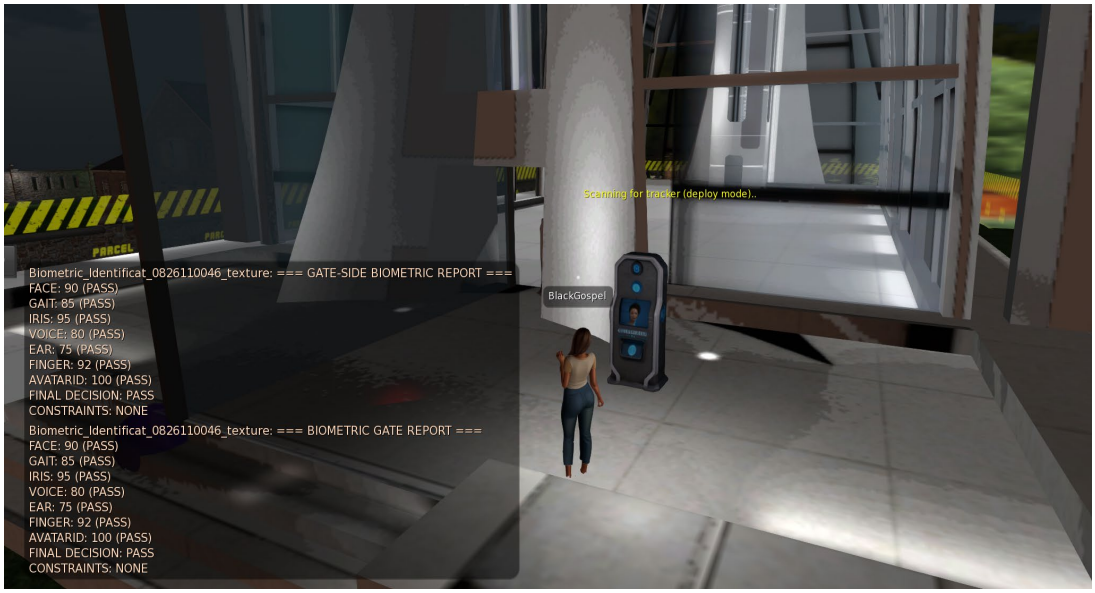


Figure 7.3 Gate and Output Test



Figure 7.4 Blender curated Biometric machine

Avatar 1 Snapshots



Figure 7.5 Avatar 1

Avatar 2 Snapshots



Figure 7.6 Avatar 2

Avatar 3 Snapshots



Figure 7.7 Avatar 3

Avatar 4 Snapshots

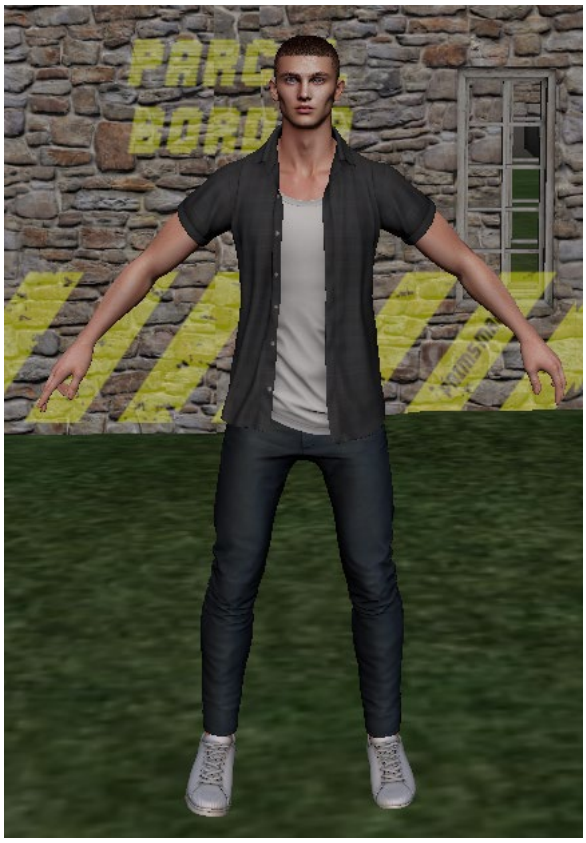


Figure 7.8 Avatar 4

Avatar 5 Snapshots



Figure 7.9 Avatar 5

Avatar 6 Snapshots



Figure 7.10 Avatar 6

Avatar Industrial Face Mask



Figure 7.11 Industrial Face Mask

Avatar Industrial Face Mask & Heavy Load



Figure 7.12 Industrial Face Mask & Heavy Load

Avatar Industrial Face Mask & Helmet

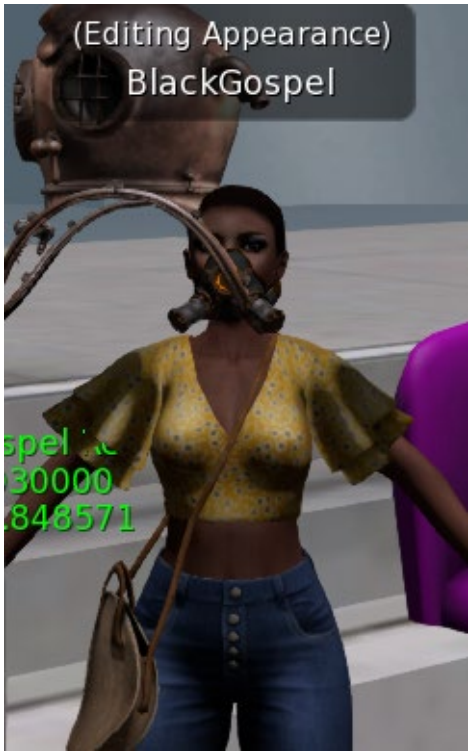


Figure 7.13 Industrial Face Mask & Helmet

Avatar Lowlight, Fastmove & Heavy Load



Figure 7.14 Lowlight, Fastmove & Heavy Load