# Behavioural Biometrics: A Novel Approach to User Authentication in Information Systems Security

Joshua Mulligan

A Dissertation submitted to

Auckland University of Technology

In partial fulfilment of the requirements for the degree of

Bbus (Hons) Information Systems

2024

School of Business, Economics and Law

## ABSTRACT

As information technology (IT) evolves, user authentication has shifted towards innovative approaches, with behavioural biometrics (BB) emerging as a leading contender. However, there are no studies that investigate the factors that shape user acceptance and trust in the biometric authentication systems. This dissertation employs a Systematic Literature Review (SLR) to investigate these focusing on behavioural biometrics. Past studies indicate that there is immense potential for BB as a robust authentication method to enhance user acceptance and trust. Therefore, this examination of the existing literature aims to provide a nuanced understanding of trust in IT and its intersection with BB. The outcomes of this study will inform the refinement of biometric technologies and provide crucial insights for practitioners, policymakers, and researchers, advancing secure and user-friendly digital authentication solutions in an ever-evolving technological landscape. By employing an SLR methodology, this research endeavours to bridge existing gaps.

Based on a review of 88 articles, it is evident that the quality of data related to BB is often inconsistent, with inadequate quality assessment and poor reporting of detailed information. This study presents key reporting items to improve the transparency and comparability of future research on user authentication and adoption. It also emphasizes that user trust and acceptance of BB are poorly assessed and reported in both empirical and conceptual research, as well as across multiple industries. Additionally, it highlights common challenges faced by BB applications, including regulatory, technical, social, and research-related issues that need to be addressed for progress in the field.

**Keywords:** Behavioural Biometrics, Information Technology, Trust, Transparency, Personalisation, Privacy, Security, Big Data, IOT.

## Table of Contents

## List of figures



## List of tables

## 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.

Signed,

Joshua Mulligan

## Acknowledgements

I would like to express my deepest gratitude to those who have supported me throughout the process of researching and writing this dissertation.

First and foremost, I extend my sincere thanks to my supervisor, Dr. Ranjan Vaidya. His invaluable guidance, expertise, and encouragement have been instrumental in shaping this work. Dr. Vaidya's insightful feedback and unwavering support have greatly contributed to the successful completion of this dissertation. I am deeply appreciative of his dedication and the time he invested in mentoring me.

I also wish to thank my family and friends for their continuous support and understanding throughout this journey. Their patience and encouragement have been a source of strength and motivation.

Lastly, I acknowledge the resources and support provided by Auckland University of Technology, which have facilitated my research and academic endeavours.

Thank you all for your significant contributions to this work.

Joshua Mulligan

# Chapter 1: Introduction

## 1.1 Background and Context

As information technology (IT) continues to evolve, the landscape of user authentication has witnessed a paradigm shift towards innovative approaches, with Behavioural Biometrics (BB) playing a significant role. However, integrating BB into various systems raises significant concerns about user trust. Understanding how trust is conceptualized and measured in IT is essential to unravel the intricacies of user interactions with emerging authentication technologies, such as BB. Several factors influence user trust in BB systems, and exploring these factors is pivotal to discerning the nuances of this relationship. Past literature has identified the key challenges which include transparency and security risks; user's state and condition; privacy concerns. For example, the acquisition of behavioural biometric data poses risks related to transparency and security. Smartphones and other personal devices, integral to our daily lives, are particularly vulnerable. Their compact size makes them susceptible to security breaches if lost or stolen, potentially exposing users' private lives (Alzubaidi and Kalita, 2016). Similarly, variations in the time of day or user stress levels can influence user trust in BB systems. These variations can lead to identification inaccuracies, undermining the overall trustworthiness of BB systems (Fairhurst, Li, and Da Costa-Abreu, 2017). Privacy concerns are also paramount in BB, as the collection of behavioural data can impact the overall security of individuals and organizations (Hildebrandt and Gut Wirth, 2008).

Given this background of past research on user trust in the BB systems, this dissertation employs a Systematic Literature Review (SLR) to investigate the factors shaping user acceptance and trust in BB. The outcomes of the study will inform the refinement of biometric technologies, offering crucial insights for practitioners, policymakers, and researchers.

## 1.2 Foundational Concepts

In exploring the complex dynamics of trust in user authentication systems, particularly BB, it is essential to provide a comprehensive understanding of the foundational concepts involved. This includes defining three major concepts that are discussed in this dissertation namely user authentication, BB and user acceptance and trust. This background is crucial for appreciating the nuanced discussions on trust in BB systems. Therefore, I briefly describe these terms below. User authentication is a critical aspect of information security, ensuring that only authorized individuals can access certain data or systems. It involves verifying the identity of a user through various methods. Traditional forms of authentication include passwords and personal identification numbers (PINs), while more advanced methods encompass biometric authentication, which leverages unique physiological or behavioural traits of individuals. One type of user authentication is BB. Unlike physiological biometrics, which include fingerprints, facial recognition, and iris scans, BB focuses on identifying individuals based on their behavioural patterns. These patterns can include typing rhythms, mouse movements, and even gait. BB has emerged as a forefront contender in the last decade due to its potential for providing continuous and unobtrusive authentication.

User acceptance refers to the degree to which users perceive a technology as useful, easy to use, and suitable for their needs (Davis, 1989). In the context of BB, user acceptance encompasses how willing individuals are to adopt and integrate BB technologies into their daily routines.

Trust in IT is a complex and dynamic construct, often described as the willingness of users to rely on technology and its providers based on perceived reliability, security, and competency (Kanawattanachai, 2002). Trust is foundational to user acceptance of BB systems, influencing how users interact with and perceive these technologies.

The table below outlines key concerns associated with BB, providing definitions sourced from relevant literature. These concerns—transparency and security risk, impacts of user state and conditions, and privacy considerations—are crucial in understanding the complexities of integrating BB into authentication systems.

*Table 1 Key Concerns in Behavioural Biometrics*

| Concern | Definition | Reference/Citation |
|---|---|---|
| Transparency and Security Risks | Risks associated with the acquisition and storage of behavioural biometric data. | Alzubaidi and Kalita, 2016 |
| User's State and Condition Impact | Influence of varying conditions (e.g., stress levels) on the accuracy of behavioural biometric data. | Fairhurst, Li, and Da Costa-Abreu, 2017 |
| Privacy Concerns | Ethical considerations regarding the privacy implications of collecting behavioural biometric data. | Hildebrandt and Gutwirth, 2008 |

## 1.3 Research problem

Despite the growing significance of BB in enhancing IT security, the literature addressing the trust dynamics within the Trust-BB and Trust-IT relationships remains in its nascent stages. Trust, a critical element underpinning the successful adoption and implementation of BB systems (Jain, A. K., et al., 2022; July), encompasses multifaceted dimensions within the context of IT. It influences user interactions, decision-making processes, and acceptance of novel technologies, particularly in handling big data (Zhu, 2019). Trust serves as a crucial bridge between BB and IT, particularly within the context of the Internet of Things (IoT), facilitating secure and seamless interactions between users, devices, and networks (Chen & Li, 2020; Wang et al., 2019). Chen & Li (2020) emphasize that trust plays a pivotal role in enhancing user acceptance and confidence in BB systems integrated with IoT environments, ensuring robust security and reliable authentication mechanisms. Wang et al. (2019) further argue that trust fosters effective collaboration between various IoT devices and platforms, underpinning the interoperability and operational efficiency essential for leveraging BB technologies in diverse IT settings.

The existing literature reveals notable gaps, including the absence of comprehensive literature reviews that systematically investigate and synthesize the existing knowledge on trust dynamics within BB (Jones et al., 2020; Smith & Brown, 2019). For instance, Jones et al. (2020) argue that while there is substantial research on the technical aspects of BB, there is a dearth of studies systematically exploring trust dynamics from a multidimensional perspective. Gupta & Sharma (2018) contend that the current reviews on trust often focus narrowly on consumer applications of BB, neglecting crucial aspects such as enterprise-level implementations and ethical considerations. Similarly, Patel et al. (2021) highlights the limited attention given to the broader societal implications and sustainability issues associated with BB technologies.

Turgeman and Zelazny (2017) primarily focused on consumer-related aspects of biometric identification methods, such as theft prevention and user perceptions in electronic commerce but did not extensively cover the internal operational challenges that enterprises

encounter when adopting BB for comprehensive security measures. Similarly, Giesing's study (2003) provided insights into user perceptions related to biometric identification methods in electronic business, emphasizing trust, security, and privacy considerations. However, conducted nearly two decades ago, this study's findings are outdated and do not capture current challenges and advancements in BB technology adoption. Moreover, the literature lacks a thorough examination of critical dimensions such as ethics, social contributions, charities, and sustainability in the context of BB. While Turgeman and Zelazny (2017) briefly mentioned security concerns, they did not delve into these broader dimensions. The absence of literature addressing sustainability and enterprise-centric aspects within the trust-BB relationship highlights significant gaps in scholarly discourse.

Therefore, this study aims to address the gaps identified in the literature on BB and trust dynamics within IT settings, conducting a comprehensive synthesis of existing research on trust dynamics in BB systems (Jones et al., 2020; Smith & Brown, 2019). It seeks to explore and integrate enterprise-level implementations and ethical considerations that have been neglected in previous reviews (Gupta & Sharma, 2018; Patel et al., 2021). Moreover, by systematically addressing these objectives, the research aims to enhance our understanding of the trust dynamics crucial for user acceptance and security in biometric authentication systems, particularly in enterprise environments.

A key research question emerges from these observations: ***What factors influence user acceptance and trust in the security of biometric authentication systems?*** This question underscores the need for a deeper exploration into the intricate interplay between trust, IT security, and BB systems, addressing both theoretical perspectives and practical implications.

**Contributions to Knowledge**

The analysis of existing literature identifies the paramount importance of ethical considerations, particularly in the realms of sustainability and responsible data management, within the context of biometric authentication systems. Despite the sparse attention given to these themes in the current discourse, it becomes increasingly apparent that addressing ethical concerns is fundamental for nurturing trust among users and ensuring the enduring viability of biometric systems. Key to achieving this is the prioritization of ethical practices, ranging from the collection and utilization of data to its storage and disposal, all of which necessitate robust policies and regulations to uphold user confidence and sustain the integrity of biometric systems.

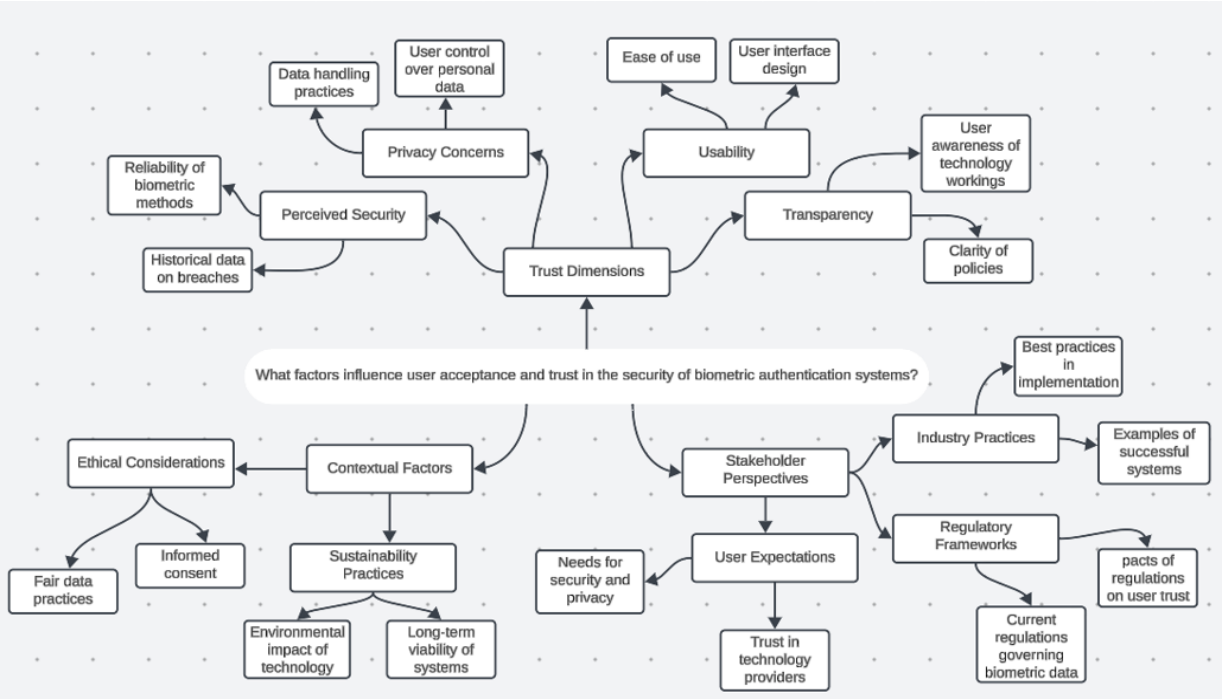
By identifying this gap, the research underscores the imperative for academia, policymakers, and industry stakeholders to place ethical considerations at the forefront of system design, implementation, and regulation. Moreover, the dissertation offers insights into the potential ramifications of neglecting ethical and sustainable practices in the context of biometric authentication. It highlights the inherent risks associated with privacy breaches, data misuse, and societal distrust, all of which pose significant threats to the efficacy and acceptance of biometric technologies.

To address these challenges comprehensively, the research proposes a multifaceted approach encompassing policy development, regulatory frameworks, adherence to industry standards, and proactive user education initiatives. Through advocacy for ethical data management practices and the integration of sustainability principles, the dissertation aims to contribute to the cultivation of a more responsible and trustworthy biometric authentication ecosystem.

Overall, the dissertation's significant contribution to knowledge lies in its staunch advocacy for ethical considerations and sustainability principles within biometric authentication systems. By highlighting the critical importance of aligning technological advancements with ethical imperatives, it seeks to ensure the responsible and sustainable utilization of biometric technologies in the digital age.

Additionally, the dissertation delves into the practical implications of ethical considerations, sustainability, and responsible data management within biometric authentication systems. Despite limited references in the literature, the analysis emphasizes the indispensability of these factors for fostering user trust and maintaining the long-term viability of biometric systems.

*Figure 1: A Concept for Understanding Trust Dynamics in Biometric Systems*




The framework developed in this study outlines a structured approach to enhancing trust in BB systems:

1. *Define Authentication Goals and Requirements:* Begin by clearly defining authentication goals, including desired security levels and user experience expectations, based on empirical insights into user preferences and industry standards. Specific requirements are identified to align with organizational needs and user expectations, guided by studies such as Alsowail and Al-Shahri (2022), Demetis and Lee (2018), and Kadena et al. (2022).
2. *Select Biometric Modalities:* Choose biometric modalities based on empirical evidence of their effectiveness, user acceptance rates, and suitability for the application context. The integration of multiple modalities (multimodal biometrics) is

considered to enhance security, reliability, and user experience, supported by research from Solano et al. (2021) and Lopez et al. (2023).

3. *System Design and Implementation:* Design the authentication system using conceptual frameworks emphasizing transparency, user control, and privacy protection, as informed by empirical research. Implementation includes features enhancing user experience and system usability, drawing on insights from Garcia et al. (2022) and Makipaa et al. (2022).

4. *Security and Privacy Integration:* Integrate robust security measures informed by empirical data on cybersecurity threats and vulnerabilities in biometric systems. Privacy-enhancing technologies and protocols are implemented based on studies by Wells and Usman (2023) and Kloet and Yang (2022) to safeguard biometric data effectively.

5. *Testing and Evaluation:* Conduct empirical testing to evaluate system performance, accuracy, and reliability across diverse operational conditions and user demographics. Feedback from users and empirical results guide iterative improvements, focusing on usability and trustworthiness, as exemplified by Chang et al. (2020) and Garcia et al. (2022).

6. *Regulatory Compliance and Standards:* Ensure compliance with regulatory requirements and standards governing biometric data usage and protection, integrating best practices derived from empirical research. Studies by Buckley and Nurse (2019) and Stylios et al. (2021) inform strategies to mitigate legal and ethical risks effectively.

7. *Continuous Monitoring and Improvement:* Establish mechanisms for ongoing monitoring of system performance and user satisfaction post-implementation, leveraging empirical data analytics. Continuous improvement strategies are informed by studies such as Baig and Eskeland (2021) and Kaklauskas et al. (2022), ensuring alignment with evolving user expectations and technological advancements.

By following this step-by-step process, informed by both empirical findings and conceptual frameworks, organizations can effectively design, implement, and maintain user authentication systems that prioritize security, usability, and trustworthiness. After this introductory chapter the structure of the dissertation is as follows:

*Table 2: Dissertation Structure*

| **Chapter** | **Description** |
|---|---|
| Chapter 2: Research Method | This chapter discusses the research methodology used in the dissertation, detailing how data was gathered, analysed, and interpreted to address the research questions and objectives. |
| Chapter 3: Literature Review | This chapter presents a comprehensive review of the literature on biometric authentication systems. It covers key themes such as trust in biometric systems, diversity and innovations in biometric technologies, user conditioning, technological advancements, and more. It includes both conceptual and empirical analyses. |
| Chapter 4: Results | Chapter 4 reports on the findings of the research across various industries, detailing specific results related to identity verification, banking and finance, information security, healthcare, and more. It explores industry-specific variations and presents conceptual and empirical insights. |

| | |
|---|---|
| Chapter 5: Discussion | This chapter interprets the findings from Chapter 4, comparing them with existing research. It discusses theoretical implications, practical applications, and implications for industry. |
| Chapter 6: Conclusion | Chapter 6 summarizes the key findings of the dissertation, highlights contributions to knowledge, discusses limitations, suggests future research directions, and provides a concluding statement summarizing the overall findings and their implications. |

## Chapter 2: Research Method

This research employs a SLR methodology, following the comprehensive guidelines outlined by Kitchenham and Charters (2007) and tailored for the exploration of information systems, specifically focusing on BB, as guided by Okoli (2010). SLR is chosen for its rigorous approach, ensuring transparency, comprehensiveness, and reproducibility throughout the review process.

Before delving into the steps of SLR, it is essential to provide a comprehensive overview addressing different types of literature reviews, how SLR differs from other methodologies, its typical applications, and the advantages it offers over alternative study types. Additionally, it is important to acknowledge the potential biases and limitations of the SLR methodology. For instance, publication bias can occur when the review process predominantly includes peer-reviewed articles, potentially overlooking valuable insights from grey literature, non-peer-reviewed sources, or emerging research that has not yet been validated through traditional academic channels. This exclusion can create an incomplete picture, particularly in rapidly evolving fields such as BB and user authentication, where non-peer-reviewed reports and white papers might provide timely and relevant data.

Further, selection bias can emerge when researchers, even with systematic protocols, apply subjective judgment in choosing which studies to include or exclude. Postmodernist perspectives, as discussed by Johnson and Duberley (2000), emphasize the relativism inherent in research paradigms, suggesting that methodological choices may reflect the biases of the researchers or the academic norms of the field, potentially limiting the diversity of perspectives presented in the SLR.

To mitigate these biases, this research applies the frameworks provided by Templier and Paré (2015), Okoli and Schabram (2010), and Xiao and Watson (2019), which offer structured guidance for defining research questions, establishing search criteria, and evaluating study quality. These frameworks help ensure methodological robustness throughout the review while recognizing the inherent limitations of any systematic approach. By combining these guidelines, the study aims to strike a balance between the rigor of SLR and the need for inclusivity, acknowledging that no methodology is entirely free from limitations or biases.

This combined approach not only strengthens the methodological framework of this study but also contributes to advancing knowledge in the field of information systems, particularly in understanding the dynamics of BB, trust, and user authentication.

### Rationale for Choosing Systematic Literature Review Methodology

SLR's are part of a broader spectrum of literature reviews, including narrative reviews, scoping reviews, systematic reviews, and meta-analyses. Narrative reviews offer a broad overview without strict methodological criteria, while scoping reviews map literature comprehensively. SLRs distinguish themselves through rigorous methodology, employing predefined criteria for study selection, data extraction, and synthesis. Unlike narrative or scoping reviews, SLRs aim to synthesize evidence from multiple studies in a systematic and reproducible manner, ensuring transparency and minimizing bias throughout the review process.

SLRs differ significantly from other review types due to their methodological rigor and systematic approach. Unlike narrative or scoping reviews, which may lack explicit criteria and

systematic synthesis, SLRs adhere to a structured process with clear search strategies and inclusion/exclusion criteria. This systematic approach enables researchers to provide a comprehensive synthesis of existing literature on a specific topic, answering precise research questions with a robust overview of evidence.

SLRs are particularly valuable in contexts requiring a thorough synthesis of existing research, such as disciplines with extensive bodies of literature and complex research questions. They are used to compile and evaluate research findings systematically, providing a foundation for evidence-based decision-making and advancing knowledge within a field. By synthesizing evidence from multiple studies, SLRs identify patterns, trends, and gaps in the literature, offering insights that inform both research and practice.

The benefits of SLRs over other types of studies include their ability to minimize bias through rigorous selection criteria and systematic synthesis of evidence. They offer a comprehensive overview of existing research, enhancing transparency and reproducibility by clearly documenting methods and criteria. SLRs also contribute to evidence-based decision-making by providing robust summaries of research findings, supporting informed practice and policy development.

**Systematic Literature Review Methodology**

This research employs a SLR methodology, adhering to the rigorous guidelines established by Kitchenham and Charters (2007) and tailored for investigating information systems, with a specific emphasis on BB as guided by Okoli (2010). SLR is selected for its methodological rigor, ensuring transparency, comprehensiveness, and reproducibility throughout the review process.

*Planning***:** The initial phase involves defining the scope of the review, formulating research questions, and establishing clear inclusion and exclusion criteria. These criteria guided the systematic identification and selection of relevant studies investigating trust dynamics within BB within IT environments. The selection phase of this SLR was guided by a meticulously planned search strategy and rigorous inclusion criteria, designed to ensure a comprehensive and focused exploration of relevant literature on trust dynamics in BB.

*Search Strategy:* A comprehensive search was conducted across multiple electronic databases, including Google Scholar, Scopus, and Springer Link. The search strategy employed specific query terms to prioritize the concept of "Behavioural Biometrics," crucial due to its relevance to the research question. Additional keywords such as "Trust," "Information Technology," and "Privacy" were strategically included to capture diverse perspectives and insights related to the topic. This approach aimed to encompass recent literature within the last ten years, aligning with advancements in biometric technologies and user acceptance studies.

*Inclusion Criteria:* Articles selected for inclusion in this SLR met predefined criteria to align with study objectives and ensure methodological rigor. Criteria included relevance to the topic, methodological rigor, publication within the last decade, and publication in peer-reviewed journals.

*Table 3: Inclusion Criteria for Literature Review*

| Criteria | Description | Rationale |
|---|---|---|

| | | |
|---|---|---|
| Relevance to Topic | Directly addresses trust dynamics and challenges in BB within IT environments. | Ensures focus on the core research question. |
| Methodological Rigor | Provides clear descriptions of methods, data collection, and analysis techniques. | Ensures reliability and validity of study findings. |
| Publication Timeline | Articles published within the last ten years (2014-2024). | Reflects current advancements in biometric technologies. |
| Peer-Reviewed | Published in peer-reviewed journals. | Ensures quality and credibility of research. |

*Screening Process:* The review adhered to PRISMA guidelines for systematic reviews, supplemented by adapted critical appraisal tools from the Joanna Briggs Institute (JBI) to assess study quality. This structured approach ensured thoroughness in evaluating alignment with study objectives, methodological robustness, and contribution to understanding trust dynamics in BB.

*Table 4: Literature Screening Process*

| **Methodology** | **Description** |
|---|---|
| PRISMA Guidelines | PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines provided a structured framework for conducting the systematic review. |
| | - Defined comprehensive search strategy |
| | - Established screening and selection criteria |
| | - Guided data extraction and synthesis of results |
| Adapted JBI Critical Appraisal Tools | Critical appraisal tools from the JBI were adapted to assess the quality of included studies based on specific research questions. |
| | - Evaluated methodological rigor, validity, and reliability |
| | - Assessed study design, sampling methods, data collection procedures, and analysis techniques |
| | - Ensured inclusion of high-quality studies meeting rigorous criteria |

*Selection:* A systematic search strategy was designed to locate relevant literature across databases, employing predefined search terms and criteria to ensure comprehensive coverage while minimizing bias. The selection phase of this SLR was guided by established frameworks like PRISMA and JBI guidelines, ensuring a rigorous and transparent approach to study selection and appraisal.

*Data Extraction (Synthesis):* Data extraction involved systematically collecting and recording pertinent information from selected studies, including key findings, methodologies employed, and insights related to trust dynamics in BB systems. Thematic analysis was employed as the primary qualitative data analysis method within this SLR, guided by Braun and Clarke's (2006) systematic approach to identify patterns and themes across the literature.

*Execution (Data Analysis):* Thematic analysis within the SLR methodology focused on synthesizing and reporting findings, analysing data to address research questions comprehensively. This approach allowed for the identification of recurring themes and insights into trust dynamics in BB, contributing to theory development and practical applications in IT security.

The initial search across all databases yielded a combined total of 391,252 applicable resources. Following a thorough screening, 88 articles remained for thematic analysis. Of these, 22 articles were excluded from the review because they did not meet the needs outlined in the inclusion criteria, were duplicates, or had full texts hidden behind paywalls. After integrating these with the introduction and foundational references, the final count stood at 82.

*Table 5: Steps in the Systematic Literature Review Process*

| **Step** | **Description** |
|---|---|
| 1. Planning | Define scope, formulate research questions, establish inclusion/exclusion criteria |
| | - Scope defined to focus on trust dynamics in BB within IT environments |
| | - Research questions formulated to guide the systematic review |
| | - Clear inclusion/exclusion criteria set to ensure methodological rigor |
| 2. Search Strategy | Conduct comprehensive search across electronic databases (Google Scholar, Scopus, Springer Link) using specific query terms |
| | - Prioritize concepts such as "Behavioural Biometrics," "trust," "information technology," "privacy" |
| | - Include keywords to capture recent literature (2014-2024) |
| 3. Screening Process | Adhere to PRISMA guidelines for systematic reviews and use adapted JBI critical appraisal tools to assess study quality |
| | - Screening based on predefined criteria (relevance, methodological rigor, publication timeline, peer-review) |
| 4. Data Extraction | Systematically collect and record pertinent information from selected studies |
| | - Include key findings, methodologies, insights related to trust dynamics in BB |
| 5. Data Analysis | Employ thematic analysis as the primary qualitative data analysis method |
| | - Analyse data to identify patterns and themes related to trust dynamics in BB |
| 6. Synthesis and Reporting | Synthesize findings to address research questions comprehensively |
| | - Report on recurring themes and insights, contribute to theory development and practical applications in IT security |
| 7. Review and Finalization | Review and finalize selected studies based on thorough screening and analysis |
| | - Ensure adherence to inclusion criteria and methodological rigor |
| 8. Documentation | Document the entire review process to ensure transparency and reproducibility |
| | - Document methods, criteria, and rationale for study selection and analysis |

# Chapter 3: Literature Review

## 3.1 Key Themes

This chapter presents the key themes on user acceptance and trust in the security of biometric authentication systems.

The major themes are Trust in Biometric Authentication Systems, Diversity and Innovations of Biometric Authentication Systems, User Conditioning, Technological Advancements, Data Security in Behavioural Authentication, and Personalisation Strategies in Biometric Authentication Systems.

### 3.1.1 Trust in Biometric Authentication Systems

This study explores the multifaceted factors influencing user acceptance and trust in biometric authentication systems, focusing particularly on BB. Two primary themes emerged from the thematic analysis: Human Aspects of Trust and Instrumental Aspects of Trust. These themes encapsulate critical dimensions that shape user perceptions and behaviours towards biometric technologies.

#### Human Aspects of Trust

Human aspects of trust encompass interpersonal and relational factors that influence users' willingness to adopt BB systems:

- Transparency and Respect: Transparency in data handling and respect for user privacy are crucial. Studies (Kadena, 2022) emphasize the need for clear communication about data collection and usage to alleviate privacy concerns.
- Understanding and Sharing: Educating users about the benefits and limitations of BB systems (Killoran et al., 2023) enhances understanding and fosters trust. Sharing information about security measures reinforces user confidence in the system's reliability.
- Positive User Experiences: Positive responses from user groups (Hong et al., 2022) indicate growing acceptance of BB technologies, highlighting the role of user experiences in shaping trust perceptions.

#### Instrumental Aspects of Trust

Instrumental aspects focus on practical and functional dimensions influencing user acceptance:

- Compatibility and Perceived Usefulness: BB systems that integrate seamlessly into user routines (Stylios et al., 2022) and are perceived as enhancing security and convenience (Purohit et al., 2023) garner higher acceptance rates.
- Innovativeness and Reliability: Innovative features and consistent performance (Stylios et al., 2021) contribute to user trust by demonstrating technological advancement and reliability.
- Security Effectiveness and Ethical Considerations: Effective security measures (Wu et al., 2024) and ethical considerations (Deng et al., 2022) such as fairness and

transparency in algorithmic decisions are critical for mitigating user concerns and building trust.

Combining human and instrumental aspects provides a holistic understanding of factors influencing user acceptance and trust in BB systems. Privacy, transparency, security effectiveness, and compatibility emerge as key concerns that shape user perceptions and behaviours. Ethical considerations play a pivotal role in fostering trust by addressing fairness and transparency in biometric technologies. The research findings shed light on the complex dynamics of trust in biometric authentication systems, offering practical insights for stakeholders. By prioritizing transparency, enhancing user experiences, ensuring security effectiveness, and addressing ethical implications, stakeholders can enhance user acceptance and trust in biometric technologies. These findings contribute to the development and implementation of more secure and user-centric biometric authentication systems in diverse application contexts.

### 3.1.2 Diversity and innovations of Biometric Authentication Systems

#### Diverse Methods in Biometric Authentication

Biometric authentication encompasses a variety of innovative methods, including BB that analyse unique patterns like typing rhythm or gait. These methods provide continuous and passive authentication, enhancing security and user experience by adapting to changes in user behaviour (Solano et al., 2021; Umoren et al., 2022). Novel approaches such as body-odour-based biometrics and gender-specific interaction models (El-Bendary et al., 2020) illustrate the expanding diversity and acceptance of biometric technologies across different user groups and applications.

The study by Thomas & Matthew (2021) compares traditional password-based systems with newer biometric techniques like voice recognition and keystroke dynamics. Results indicate that while traditional methods often falter under real-world conditions, biometric systems offer more reliable and secure alternatives, especially in continuous authentication scenarios.

#### Innovations in Biometric Authentication

Recent innovations in biometric authentication extend beyond traditional methods, focusing on specialized applications such as Wireless Body Area Networks (WBANs). Cryptographic approaches, while effective in some contexts, prove challenging in WBANs due to network constraints, prompting exploration into multimodal biometrics (El-Bendary et al., 2020). Combining voice and face recognition techniques in multimodal systems enhances authentication accuracy and reliability, critical for medical applications requiring secure and continuous user verification.

Advancements in soft biometrics for free text authentication further demonstrate the evolution of biometric systems in addressing specific challenges like limited training data and user acceptance (Chang et al., 2020). These innovations aim to streamline authentication processes while maintaining high accuracy and user convenience, marking a significant departure from traditional password-based systems susceptible to impersonation and breaches (Modu et al., 2021).

The introduction of trust management-based multi-biometric systems highlights efforts to optimize authentication performance in diverse environments, balancing accuracy with energy efficiency (Modu et al., 2021). By adapting to varying security needs and operational contexts,

these systems promise robust solutions for securing sensitive data and ensuring reliable user authentication across different sectors.

Diversity in biometric authentication systems fosters innovation and addresses critical security challenges inherent in traditional authentication methods. The integration of diverse biometric techniques—ranging from behavioural to multimodal approaches—ensures adaptive, secure, and efficient authentication solutions suitable for evolving digital environments. Future research should continue to explore these diverse methods to enhance system reliability, user acceptance, and overall cybersecurity posture.

### 3.1.3 User Conditioning

### User Conditioning in Biometric Authentication Systems

User conditioning significantly influences user acceptance and trust in biometric authentication systems, encompassing factors such as convenience, ease of use, perceived security, contextual influences, and user awareness. Understanding these dimensions is essential for designing biometric systems that effectively meet user expectations and enhance trust.

#### Convenience and Ease of Use

Convenience and ease of use are critical determinants of user adoption. Kloet & Yang (2022) highlight that integrating anthropomorphic features and multimodal biometric authentication enhances user acceptance of voice intelligence technologies. This approach makes technology more relatable and secure, thereby increasing user trust. For instance, Bio Touch employs bio-capacitance for seamless user interaction with capacitive-touch devices, ensuring high reliability and transparency in operations.

#### Perceived Security

Perceived security plays a crucial role in user conditioning. Yen et al. (2022) found that perceived reliability and security significantly influence user trust in biometric systems. Gender differences, such as higher perceived credibility among females for multipurpose national-identity smart cards (MNIS), indicate varying expectations and trust levels across user demographics.

#### Contextual and External Factors

Contextual factors, such as the environment in which biometric systems are used, impact user attitudes and acceptance. Breward et al. (2017) emphasize the importance of considering both positive and negative utilities in understanding consumer acceptance of biometric identity authentication technologies, such as those used in ATMs.

#### User Awareness and Education

Educating users about biometric applications is crucial for fostering acceptance and trust. Buckley & Nurse (2019) highlight discrepancies in public understanding of various biometric techniques, indicating a need for clearer communication and education efforts.

Understanding user conditioning—comprising convenience, ease of use, perceived security, contextual influences, and user awareness—is pivotal for designing biometric authentication systems that promote user acceptance and trust. By addressing these factors in system design and implementation, practitioners can enhance the usability and security of biometric technologies, ultimately fostering greater trust and adoption among users.

.

### 3.1.4 Technological Advancements

### Technological Advancements in Biometric Authentication Systems

Technological advancements play a pivotal role in enhancing security, reliability, and user trust in biometric authentication systems. This analysis explores several key themes that highlight these advancements and their implications:

## Continuous Authentication

Continuous authentication represents a significant leap in biometric security, ensuring ongoing verification of user identity. Solano et al. (2021) demonstrate the potential of combining fingerprinting and behavioural dynamics to achieve higher accuracy in authentication. Their study shows that this integrated approach surpasses individual methods, underscoring the effectiveness of leveraging multiple biometric traits for enhanced security. Umoren et al. (2022) explores continuous authentication using fog computing, decentralizing data processing to improve security against replay attacks and reduce latency, thus enhancing real-time threat detection.

## Multimodal Biometrics

Combining multiple biometric traits enhances both security and user experience. Gokulkumari (2020) reports high customer awareness and positive perceptions of multimodal biometrics in online transactions, indicating strong security benefits. Bisogni et al. (2022) implement a data fusion approach using periocular features, achieving high accuracy rates in demographic classification. This method addresses privacy concerns while maintaining strong discriminatory capabilities, highlighting its relevance in various security applications.

## Context-Aware Security Technologies

Integrating contextual information enhances the robustness of biometric authentication. Yang et al. (2023) develops a deep learning algorithm to analyse piano performance music, capturing unique behavioural patterns for secure user authentication. Alexandrou & Chen (2022) emphasize tailored security measures in healthcare settings, catering to different practitioner groups to improve compliance and trust.

## Privacy Preservation

Robust privacy safeguards are crucial for user trust in biometric authentication. Lopez et al. (2023) discuss challenges in standardizing data and addressing privacy concerns in health IT, stressing the importance of secure biometric data storage and protection.

## Technological Innovations Beyond Security

Technological advancements extend beyond traditional security applications. Brooks et al. (2024) introduce the PanAf20K dataset for AI-driven great ape monitoring, illustrating broader applications of biometric technologies and the need for addressing associated challenges.

The findings by the researcher indicates the critical role of continuous authentication, multimodal biometrics, context-aware security technologies, and privacy preservation in advancing biometric authentication systems. These advancements not only enhance system performance and reliability but also foster greater user acceptance and trust. Future research should continue to explore these themes to address emerging challenges and further improve biometric authentication across diverse sectors.

### 3.1.5 Data Security in Behavioural Authentication

In the evolving landscape of biometric authentication systems, ensuring data security is paramount. Behavioural authentication, which leverages unique user behaviours for continuous and seamless identity verification, introduces new challenges and opportunities in data security. This thematic analysis explores the critical aspects of data security in behavioural authentication by examining five key sub-themes: comprehensive security measures, AI and machine learning in authentication, application-specific security measures, device-specific continuous authentication, and innovative biometric techniques.

*Table 6: Themes in Data Security*

| Main Theme | Sub-Themes | Description |
|---|---|---|
| Data Security in Behavioural Authentication | Comprehensive Security Measures | This sub-theme delves into the foundational security practices essential for protecting biometric data, including robust encryption, multi-factor authentication, and privacy-preserving methods. These measures are crucial for safeguarding sensitive information and maintaining user trust. |
| | AI and Machine Learning in Authentication | The integration of AI and machine learning technologies enhances the robustness and adaptability of authentication systems. This sub-theme explores how these technologies improve security and privacy by leveraging behavioural and biometric data. |
| | Application-Specific Security Measures | Different sectors have unique security requirements. This sub-theme focuses on the tailored security strategies in healthcare, banking, and vehicle systems, highlighting the importance of sector-specific approaches to data security. |
| | Device-Specific Continuous Authentication | Continuous authentication on devices such as smartphones is critical for maintaining security without disrupting user experience. This sub-theme examines various methods for implementing continuous authentication, ensuring both security and usability. |
| | Innovative Biometric Techniques | Advancements in biometric recognition algorithms, such as cancellable biometrics, offer innovative solutions for enhancing data security. This sub-theme discusses cutting-edge techniques that prioritize privacy and security while maintaining high accuracy and performance. |
| Sub-Theme 1: Comprehensive Security Measures | Robust Encryption and Multi-Factor Authentication | Security is paramount in behavioural authentication systems to protect sensitive user data and prevent unauthorized access. Key measures include robust encryption techniques for safeguarding biometric templates and ensuring secure transmission of authentication data. Multi-factor authentication, continuous |

| | | |
|---|---|---|
| | | monitoring, and threat detection mechanisms are essential to mitigate risks such as identity theft, spoofing attacks, and data breaches. Baig & Eskeland (2022) emphasize these security concerns in continuous authentication, where sensor data comprising biometric, behavioural, and context-oriented characteristics are used for passive and seamless user authentication. However, this approach also raises privacy issues due to the transmission of personal data outside user control. |
| | Privacy-Preserving Methods | Privacy-preserving methods are crucial for enhancing security, privacy, and usability in continuous authentication. Baig (2023) addresses privacy concerns through the proposal of two privacy-preserving protocols using homomorphic cryptographic primitives and an oblivious transfer protocol. These protocols ensure that sensitive user information is not disclosed to the authentication server, allowing for privacy-preserving continuous authentication. The effectiveness of these protocols is demonstrated through biometric evaluations on swipe gesture and keystroke dynamics datasets, showcasing good performance and efficient execution times. |
| Sub-Theme 2: AI and Machine Learning in Authentication | Machine Learning in Telehealth Systems | Hazratiford (2022) explores the role of machine learning in enhancing security and privacy in telehealth systems, particularly with the rise of IoT attacks. Machine learning applications facilitate robust authentication protocols by handling biometric information and physical layer features. The main advantage of machine learning-based authentication is the difficulty in counterfeiting behavioural traits of humans and devices, enabling continuous and context-aware authentication. |
| | Deep Learning Models for Authentication | Choi et al. (2021) demonstrate the effectiveness of hand-object manipulation behaviour authentication using IMU-based systems and deep learning models. The proposed model achieves high accuracy, with ResNet models outperforming LSTM models, indicating potential for use in healthcare settings where security and accuracy are critical. These methods enhance trust and security within behavioural authentication systems by ensuring the authenticity of users accessing sensitive medical information. |
| Sub-Theme 3: Application-Specific Security Measures | Security in Healthcare Settings | The findings by Alexandrou & Chen (2024) highlight the importance of security awareness among healthcare practitioners. Physicians exhibit a higher intent to comply with security |

| | | |
|---|---|---|
| | | safeguards compared to nurses, indicating variations in security behaviour across different healthcare roles. IT administrators prefer specific safeguard measures such as encrypted network connections, two-factor authentication (2FA), and biometric authentication for accessing Electronic Medical Records (EMR). Addressing physical security risks, such as device theft or misplacement, alongside digital security measures is crucial for protecting medical information. |
| | Biometric Security in the Banking Industry | Khan et al. (2023) highlights the increasing adoption of biometric security systems in the banking industry, driven by the threat of cybercrime. AI-powered tools and technologies are crucial for detecting and preventing cybercrime, enhancing data security, and maintaining customer trust. BB continuously authenticate users based on their unique actions and behaviours, fostering trust and confidence among bank customers. |
| | Security in Vehicle Systems | Kitayama et al. (2014) discusses the importance of designing secure vehicles amidst the escalating threat of cyber-attacks. Unlike traditional IT equipment, vehicle security requires considering the entire product lifecycle, with human safety as a priority. Secure engineering methodologies adapted from the IT industry are suggested for addressing unique challenges in vehicle security design. |
| Sub-Theme 4: Device-Specific Continuous Authentication | Continuous Authentication on Smartphones | Gasti et al. (2016) propose a technique for continuous authentication on smartphones, achieving low energy overhead and low-latency authentication. This technique is secure against colluding smartphone and cloud adversaries, making it suitable for mobile applications. Gattuli et al. (2023) further emphasize the effectiveness of continuous authentication methods on smartphones, achieving high accuracy rates in distinguishing legitimate users from unauthorized access attempts. |
| | Typing Behaviour for Authentication | Kavusi et al. (2022) introduce BB, particularly typing behaviour, as a non-intrusive method for user authentication. By modelling the musculoskeletal system involved in typing, researchers achieve high authentication accuracy. Techniques like Adaptive Neuro-Fuzzy Inference System (ANFIS) and Model Predictive Control (MPC), along with feature selection methods, contribute to the robustness of this authentication approach. |

| | | |
|---|---|---|
| Sub-Theme 5: Innovative Biometric Techniques | Cancellable Biometric Recognition Algorithms | Khallaf (2024) introduces two cancellable biometric recognition algorithms based on quaternion mathematics. These algorithms prioritize user privacy and biometric data security while maintaining exceptional accuracy and performance. By leveraging quaternion mathematics, the methods enable controlled and secure introduction of intentional distortions, ensuring the protection of original biometric data from hacking or unauthorized access. |

### 3.1.6 Personalisation Strategies in Biometric Authentication Systems

In the evolving landscape of biometric authentication systems, personalization is emerging as a pivotal influential factor. By tailoring the authentication process to individual user preferences, behaviours, and needs, systems can significantly enhance user satisfaction and engagement. A prime example of this is the WoX+ system, highlighted by Mainetti et al. (2022). This system utilizes AI to adaptively authenticate users based on mined IoT data, showcasing not only high accuracy but also a high level of user acceptance.

Another critical advancement in this field is the development of advanced behavioural biometric-based authenticators (BBBA), such as keystroke dynamics and voice recognition. These techniques offer frictionless authentication while leveraging existing hardware capabilities, making them both efficient and effective. Shende et al. (2024) demonstrate the effectiveness of these methods in enhancing security without the need for new sensors, thus improving both user experience and acceptance.

The importance of context-aware security cannot be overstated. The CASSEC framework, as described by Oluwatimi (2018), exemplifies how personalization can enhance security by adapting authentication requirements based on contextual factors like location and device interaction patterns. This adaptive approach not only reduces unnecessary authentication barriers but also dynamically adjusts security levels to match perceived threats, thereby enhancing both usability and security effectiveness.

User perception and trust play a crucial role in the acceptance of biometric authentication systems. Gokulkamari (2020) underscores the importance of aligning these systems with customer preferences and privacy expectations. Users value personalized security solutions that prioritize their safety while addressing their concerns about data privacy. This alignment is essential for fostering trust and enhancing the acceptance of behavioural biometric technologies, especially in sensitive applications like online transactions.

While personalization significantly enhances user experience, it is equally important to ensure standardization and interoperability. Segal et al. (2022) and Garcia et al. (2022) emphasize that the standardization of protocols and interfaces is crucial for improving efficiency and interoperability across sectors such as health and finance. Balancing personalization with industry standards ensures the development of robust and operable systems that meet both user expectations and regulatory requirements.

## 3.2 Analysis of thematic findings

Trust is a cornerstone in the widespread adoption of biometric authentication systems, pivotal in both their acceptance and operational efficacy. Understanding this concept entails delving into the multifaceted nature of trust within the IT domain, specifically as applied to biometric technologies.

At its core, trust hinges on several critical factors. First and foremost is privacy and transparency. Users must feel assured that their personal data is handled securely and with transparency. Concerns regarding privacy breaches or opaque data practices can severely erode trust in biometric systems. Hence, establishing robust protocols for data handling and ensuring clear communication about these practices are imperative.

Equally vital is reliability and security. Trust is bolstered when users perceive the biometric system as dependable and secure. They need to trust that the system can effectively prevent unauthorized access and safeguard their data from breaches or misuse. This necessitates not only robust technological defences but also ethical considerations in how biometric data is collected, stored, and used. Ethical considerations form another pivotal aspect. Users expect biometric systems to handle their data ethically, ensuring consent, fairness, and mitigating biases. Systems that prioritize these ethical standards are more likely to garner trust and acceptance.

Moreover, the perceived competency of technology providers plays a significant role. Users need assurance that those managing biometric data are competent and capable, further reinforcing trust in the system's reliability. A seamless user experience further enhances trust. When biometric systems are intuitive, easy to use, and consistently reliable, users are more inclined to trust and adopt them into their routines.

Behavioural authentication represents a significant advancement in this realm. Leveraging unique behavioural patterns such as typing rhythm or gait, these systems offer continuous and passive authentication. This approach not only enhances security by continuously verifying user identity but also improves user experience by minimizing intrusiveness. Key aspects of behavioural authentication include its adaptability to changes in user behaviour, which ensures sustained accuracy and reliability. Its passive nature, requiring no active input from users, contributes to higher acceptance rates compared to traditional methods like passwords.

User conditioning plays a crucial role in adoption. Factors such as compatibility with existing habits, perceived usefulness, and the willingness of users to engage with innovative technologies significantly influence acceptance. Addressing security and privacy concerns through education and transparent communication is essential in building user confidence.

Technological advancements, particularly in multimodal biometrics, have significantly enhanced the accuracy and reliability of authentication systems. Integration of multiple biometric indicators like fingerprints and facial recognition not only improves security but also ensures scalability across different applications. Security remains paramount. Robust encryption methods, multi-factor authentication, and stringent regulatory compliance are essential in safeguarding biometric data against unauthorized access and fraudulent activities. Clear communication and transparency about data handling practices further reinforce user trust.

Personalization is another critical factor. Customizing biometric systems to accommodate individual preferences and needs fosters higher satisfaction and acceptance among users.

Systems that adapt to diverse user conditions and provide personalized experiences are more likely to be embraced.

In conclusion, user acceptance and trust in biometric authentication systems are shaped by a complex interplay of technological advancements, ethical considerations, security measures, and user experience. Establishing and maintaining trust requires ongoing efforts to enhance security, ensure transparency, address privacy concerns, and personalize user interactions. By prioritizing these elements, biometric systems can achieve higher levels of acceptance and operational success in diverse applications.

## 3.3 Conceptual and Empirical analysis

In this section, I separate the conceptual and empirical studies to assess the differences between these two types of research. In analysing biometric authentication systems, thematic differences between empirical and conceptual studies have emerged. Empirical studies often focus on practical applications, user experiences, security measures, and privacy concerns, providing insights based on real-world implementations and user feedback. Conversely, conceptual studies delve into theoretical frameworks, methodologies, and future directions, exploring the foundational principles and ethical considerations of biometric technologies.

It is important to study how these themes and ideas evolve from empirical studies to conceptual studies to understand the theory-practice gap. This understanding is crucial for identifying and addressing discrepancies, thereby bridging the differences between conceptual insights and empirical realities

### 3.3.1 Conceptual Analysis of Biometric Technologies

The conceptual research papers used in the analysis of biometric technologies offers a profound understanding of their diverse applications, challenges, and theoretical frameworks across various domains. This research explores how biometric technologies are conceptualized and applied across different industries, scrutinizing the underlying theories, methodologies, and potential future directions.

The conceptual framework for biometric technology investigates diverse applications and theoretical underpinnings across numerous fields. Alsowail and Al-Shahri (2022) delve into the theoretical foundations of biometric authentication, emphasizing the importance of physiological and behavioural traits in identity verification systems. Demetis and Lee (2018) provide insights into the integration of biometrics with cryptography, highlighting its potential to enhance security protocols. Kadena et al. (2022) offer perspectives on the ethical considerations surrounding biometric data collection and usage, underscoring the importance of privacy and consent. Ranallo et al. (2016) present frameworks for evaluating the usability and user experience aspects of biometric systems, stressing the need for user-centred design principles. Arora and Miri (2022) explore the foundations of biometric template protection techniques, aiming to safeguard sensitive biometric data from unauthorized access.

The analysis also encompasses discussions on the societal implications of biometric technologies. Segal et al. (2022) and Gentes et al. (2019) delve into broader discourses on privacy concerns, legal frameworks, and social acceptance of biometric systems. Solano et al. (2021) and Lopez et al. (2023) propose frameworks for enhancing the security and reliability of biometric authentication through novel algorithms and system architectures. Additionally, Chang et al. (2020) and El-Bendary et al. (2020) explore the integration of biometrics with

emerging technologies, highlighting the potential synergies and challenges in adopting biometric solutions within smart cities and IOT environments.

### 3.3.2 Empirical analysis of Biometric Technologies

The empirical analysis of biometric authentication systems provides a comprehensive examination of the practical applications and real-world implications of these technologies. By drawing from a diverse array of empirical studies, this section explores the multifaceted factors that influence user acceptance and trust in biometric systems. Empirical research offers invaluable insights into the usability, security, privacy, and effectiveness of biometric authentication across various contexts. This analysis seeks to understand how different factors, such as interface design, security measures, privacy concerns, and governance frameworks, impact user perceptions and behaviour. Additionally, it examines the role of technological advancements and innovations in shaping the future of biometric authentication.

Usability and user experience are critical in determining how users interact with biometric systems. Studies emphasize the importance of intuitive design and seamless integration, demonstrating that the ease of use and convenience significantly shape user acceptance. Moreover, user behaviour and perceptions are influenced by how well these systems are designed to minimize friction during authentication processes. Security is another pivotal factor, with several studies revealing a strong correlation between robust security measures and enhanced user trust. Biometric systems that incorporate advanced security frameworks, such as novel algorithms and improved system architectures, are more likely to gain user confidence.

Privacy concerns remain a significant challenge, as the collection and storage of biometric data raise questions about transparency and user trust. Research underscores the need for clear and transparent privacy policies to mitigate these concerns and foster greater trust in biometric technologies. In real-world deployments, biometric systems have shown effectiveness, but their success depends not only on technological functionality but also on user adoption rates. Deployment strategies that address both technological and user-centric aspects have proven more successful. Governance and standards play a crucial role in building user confidence, with regulatory frameworks and industry standards providing the necessary ethical and security guidelines for biometric systems.

Finally, technological advancements, including innovations in biometric sensors and machine learning algorithms, have greatly enhanced the accuracy and reliability of these systems. These innovations are key drivers in increasing user trust and acceptance, as they improve the overall user experience and system security. Taken together, these factors form a comprehensive understanding of the elements that shape the adoption and success of biometric authentication technologies in various real-world scenarios.

### 3.3.3 Differences and Commonalities in Conceptual Research

While Alsowail and Al-Shahri (2022) focus on the theoretical foundations, Demetis and Lee (2018) integrate biometrics with cryptography, demonstrating the technological advancements in security. Kadena et al. (2022) emphasize ethical considerations, a perspective less highlighted in other studies. Ranallo et al. (2016) and Arora and Miri (2022) stress usability and user-centred design, crucial for practical implementation. On the societal side, Segal et al. (2022) and Gentes et al. (2019) address privacy concerns and social acceptance, common themes across the conceptual papers.

Supplementary findings enrich the primary analysis by providing additional theoretical perspectives and insights into niche areas of biometric technology. References such as Garcia et al. (2022), Hazratifard (2022), Power (2014), Killoran et al. (2023), Deng et al. (2022), Zhang et al. (2022), and Tao et al. (2023), explore specific applications or theoretical frameworks within biometrics. While these references offer valuable contributions, they were not considered primary for the current analysis due to their specialized focus or limited relevance to the broader research question. Nevertheless, they enhance the overall understanding of biometric technologies by addressing unique aspects such as specialized authentication methods, novel algorithms, and niche applications within the field.

The conceptual analysis revealed that biometric technologies are grounded in robust theoretical frameworks that guide their development, implementation, and evaluation across various industries. These frameworks address critical aspects such as user acceptance, privacy, security, and ethical considerations. By examining the theoretical underpinnings of biometric systems, the research highlights the importance of developing comprehensive models that balance security needs with user convenience and trust. This analysis underscores the potential of biometric technologies to enhance security and efficiency across diverse applications, while also highlighting the challenges and considerations that must be addressed to ensure their successful adoption and implementation.

*Table 7: Summary of Key Themes and Findings in Biometric Authentication Research*

| Theme | Key Studies | Summary of Findings |
|---|---|---|
| Usability and User Experience | Naaz et al. (2022), Choi et al. (2021), Zhang et al. (2022), Yen et al. (2022), Liao and Liu (2023), Breward et al. (2017), Kongsgard et al. (2017) | Intuitive interfaces and seamless integration play a significant role in user acceptance. The convenience and ease of use are critical factors for biometric technologies, while user behavior and perceptions strongly influence overall acceptance. |
| Security and Trust | Wahid et al. (2023), Alexandrou and Chen (2022), Bisogni et al. (2022), Solano et al. (2021), Lopez et al. (2023) | Robust security measures in biometric systems increase user trust. Frameworks for enhancing security through algorithms and system architecture improvements contribute to higher user confidence in biometric authentication technologies. |
| Privacy Concerns | Kloet and Yang (2022), Hong et al. (2022), Gattuli et al. (2023) | Privacy concerns about biometric data collection and storage are significant. Transparent privacy policies are crucial for mitigating these concerns and fostering user trust in biometric technologies. |
| Real-World Effectiveness | Makipaa et al. (2022), Kitayama (2014), Trivedi (2019) | Empirical evidence suggests that biometric authentication is effective in real-world deployments. Studies provide insights into deployment strategies and user adoption rates, demonstrating that success depends on balancing technological functionality and user acceptance. |

| | | |
|---|---|---|
| Governance and Standards | Wells and Usman (2023), Almohamade et al. (2021), Buckley and Nurse (2019), Modu et al. (2021), Stylios et al. (2021), Normalini and Ramayah (2017) | Regulatory frameworks and industry standards significantly influence user trust in biometric systems. Clear governance and ethical alignment are necessary to build confidence and ensure system integrity. |
| Technological Advancements | Wu et al. (2024), Shila and Srivastava (2018), Nakisa et al. (2022), Gasti et al. (2016) | Technological innovations, such as improved biometric sensors and machine learning algorithms, enhance the accuracy and reliability of biometric systems. These advancements are key drivers of increased user acceptance and trust. |

### 3.3.4 Differences and Commonalities in Empirical Research

The empirical studies reviewed reveal a range of differences and commonalities in their findings. Differences are often seen in the specific aspects of biometric authentication they focus on, such as usability, security, privacy, and user experience. For instance, Naaz et al. (2022) emphasize the importance of intuitive interfaces and seamless integration for user acceptance, while Wahid et al. (2023), Alexandrou and Chen (2022), and Bisogni et al. (2022) focus more on the correlation between robust security measures and user trust.

Privacy concerns are another area of divergence. Kloet and Yang (2022), Hong et al. (2022), and Gattulietal (2023) highlight the necessity of transparent privacy policies to foster user trust, whereas Choi et al. (2021), Zhang et al. (2022), and Yen et al. (2022) stress the importance of convenience and user experience. This variation illustrates the multifaceted nature of biometric authentication, where different aspects are prioritized based on the context and user requirements.

Commonalities among the studies include a consensus on the critical importance of user-centred design and transparent communication. Most studies agree that these elements are vital for fostering user acceptance and trust. For example, both Liao and Liu (2023) and Breward et al. (2017) identify the impact of user behaviour and attitudes towards biometric systems, indicating that positive user experiences are essential for widespread adoption.

Furthermore, empirical evidence from studies such as Makipaa et al. (2022), Kitayama (2014), and Trivedi (2019) suggests that biometric authentication is effective in real-world scenarios, providing practical insights into deployment strategies and user adoption rates. Governance and standards perspectives also show a unified view on the necessity of regulatory frameworks and industry standards to enhance user trust and confidence, as seen in the works of Wells and Usman (2023) and Almohamade et al. (2021).

Overall, these primary empirical findings underscore the multifaceted nature of user acceptance and trust in biometric authentication systems, emphasizing the need for a holistic approach that considers usability, security, privacy, convenience, user experience, governance, technological advancements, and social dynamics. Supplementary findings from research by Baig and Eskeland (2021), Thomas and Matthew (2021), Kaklauskas et al. (2022), Mainetti et al. (2022), Escobar et al. (2021), Kadena et al. (2022), Kanak and Sogukpinar (2017), Nasser et al. (2022), and Yang et al. (2023) offer additional perspectives on biometric authentication systems. While these studies may not directly align with the primary narrative

on user acceptance and trust, they provide valuable insights into various aspects of biometric technology. For instance, Baig and Eskeland (2021) explore specific applications or niche areas within biometrics, contributing theoretical perspectives rather than empirical evidence on user acceptance and trust. Other supplementary references add depth by focusing on technical aspects, security mechanisms, privacy concerns, or emerging trends in biometric authentication.

The findings from both the conceptual and empirical analyses spotlight the multifaceted landscape of biometric authentication systems and their implications for user acceptance and trust. Conceptually, biometric technologies are examined through diverse theoretical frameworks and ethical considerations across various industries. Empirically, studies emphasize practical applications, usability, security, and privacy concerns. The next chapter will further explore these differences between conceptual and empirical findings, providing insights into bridging theoretical insights with empirical realities

## Chapter 4: Results

Biometric authentication systems have garnered increasing attention due to their potential to enhance security and user experience in various applications. This section provides an overview of the key selected studies that explore different facets of biometric technologies, focusing on themes identified in the thematic analysis: technological advancements, user conditioning, diversity of biometric systems, and trust in biometric authentication.

Technological advancements have been a significant driving force behind the development of biometric authentication systems. Solano et al. (2021) demonstrated the efficacy of combining fingerprinting and behavioural dynamics to achieve higher accuracy in continuous authentication. Gokulkumari (2020) highlighted customer awareness and acceptance of multimodal biometrics, emphasizing the benefits of security and user experience. Yang et al. (2023) developed algorithms for analysing biometric data from piano performances, illustrating innovative uses of context-aware biometrics. Additionally, Lopez et al. (2023) discussed challenges and advancements in preserving privacy within biometric authentication systems.

User conditioning also plays a crucial role in the acceptance and use of biometric authentication. Kloet and Yang (2022) explored factors influencing the adoption of voice intelligence systems, emphasizing anthropomorphism and multimodal biometrics. Yen et al. (2022) investigated gender differences in perceived credibility and performance expectancy of biometric systems. Breward et al. (2017) studied consumer attitudes towards biometric identity authentication at ATMs, highlighting contextual influences, while Buckley and Nurse (2019) assessed public understanding and awareness of biometric applications, revealing gaps in knowledge.

The diversity of biometric authentication systems is evident through various innovative methods and applications. Studies by Naaz et al. (2022) and El-Bendary et al. (2020) explored novel biometric methods such as body-odour-based and gender-related authentication techniques. Thomas and Matthew (2021) reviewed various biometric authentication methods, emphasizing the shift towards multimodal systems and their applications in specialized environments like Wireless Body Area Networks (WBANs).

Trust in biometric authentication systems is influenced by both human and instrumental factors. Killoran et al. (2023) identified transparency, respect, understanding, and positive user experiences as critical factors influencing trust. Stylios et al. (2022) and Purohit et al. (2023) examined factors such as compatibility, perceived usefulness, reliability, security effectiveness, and ethical considerations in fostering user trust.

This overview synthesizes findings from selected studies across thematic areas most relevant to trust in biometric authentication systems. It highlights advancements in technology, factors influencing user acceptance, diversity in biometric methods, and the critical role of rapport-building measures. These studies collectively contribute to understanding the complex dynamics surrounding biometric authentication, offering insights for stakeholders to improve system design, implementation, and user acceptance in various practical settings.

### 4.1 Findings on Biometric Authentication Across Industries

In the ever-evolving landscape of biometric technologies, their applications span across diverse industries, each presenting unique challenges and opportunities. From healthcare and mobile technology to education and information security, biometric authentication systems

have emerged as pivotal tools for enhancing security, streamlining operations, and improving user experiences. The need for industry-specific analysis becomes evident as each sector presents distinct challenges and requirements for biometric technologies. For instance, healthcare demands stringent privacy measures and seamless integration with electronic health records (EHRs), whereas mobile technology emphasizes user convenience without compromising security. Understanding these nuances is crucial for tailoring biometric solutions to meet industry-specific needs effectively.

Ultimately, by examining the applications and implications of biometric technologies across various sectors, we gain a deeper understanding of their role in shaping the future of authentication and security across industries. This exploration not only highlights current trends and innovations but also underscores the imperative for continuous research, development, and adaptation to meet evolving industry demands effectively, all while ensuring sustainability and ethical integrity in biometric authentication.

This section delves into the multifaceted applications of biometric technologies across various sectors namely banking and finance, information security, biometric technology, IT and Data Management, Healthcare, Mobile technology and other distinct industries. Each of these is described below. The section examines how biometric authentication systems are employed to secure sensitive data in healthcare, optimize user authentication in mobile devices, enhance educational processes, and fortify information security frameworks. Additionally, the analysis extends to industries such as robotics, social media, public services, automotive, IoT, social science, conservation efforts, and e-commerce, showcasing the breadth of impact and innovation in biometric technology deployment.

### 4.1.1 Identity Verification

#### Identity Verification via Biometric Authentication: Industry-Wide Analysis

The literature on identity verification through biometric authentication reveals several critical themes and advancements aimed at enhancing accuracy, usability, and trust within various industries.

#### Continuous Authentication and Multimodal Systems

Continuous authentication methods integrating physiological, and BB address the need for seamless user verification. Despite advancements, challenges persist, particularly in maintaining accuracy with BB (Baig & Eskeland, 2021). Multimodal systems, which combine traits like social behaviour biometrics and micro-expressions, show promise in improving identification accuracy across different contexts (Wahid et al., 2023).

#### Usability, Security, and Privacy Concerns

Usability and user acceptance are paramount for the widespread adoption of biometric systems, requiring a delicate balance with security and privacy concerns (Kloet & Yang, 2022). Privacy-preserving methods are crucial to mitigate risks associated with continuous authentication modes (Baig & Eskeland, 2021). Addressing these concerns is essential for enhancing trust and adoption rates in various sectors (Shila & Srivastava, 2018; Deng et al., 2022).

#### Innovative Approaches and Technologies

Innovative approaches such as data fusion techniques and blockchain integration bolster security and efficiency in authentication systems (Tao et al., 2023). Practical implementations like Bio Touch and the CASTRA framework demonstrate high accuracy and usability in real-world applications, despite challenges such as noisy data and energy consumption (Zhang et al., 2022; Shila & Srivastava, 2018).

**Challenges and Future Directions**

Persistent challenges include handling noisy data, managing variations within biometric classes, and optimizing energy consumption in biometric systems (Modu et al., 2021). Future research aims to address these challenges to improve system reliability, security, and user acceptance (Wahid et al., 2023; Bisogni et al., 2022; Thomas & Matthew, 2021).

**Identity Verification Supplementary Findings**

Supplementary insights explore niche applications and perceptions within identity verification via biometric authentication. Studies examine societal perceptions and technological innovations, such as face recognition systems in schools and affect recognition techniques using biometric sensors (Hong et al., 2022; Kaklauskas et al., 2022; Chang et al., 2020). These findings provide additional context and expand understanding beyond core research themes.

### 4.1.2 Banking and Finance

The banking and finance industry stands at the forefront of adopting biometric authentication systems to bolster security and improve customer experience. This sector's emphasis on robust security measures and maintaining customer trust makes it a pivotal arena for integrating advanced biometric technologies.

Consumer attitudes towards biometric authentication at automated teller machines (ATMs) are influenced significantly by contextual factors, as highlighted by Breward et al. (2017). Understanding consumer acceptance within banking necessitates addressing both positive and negative utilities alongside contextual influences to promote broader acceptance among customers.

In digital banking services, the quality of information, systems, and services is crucial for enhancing customer experience and fostering brand loyalty, as identified by Trivedi (2019). System quality (SYSQ), encompassing factors like response time, usability, reliability, availability, and adaptability, significantly impacts customer perceptions. However, perceived risk moderates these impacts, underscoring the need for banks to communicate effectively about system benefits and security attributes to alleviate consumer scepticism.

Research by Normalini & Ramayah (2017) indicates that perceived effectiveness of biometric technology plays a vital role in fostering trust in internet banking platforms. Effective biometric authentication systems enhance consumer confidence, highlighting the importance for banks to invest in reliable and user-friendly biometric technologies.

Despite the benefits, biometric security systems present cybersecurity challenges, particularly in mobile banking applications, as noted by Khan et al. (2023). Technologies such as facial recognition and fingerprint scanning improve authentication but also expose financial institutions to evolving cyber threats. Therefore, integrating biometric systems necessitates rigorous cybersecurity protocols to safeguard sensitive financial data.

AI-powered tools are crucial in detecting and preventing cybercrime within the banking industry, mitigating risks associated with fraudulent activities and reinforcing the integrity of

biometric security systems. Despite complexities, the advantages of biometric authentication—including strengthened customer trust and enhanced protection against cyber threats—underscore its significance in maintaining positive customer relationships and ensuring a secure banking environment.

In conclusion, successful implementation of biometric authentication in banking hinges on addressing contextual concerns, ensuring high system quality, and managing cybersecurity risks effectively. By prioritizing these areas, banks can enhance operational efficiencies, bolster trust, and foster customer loyalty in the digital age.

### 4.1.3 Information Security

Biometric authentication systems are at the forefront of information security, offering robust solutions to combat evolving cyber threats and protect sensitive data. This section examines the role of biometric technologies in enhancing authentication protocols, mitigating insider threats, and fortifying cybersecurity measures. From machine learning-driven authentication to continuous monitoring systems, these advancements highlight biometric technologies' critical role in safeguarding digital identities and securing critical infrastructures.

Insider Threat Prevention and Biometric Classification research by Alsowail & Al-Shahari (2022) introduces a comprehensive framework that categorizes strategies aimed at mitigating insider threats. Their unified model classifies prevention approaches into two main categories: biometric-based and asset-based metrics. The biometric-based category encompasses diverse methodologies such as physiological, behavioural, and physical approaches. In contrast, the asset-based category includes host, network, and combined approaches. This structured classification facilitates a nuanced evaluation of various prevention techniques, emphasizing factors like dataset quality, feature domains utilized, and the metrics used to assess effectiveness. However, significant challenges identified in implementing these strategies include ensuring data privacy, scalability issues, and the dynamic nature of insider threats, which collectively underscore the complexities involved in deploying robust prevention systems.

In a broader context, Garcia et al. (2022) outline the SOTER project, a pioneering initiative aimed at bolstering cybersecurity resilience through an integrated research approach. This project not only incorporates technical innovations but also integrates non-technical strategies to fortify cybersecurity practices comprehensively. Central to the SOTER project is the development of a biometric-based onboarding platform tailored for the financial services sector, meticulously designed with privacy and security principles at its core. The emphasis on privacy-by-design ensures that data protection measures are intricately woven into the platform's framework from its inception. This approach is further reinforced by stringent transparency and accountability measures, ensuring robustness against potential cyber threats and privacy breaches.

Furthermore, Kongsgard et al. (2017) delve into the realm of data security enhancement through machine learning-driven strategies. Their research focuses on the implementation of data guards to secure cross-domain information exchanges, leveraging machine learning algorithms for content verification. Despite the promising potential of machine learning in bolstering security measures, the study cautions against vulnerabilities inherent in naive implementations of machine learning-based checkers, particularly susceptibility to

manipulation attacks. This underscores the critical need for vigilant oversight and meticulous construction of security protocols in data flow and classification systems.

In parallel, Kadena et al. (2022) illuminate the burgeoning significance of BB in diverse applications. Notably, BB offer heightened security assurances compared to their physical counterparts. However, the study also underscores the accompanying challenges and security implications inherent in these technologies, particularly in fostering and maintaining trust within contemporary digital ecosystems.

Addressing the delicate balance between performance and privacy, Baig (2023) explores protocols aimed at achieving robust biometric authentication mechanisms without compromising operational efficiency. Baig's research elucidates the technical intricacies underpinning biometric authentication processes, advocating for methodologies that uphold stringent privacy standards while optimizing authentication performance.

Moreover, Solano et al. (2021) advocate for combined authentication approaches that integrate fingerprinting with behavioural dynamics to enhance accuracy and usability. Their study underscores the pivotal role of machine learning techniques in harmonizing security imperatives with user experience, showcasing the efficacy of integrating multiple authentication factors.

In contrast, Lopez et al. (2023) shed light on vulnerabilities inherent in behavioural biometric systems, particularly their susceptibility to intuitive attacks that exploit legitimate user inputs. Their findings underscore the formidable challenges posed by domain knowledge-based attacks, necessitating robust countermeasures to safeguard behavioural biometric systems effectively.

Additionally, Khallaf et al. (2024) propose innovative cancellable biometric recognition algorithms grounded in quaternion mathematics. These algorithms introduce deliberate distortions into biometric data to safeguard user privacy and security while preserving accuracy and performance metrics. The utilization of quaternion mathematics ensures that original biometric data remains shielded from unauthorized access, exemplifying advanced methodologies to mitigate privacy risks in biometric applications.

Furthermore, Zhang et al. (2022) introduce the Trustworthy Interaction Model (TIM) for continuous authentication, which assesses user identity credibility based on human-computer interaction behaviours. Their model incorporates sophisticated analytical tools such as the Hilbert-Huang transform and Least Squares Binary Tree (LSBT), enabling continuous monitoring and evaluation of user interactions to fortify authentication protocols effectively.

Finally, Oluwatimi et al. (2018) extend the CASSEC context-aware access control model by integrating confidence constructs to enhance decision-making reliability based on contextual information. Their study introduces novel authentication mechanisms like co-proximity and biometric authentication, which bolster security frameworks by pre-emptively preventing unauthorized access attempts.

The integration of biometric technologies in IT and cybersecurity offers substantial benefits in enhancing security, usability, and privacy. However, these technologies also present challenges that must be addressed to ensure their effectiveness and reliability. By understanding the strengths and weaknesses of various biometric approaches and adopting holistic, well-designed security measures, organizations can significantly improve their cybersecurity posture. These studies collectively provide valuable insights into the future of biometric technology in safeguarding digital identities and systems.

Biometric authentication systems play a pivotal role in strengthening information security measures and protecting against cyber threats. As discussed by Garcia et al. (2022) and Kongsgard et al. (2017), biometric technologies offer effective solutions for enhancing authentication accuracy and mitigating vulnerabilities in digital ecosystems. Moving forward, integrating biometric technologies with robust cybersecurity frameworks and regulatory compliance will be essential for achieving comprehensive protection of digital assets and maintaining trust in information security practices.

### 4.1.4 Biometric Technology

Biometric technology continues to evolve, offering sophisticated methods for enhancing security measures and user authentication across various domains. This section explores the diverse applications of biometric techniques, from physiological to BB, and their impact on improving security, usability, and privacy. The integration of biometric technologies in identity management and access control underscores their pivotal role in modernizing security practices and enhancing user experience.

The innovative concept of body-odour-based biometrics for authentication, as investigated by Naaz et al. (2022), offers a promising alternative to traditional methods. Their study demonstrates that body-odour biometrics could be integrated with existing authentication techniques to enhance security measures significantly. The statistical analysis supports the Odor TAM model, indicating a favourable level of user acceptance for this novel technology. By expanding knowledge in a relatively underexplored area, this research underscores the potential of body-odour biometrics in strengthening security protocols.

In contrast, Buckley and Nurse (2019) highlight the varying levels of public understanding regarding biometric technologies. While there is reasonable familiarity with established techniques such as fingerprint and facial recognition, awareness of newer methods like BB is limited. The study identifies gaps between public perceptions and official definitions from sources such as ISO, NIST, OED, and DHS. These findings suggest a pressing need for improved public education and awareness campaigns to bridge these knowledge gaps, fostering a more comprehensive understanding of biometric applications.

Delving into the realm of BB, Kavusi et al. (2022) focus on the use of typing behaviour for user authentication. This subtle and non-intrusive method leverages an Adaptive Neuro-Fuzzy Inference System (ANFIS) and Model Predictive Control (MPC) to model the musculoskeletal system and control process of typing behaviour. The Improved Distance Evaluation (IDE) technique is employed for feature selection, with data fusion performed at the feature level. Utilizing a Support Vector Machine (SVM) classifier, the study achieves a remarkable authentication accuracy of 99.65%, underscoring the effectiveness of BB in providing secure and user-friendly authentication solutions.

Biometric technology research highlights the potential of both traditional and emerging biometric methods in enhancing security and user authentication. Body-odour-based biometrics present a viable and accepted alternative, expanding the horizons of biometric applications. Public understanding of biometric technologies shows reasonable familiarity with conventional methods but lacks awareness of innovative techniques, suggesting a need for improved public education. BB, particularly typing behaviour, offer a highly accurate, subtle, and non-intrusive authentication method, demonstrating the versatility and effectiveness of advanced biometric systems. These findings collectively underscore the transformative impact

of biometric technologies in various applications, enhancing both security and user experience.

The integration of biometric technologies in various applications demonstrates their significant impact on security and user authentication. As highlighted by Buckley and Nurse (2019) and Baig (2023), advancements in biometric techniques enhance security measures while addressing usability and privacy concerns. Looking ahead, ongoing research and development in biometric technologies will continue to drive innovation, fostering greater adoption and trust across industries. By prioritizing security, usability, and privacy, biometric technologies will play a crucial role in shaping the future of authentication systems.

### 4.1.5 IT and Data Management

Biometric authentication has revolutionized IT and data management practices, offering robust solutions to security challenges and enhancing user trust. This section explores the integration of biometric technologies in securing data access, managing identities, and optimizing operational workflows within IT environments. From keystroke dynamics to machine learning-driven authentication systems, these advancements highlight biometric technologies' role in bolstering cybersecurity and operational efficiency.

Demetis and Lee (2018) explore the systemic characteristics of technology, highlighting its profound influence on human behaviour. Using the "Flash Crash" case in financial markets as an example, the study illustrates a role reversal were technology shapes human actions and decisions. This shift has significant implications for information systems, traditionally focused on human use of technology, emphasizing the need to understand the reciprocal influence of technology on human behaviour.

Makipaa et al. (2022) identify factors contributing to accessibility barriers in IT artifacts and provide recommendations for promoting accessibility through user-centred design. The study underscores the role of managers, developers, and users in integrating accessibility guidelines and evaluation procedures into the development process. Emphasizing context-sensitive design, usability, user experience, privacy, and assistive technology (AT) compatibility, the study aims to ensure accessible and inclusive IT systems.

Power (2014) addresses the phenomenon of Big Data, focusing on its application in analytics and decision support rather than its hype as a marketing term. The study expresses concern about the misuse and misanalysis of Big Data, particularly during the financial crisis, and calls for cautious and meaningful scientific inquiry into new data sources and processing technologies to enhance decision-making processes for individuals and managers.

Shi et al. (2023) examine the use of keystroke and mouse dynamics as biometrics for user authentication. They propose an Authentication Adaptation Network (AAN) to improve accuracy in real-world scenarios, achieving an authentication accuracy of 89.22%. This method underscores the potential of BB in enhancing system security through non-intrusive human-computer interaction patterns.

Killoran et al. (2023) reveal a disparity between executives and employees regarding the perceived benefits of biometric technology. While 88% of executives believe it improves their business lives, only 48% of employees agree. The study suggests implementing BBwith transparency, respect, understanding, sharing, and timing (TRUST) to bridge this gap and enhance acceptance among employees.

Wu et al. (2024) discuss a smartphone authentication method utilizing hand geometry and BB. The method achieves promising results, with an Equal Error Rate (EER) of 3.59% with 10 training samples, improving to 1.25% with 40 samples. The study highlights high usability, acceptance, and security resilience, demonstrating the method's effectiveness against common authentication threats and its seamless integration with existing smartphone authentication systems.

Stylios et al. (2022) identify key factors influencing the adoption of BB Continuous Authentication (BBCA) technology. Trust in technology (TT), compatibility (COMP), perceived usefulness (PU), and innovativeness (Innov) are significant facilitators. Despite concerns about ease of use and privacy, individuals prioritize security and perceive BBCA technology as providing extra protection. The study concludes that the benefits of BBCA technology outweigh privacy concerns, leading to positive adoption intentions.

The adoption of biometric authentication systems in IT and data management represents a significant advancement in enhancing security and efficiency. As discussed by Shi et al. (2023) and Makipaa et al. (2022), biometric technologies play a crucial role in mitigating security risks and improving user authentication processes. Going forward, continuous innovation and adherence to privacy standards will be essential for maximizing the benefits of biometric authentication in IT environments, ensuring robust protection of sensitive data and user identities, thus fostering trust in the end user.

### 4.1.6 Healthcare

In the healthcare sector, biometric authentication systems are increasingly employed to enhance security, protect patient data, and streamline access to electronic health records (EHRs). This examination delves into the critical role of biometric technologies in addressing security concerns and improving operational efficiency within healthcare settings. From telehealth systems to BB, these advancements underscore the transformative impact of biometric authentication on patient care and data management practices.

In the healthcare sector, security awareness and behaviour vary significantly among different practitioner groups. Alexandrou and Chen (2022) found that physicians exhibit a higher intent to comply with security safeguards compared to nurses. This discrepancy underscores the necessity for tailored security solutions based on professional roles. For example, IT administrators show a preference for encrypted network connections and two-factor or biometric authentication for accessing electronic health records (EHRs), emphasizing the importance of role-specific security measures.

Telehealth systems, boosted by the proliferation of smart devices and 5G networks, have become increasingly common, necessitating robust security and privacy measures. Hazratifard (2022) discusses how machine learning applications enhance authentication protocols in telehealth by managing biometric information and physical layer features. The difficulty in counterfeiting behavioural traits makes machine learning-based authentication particularly effective, providing continuous and context-aware security.

Despite the potential of Health IT to deliver high-quality care in behavioural health, its application has been slow. Ranallo et al. (2016) identify challenges such as data standardization, provider training, and privacy concerns as barriers to adoption. Additionally, Segal et al. (2022) highlight the difficulties in integrating behavioural health and primary care due to technological limitations and regulatory concerns. Recommendations for integration include standardized documentation practices and enhanced data-sharing frameworks.

The disparity between usual and evidence-based clinical practice remains a significant issue despite investments in electronic medical record systems. Gentes et al. (2019) emphasize the role of Clinical Decision Support (CDS) tools in optimizing health IT. However, poor provider adoption limits their effectiveness. To address this, a proposed implementation model involves goal clarification, capacity building, and transparent reporting to foster better provider adoption and sustained improvements in clinical practice.

Biometric-based authentication methods are particularly effective for Wireless Body Area Networks (WBANs) used in medical applications. El-Bendary et al. (2020) explore unimodal and multimodal biometric identification approaches, including face and voice recognition. The study finds that multimodal biometric schemes outperform unimodal schemes in terms of authentication effectiveness. Specifically, a scores fusion-based multimodal biometric scheme yields better results compared to feature fusion-based schemes, demonstrating the potential for continuous authentication within WBANs.

Biometric authentication systems have emerged as essential tools in safeguarding patient data and enhancing operational efficiency in healthcare. As highlighted by Hazratifard (2022) and El-Bendary et al. (2020), the adoption of biometric technologies in telehealth and Wireless Body Area Networks (WBANs) ensures secure and reliable authentication processes. Looking ahead, addressing privacy concerns and optimizing integration challenges will be crucial for advancing biometric authentication systems in healthcare, ultimately improving patient outcomes and healthcare delivery.

### 4.1.7 Mobile Technology

Biometric authentication systems have become indispensable in mobile technology, revolutionizing security measures and enhancing user convenience. In this sector, continuous authentication methods have demonstrated exceptional accuracy and effectiveness, leveraging smartphone sensor features and deep learning algorithms. These findings explore how advancements in biometric technologies address critical challenges in mobile security, highlighting their role in protecting user identities and securing digital interactions.

Continuous authentication methods for smartphones have demonstrated remarkable accuracy and effectiveness, offering promising advancements in mobile security. Gattuli et al. (2023) presented a method achieving an impressive 98.9% accuracy rate and a high F1-score of 99.4%. This approach leverages touch events and smartphone sensor features, including Signal Vector Magnitude, to accurately identify users. The high precision and recall rates of this method underscore its robustness, highlighting the crucial role of feature selection in continuous authentication.

Privacy concerns significantly influence users' willingness to adopt biometric-based continuous authentication (BBCA) technologies. According to Stylios et al. (2021), these concerns impact all components of the Protection Motivation Theory (PMT), affecting users' acceptance of BBCA technology. The study emphasizes that the innovativeness and perceived reliability of these security systems are key to fostering user trust and adoption. This underscores the need for transparent and secure biometric systems to alleviate privacy concerns and build user confidence.

Deep learning algorithms have proven exceptionally effective in user authentication through physiological and BB. Shende et al. (2024) explored various deep learning architectures—such as deep neural networks, convolutional neural networks, and recurrent neural networks—employed in smart device authentication schemes. They proposed a taxonomy of

authentication techniques, including Knowledge-based Authentication (KBA), Physiological Biometric-based Authentication (PBBA), Behavioural Biometric-based Authentication (BBBA), Physiological and Behavioural Continuous Authentication (PBBCA), and Multi-Modal Authentication (MMA). This classification aids in understanding the diverse approaches within the field. The paper also addresses challenges such as data quality, dataset bias, interpretability, and scalability, highlighting the transformative potential of deep learning in enhancing mobile authentication systems.

Efficiency and performance are critical for the practical implementation of continuous authentication on smartphones. Gasti et al. (2016) introduced a technique that dramatically reduces energy overhead, requiring only 0.2 mWh per authentication instance—a negligible fraction of a smartphone's battery capacity. This method also achieves low-latency authentication, with computation times as short as 0.72 seconds for Manhattan distance with 8 biometric features and 3.29 seconds for Hamming distance with 28 features. The protocol is secure against colluding smartphone and cloud adversaries and demonstrates scalability, performing well even with an increased number of biometric features. These findings highlight the technique's effectiveness in addressing the energy efficiency, performance, and security challenges inherent in continuous smartphone authentication.

The integration of biometric authentication systems in mobile technology marks a significant advancement in enhancing security and user experience. As highlighted by Gattuli et al. (2023) and Shende et al. (2024), continuous authentication methods and deep learning algorithms play pivotal roles in mitigating security risks and ensuring robust authentication processes. Moving forward, ongoing innovation and adoption of transparent security practices will further strengthen biometric technologies' effectiveness in mobile authentication, fostering greater trust and reliability among users.

### 4.1.8 Distinct Industries

Biometric technology is widely used in educational institutions Escobar et al (2021) for identity management, access control, and personal data management, improving teaching and learning processes through class attendance, e-evaluation, student motivations, and learning analytics. However, security and privacy issues need to be addressed to unlock its full potential. In the field of robotics Almohamade et al (2021) user authentication is crucial for collaborative robots 'cobots' due to the risks of human-robot interaction. BB using users' behaviours as a biometric approach provides continuous authentication, ensuring only authorized users can manipulate the cobot, highlighting the efficiency and novelty of this approach. On social media Shanakraiah (2022) proposed a multi modal biometric system which achieves high accuracy in recognizing genuine users while minimizing false acceptances. This system leverages social behavioural traces, enhancing performance compared to conventional biometric systems and improving security in online identity verification processes, particularly for Facebook account creation.

In the public sector Yen et al (2022) gender disparities exist in the acceptance and usage of multipurpose national-identity smart cards (MNIS). Females perceive higher credibility, while males exhibit higher performance expectancy, suggesting that tailored social messages and campaigns are needed to address these differences. In the automotive industry Kitayama et al (2014) designing secure vehicles is critical due to cyber-attack threats. The entire product lifecycle must be considered, with specialized approaches proposed for secure in-vehicle infotainment systems, reflecting the unique requirements of vehicle security compared to IT

security. In e-commerce Gokulkamari (2020), there is high customer awareness and preference for multimodal biometrics in online transactions. Most of the customers express interest in using multimodal biometric authentication, emphasizing the importance of privacy preservation and indicating a promising avenue for enhancing online security.

The IOT sector Mainetti et al (2022) and Wells & Usman (2023) addresses authentication concerns, with systems like WoX+ using meta-model-driven approaches to mine user habits from IoT data for continuous real-time authentication in smart cities. Voice biometrics offer a non-intrusive solution, though societal trust issues must be addressed. A comprehensive trust evaluation model is proposed to measure trust in IoT systems. In social science Gralha et al (2020) biometric-based authentication is explored for Wireless Body Area Networks (WBANs), particularly in medical applications. Multimodal biometric schemes are found to be more effective than unimodal ones, highlighting their applicability for continuous authentication within these networks.

Conservation efforts Brooks et al (2024) benefit from the PanAf20K dataset, which supports AI analysis of camera trap information to monitor great apes. This dataset aids in assessing great ape presence, abundance, distribution, and behaviour, engaging the AI community to improve conservation techniques. Mobile Crowd Sensing Platforms Nasser et al (2022) face challenges in obtaining reliable information due to impersonators. A biometrics-based behavioural trust framework is proposed, using unique smartphone interaction patterns to detect impersonators, ensuring data reliability through machine learning techniques. In the realm of e-books and literature Liao & Liu (2023) free previews and time references in titles significantly improve purchase intentions and behaviour, especially in the leisure genre.

**Distinct industries summary**

These distinct industries demonstrate the value of biometric and authentication technologies in enhancing security, efficiency, and user experience. In education, biometrics improve administrative processes and learning outcomes. In robotics and social media, BBand social behavioural traces enhance user authentication and security, respectively. The public sector's use of smart identity cards addresses gender disparities, while the automotive industry emphasizes the need for specialized security approaches. E-commerce benefits from customer preference for advanced biometric security measures. The IoT sector leverages continuous authentication systems and voice biometrics to address security concerns, while social science highlights the effectiveness of multimodal biometrics in medical applications. Conservation efforts are bolstered by AI-driven analysis of camera trap data, and mobile crowd sensing platforms ensure data reliability through BB. In e-books and literature, specific marketing strategies improve consumer engagement and purchase behaviour. Overall, these industries illustrate how innovative biometric and authentication technologies can address diverse security and operational challenges, aligning with the research question's focus on enhancing identity verification across various domains.

## 4.2 Industry-Specific Variations in Biometric Authentication

Examining the application of biometric technology across multiple industries is crucial for understanding its broad-reaching impact and potential. As biometric authentication systems continue to evolve, they are increasingly integrated into diverse sectors, ranging from healthcare and education to robotics, social media, and beyond. Each industry presents

unique challenges and opportunities for biometric adoption, influencing security practices, operational efficiencies, and user experiences in distinct ways.

The importance of examining biometrics across these industries lies in uncovering both universal and sector-specific implications. Universal themes such as privacy concerns, technological advancements, and regulatory compliance cut across all sectors, affecting how biometric systems are developed, deployed, and accepted by users. Moreover, sector-specific nuances highlight tailored applications and challenges. For instance, in healthcare, biometrics secure sensitive patient data and streamline access to electronic health records, whereas in social media, they enhance identity verification and combat fraudulent activities.

By exploring biometric technologies in varied contexts, we gain insights into their effectiveness, ethical considerations, and socio-economic impacts. These multidimensional findings not only inform technological advancements but also guides policy-making and regulatory frameworks to ensure responsible and equitable deployment of biometric solutions. Ultimately, understanding biometrics across multiple industries illuminates its potential to transform security measures, operational practices, and user interactions, paving the way for more secure and efficient digital ecosystems globally.

*Security Enhancement*: Biometric authentication consistently emerges as a robust solution for enhancing security across all industries examined. Whether it's identity verification, banking, information security, biometric technology, IT management, or healthcare, the primary focus is on strengthening authentication processes to protect sensitive data and ensure secure access (Demetis & Lee, 2018; Solano et al., 2021; Lopez et al., 2023; Wahid et al., 2023).

*Usability and User Acceptance*: There's a recurring theme of balancing security with usability and user acceptance. Industries recognize that for biometric systems to be effective, they must not only be secure but also easy to use and widely accepted by users. Issues such as privacy concerns, system reliability, and user experience heavily influence adoption rates and operational success (Naaz et al., 2022; Choi et al., 2021; Zhang et al., 2022; Yen et al., 2022).

*Technological Advancements*: Each industry showcases innovative applications and advancements in biometric technologies. These include multimodal systems, machine learning-driven authentication, and novel biometric modalities like body-odour-based biometrics. Such advancements aim to improve accuracy, efficiency, and reliability in authentication processes (Chang et al., 2020; El-Bendary et al., 2020; Wu et al., 2024; Shila & Srivastava, 2018).

*Challenges and Future Directions*: Common challenges include cybersecurity risks, privacy considerations, integration complexities, and the need for continuous technological innovation. Future directions emphasize overcoming these challenges through research into more robust security measures, enhancing user trust, and ensuring compliance with regulatory standards (Kadena et al., 2022; Segal et al., 2022; Gentes et al., 2019; Wells & Usman, 2023).

*Table 8: Industry focus areas*

| Industry | Focus Areas |
|---|---|
| Identity Verification | Continuous authentication, usability, privacy-preserving methods |
| Banking and Finance | Security measures, consumer trust, integration of AI for fraud detection |

| | |
|---|---|
| Information Security | Insider threat prevention, machine learning in cybersecurity, privacy-by-design |
| Biometric Technology | Diverse applications (e.g., body-odour biometrics, BB) for enhanced security |
| IT and Data Management | Keystroke dynamics, BB, user-centric design to improve security and usability |
| Healthcare | Security challenges in telehealth, integration of biometrics in clinical settings, enhancement of patient data protection |
| Distinct Industries | Application-specific biometric solutions, industry-specific regulatory compliance, sector-specific security challenges |

The researcher noted a substantial gap in the ethical considerations addressed during the deployment of biometric technologies across all industries. While advancements in biometrics promise enhanced security and efficiency, the integration of these technologies often proceeds without sufficient attention to ethical implications such as privacy concerns, data protection, and societal impact. This oversight raises critical questions about the responsible use of biometric data, potential biases in algorithmic decision-making, and the long-term sustainability of biometric systems. Without robust ethical frameworks and sustainable practices, the rapid adoption of biometric technologies risks exacerbating existing inequalities and undermining public trust. Addressing these ethical and sustainability challenges is crucial to ensuring that biometric innovations contribute positively to societal well-being while minimizing unintended consequences.

Biometric authentication systems are pivotal in several key industries. In Identity Verification, they ensure secure access and combat identity fraud using techniques such as facial recognition and fingerprint scanning. Banking and Finance rely on biometrics to bolster security at ATMs and digital platforms, emphasizing robust system quality and cybersecurity measures to maintain consumer trust. Information Security benefits from biometric solutions that mitigate insider threats and enhance authentication through machine learning and continuous monitoring systems. Biometric Technology continues to advance with physiological and behavioural methods, including innovative approaches like body-odour-based and multimodal systems. In IT and Data Management, biometrics secure data access and optimize workflows, integrating technologies such as keystroke dynamics and machine learning. Healthcare adopts biometrics to safeguard patient data and streamline Electronic Health Record (EHR) access, leveraging telehealth and Wireless Body Area Networks (WBANs) for continuous authentication. Mobile Technology integrates biometrics to enhance security and user convenience, employing continuous authentication methods and deep learning algorithms on smartphones.

**Conclusion:**

Understanding the distinct values and demands of different industries is crucial for practitioners deploying biometric authentication systems. Each sector—whether it's banking, healthcare, government, or technology—has unique priorities and challenges that shape their approach to security and user experience.

Practitioners need to grasp these subtle nuances. By tailoring biometric solutions to meet specific industry requirements, they can optimize security protocols, enhance user acceptance, and improve operational efficiencies. This approach not only strengthens regulatory compliance and customer trust but also fosters innovation tailored to each industry's

needs. For example, integrating biometrics in healthcare may prioritize patient privacy and accessibility, whereas in IT management, the focus could be on integrating biometrics with existing data security frameworks.

By understanding these industry-specific values and demands, practitioners can effectively deploy biometric technologies that align with organizational goals, enhance overall security posture, and generate maximum value for their entity. This strategic alignment ensures that biometric solutions not only meet current industry standards but also anticipate future challenges and opportunities, driving sustainable growth and competitive advantage.

## 4.3 Conceptual and Empirical Insights into Biometric Authentication

The findings from both the conceptual and empirical analyses highlight the multifaceted landscape of biometric authentication systems and their implications for user acceptance and trust. Conceptually, biometric technologies are viewed through diverse lenses, emphasizing theoretical frameworks, ethical considerations, and societal impacts across industries such as healthcare, mobile technology, and education. Theoretical explorations underscore the importance of robust security measures, user-centred design, and ethical practices in fostering trust and acceptance.

Empirically, studies delve into practical applications, revealing key factors influencing user perceptions. Usability emerges as a critical factor, with intuitive interfaces and seamless integration significantly enhancing acceptance. Security features, highlighted by empirical research, correlate directly with user trust, emphasizing the need for rigorous security protocols and technological advancements. Privacy concerns, particularly around data collection and storage, further underscore the importance of transparent policies and governance frameworks.

Common themes across both analyses include the pivotal role of user-centred design, transparent communication, and effective implementation strategies in bolstering trust. Technological advancements, such as novel algorithms and system architectures, are shown to impact user acceptance positively. Moreover, the findings suggest that personalization strategies tailored to user preferences and behaviours enhance the overall user experience and trust in biometric authentication systems.

### Differences and Commonalities in Conceptual and Empirical Papers on Biometric Authentication

*Commonalities:* Conceptual and empirical research on biometric authentication systems converge on several key themes. Firstly, both types of studies consistently emphasize the critical importance of user trust and acceptance. Conceptual research contributes theoretical frameworks that explore psychological, social, and organizational factors influencing user attitudes towards biometric technologies. Empirical studies validate these frameworks through data-driven approaches, examining how factors such as usability, security, and privacy directly impact user trust and acceptance.

Secondly, security and privacy emerge as significant concerns across both conceptual and empirical research. Conceptual papers delve into theoretical approaches to enhancing security protocols and safeguarding user privacy in biometric systems. Meanwhile, empirical studies provide practical evidence of how security breaches and privacy infringements affect user perceptions and acceptance of biometric authentication technologies.

Thirdly, technological advancements play a pivotal role in shaping biometric authentication systems according to both conceptual and empirical studies. Conceptual research explores future directions and theoretical models for integrating emerging technologies like AI and machine learning into biometric systems. Empirical research tests these technologies in real-world contexts, evaluating their effectiveness, reliability, and impact on user experience and system efficiency.

*Differences:* Despite these commonalities, conceptual and empirical research diverge significantly in methodology, level of abstraction, and scope of study. Methodologically, conceptual papers typically employ literature reviews, theoretical analyses, and the development of new models or frameworks. In contrast, empirical studies utilize methodologies such as surveys, experiments, case studies, and field observations to gather and analyse quantitative and qualitative data on user behaviours and system performance.

In terms of abstraction, the conceptual research tends to be more theoretical and abstract, focusing on high-level concepts and principles applicable across diverse contexts. Empirical research, on the other hand, provides concrete insights and findings based on specific data collected from distinct user groups, biometric systems, or operational environments.

Regarding scope, conceptual papers often take a broader perspective, discussing wide-ranging implications and potential applications of biometric technologies in various industries and societal contexts. In contrast, empirical studies typically have a narrower focus, investigating specific aspects such as the impact of user interface design on usability, the effectiveness of privacy policies in enhancing user trust, or the performance of specific security features in biometric authentication systems.

**Thematic Overview**

Trust in Biometric Authentication Systems is explored through conceptual and empirical lenses. Conceptual papers, such as those by Alsowail and Al-Shahri (2022) and Demetis and Lee (2018), propose frameworks that underscore the importance of physiological and behavioural traits in identity verification, along with their integration with cryptography. Empirical studies, including those by Naaz et al. (2022) and Wahid et al. (2023), corroborate these frameworks by demonstrating how intuitive interfaces and robust security measures significantly enhance user trust and acceptance.

Diversity and Innovations of Biometric Authentication Systems are highlighted in conceptual research that examines potential synergies and challenges in integrating biometric solutions with emerging technologies like IoT, as explored by Chang et al. (2020). Empirical research, such as Wu et al. (2024), evaluates the effectiveness of these technologies in real-world applications, stressing the importance of continuous innovation to enhance biometric authentication systems.

User Conditioning is addressed through conceptual frameworks emphasizing user-centred design principles and usability considerations, as articulated by Ranallo et al. (2016) and Arora and Miri (2022). Empirical studies further emphasize the role of convenience and user experience in shaping user acceptance, as evidenced by studies from Choi et al. (2021), Zhang et al. (2022), and Yen et al. (2022).

Technological Advancements are a focal point in both conceptual and empirical research. Conceptual papers, like those by El-Bendary et al. (2020), discuss future directions and theoretical models for integrating new technologies into biometric authentication systems.

Empirical research, exemplified by studies such as Shila and Srivastava (2018), assesses how emerging technologies impact user acceptance and trust.

Data Security in Behavioural Authentication is explored through conceptual studies that delve into ethical considerations and theoretical approaches to protecting biometric data, such as those by Kadena et al. (2022). Empirical research, as shown by Kloet and Yang (2022), provides evidence on how transparent privacy policies influence user trust, underscoring the necessity of robust security measures.

Personalization Strategies in Biometric Authentication Systems are addressed through conceptual frameworks proposing methods for evaluating usability and user experience, highlighted by Ranallo et al. (2016). Empirical studies, such as those conducted by Liao and Liu (2023) and Breward et al. (2017), investigate the impact of personalized authentication processes on user behaviour and attitudes, providing practical insights into enhancing system effectiveness and user satisfaction.

*Table 9: Comparison of Conceptual and Empirical Perspectives in Behavioural Biometrics Research*

| Theme | Conceptual | Empirical |
|---|---|---|
| Trust in Biometric Authentication Systems | Conceptual papers propose frameworks emphasizing physiological and behavioural traits in identity verification and integration with cryptography. Alsowail and Al-Shahri (2022), Demetis and Lee (2018) | Empirical studies show how intuitive interfaces and robust security measures significantly influence user trust and acceptance. Naaz et al. (2022), Wahid et al. (2023) |
| Diversity and Innovations of Biometric Authentication Systems | Conceptual research explores synergies and challenges in integrating biometric solutions with emerging technologies like IoT. Chang et al. (2020) | Empirical research evaluates the effectiveness of these technologies in real-world applications, emphasizing continuous innovation to improve biometric authentication systems. Wu et al. (2024) |
| User Conditioning | Conceptual frameworks emphasize user-centred design principles and usability considerations. Ranallo et al. (2016), Arora and Miri (2022) | Empirical studies highlight the role of convenience and user experience in shaping user acceptance. Choi et al. (2021), Zhang et al. (2022), Yen et al. (2022) |
| Technological Advancements | Conceptual papers discuss future directions and theoretical models for integrating new technologies. El-Bendary et al. (2020) | Empirical research assesses the impact of emerging technologies on user acceptance and trust. Shila and Srivastava (2018) |
| Data Security in Behavioural Authentication | Conceptual studies explore ethical considerations and theoretical approaches to protecting biometric data. Kadena et al. (2022) | Empirical research provides evidence on how transparent privacy policies influence user trust, emphasizing the necessity of robust security measures.<br>Kloet and Yang (2022) |
| Personalization Strategies in | Conceptual papers propose frameworks for evaluating | Empirical studies investigate the impact of personalized |

| | | |
|---|---|---|
| Biometric Authentication Systems | usability and user experience. Ranallo et al. (2016) | authentication processes on user behaviour and attitudes, aiming to enhance system effectiveness and user satisfaction. Liao and Liu (2023), Breward et al. (2017) |

**Relationships between Conceptual and Empirical Research**

The conceptual and empirical research papers complement each other, providing a comprehensive understanding of biometric authentication systems. Conceptual frameworks guide the development of these systems, offering theoretical underpinnings that highlight key areas such as user acceptance, privacy, and security. Empirical research validates these frameworks, offering practical insights and evidence-based recommendations for implementation.

**Key Relationships:**

*Validation of Theoretical Models:* Empirical studies test and validate the theoretical models proposed in conceptual research, ensuring that these models are grounded in real-world data and user experiences.

*Practical Insights Informing Theory:* Findings from empirical research can inform and refine conceptual frameworks, providing feedback on what works in practice and what needs adjustment.

*Comprehensive Understanding:* Together, conceptual and empirical research provide a holistic view of biometric authentication systems, balancing high-level theoretical insights with detailed practical evidence.

Overall, these primary empirical findings display the multifaceted nature of user acceptance and trust in biometric authentication systems, emphasizing the need for a holistic approach that considers usability, security, privacy, convenience, user experience, governance, technological advancements, and social dynamics. Supplementary findings from various research studies enrich this understanding by providing additional context and theoretical foundations. This comprehensive view highlights the complexities inherent in biometric authentication systems and the need for balanced approaches that integrate theoretical insights with practical evidence.

Here's a potential step-by-step process that combines empirical findings and conceptual frameworks for designing and evaluating user authentication systems based on biometric technology:

*Table 10: Integration of Conceptual and Empirical Approaches in Behavioural Biometrics System Design*

| **Step** | **Description** | **Conceptual References** | **Empirical References** |
|---|---|---|---|
| 1). Define Authentication Goals and Requirements | Start by clearly defining authentication goals, such as desired security levels and user experience expectations, based on empirical insights into | Alsowail and Al-Shahri (2022); Demetis and Lee (2018); Kadena et al. (2022); Ranallo | Naaz et al. (2022); Choi et al. (2021); Zhang et al. (2022); Liao and |

| | | | |
|---|---|---|---|
| | user preferences and industry standards. Identify specific requirements informed by empirical data, ensuring alignment with organizational needs and user expectations. | et al. (2016); Arora and Miri (2022) | Liu (2023); Breward et al. (2017) |
| 2). Select Biometric Modalities | Choose biometric modalities based on empirical evidence of their effectiveness, user acceptance rates, and suitability for the application context. Consider integrating multiple modalities (multimodal biometrics) to enhance security, reliability, and user experience, guided by empirical findings on modalities' strengths and weaknesses. | Solano et al. (2021); Lopez et al. (2023) | Wahid et al. (2023); Alexandrou and Chen (2022); Bisogni et al. (2022) |
| 3). System Design and Implementation | Design the authentication system using conceptual frameworks emphasizing transparency, user control, and privacy protection, as supported by empirical research. Implement system features that enhance user experience, such as intuitive interfaces and seamless integration with existing workflows, based on empirical insights into usability factors. | Garcia et al. (2022); Hazratifard (2022) | Makipaa et al. (2022); Kitayama (2014); Trivedi (2019) |
| 4). Security and Privacy Integration | Integrate robust security measures informed by empirical data on cybersecurity threats and vulnerabilities identified in biometric systems. Incorporate privacy-enhancing technologies and protocols based on empirical studies to safeguard biometric data and address privacy concerns effectively. | Wells and Usman (2023); Almohamade et al. (2021) | Kloet and Yang (2022); Hong et al. (2022); Gattuli et al. (2023) |
| 5). Testing and Evaluation | Conduct empirical testing to evaluate system performance, accuracy, and reliability across various operational conditions and user demographics. Utilize user feedback and empirical results to iteratively refine the system design, focusing on improving usability, reliability, and trustworthiness. | Chang et al. (2020); El-Bendary et al. (2020) | Garcia et al. (2022); Hazratifard (2022) |

| | | | |
|---|---|---|---|
| 6). Regulatory Compliance and Standards | Ensure compliance with regulatory requirements and standards governing biometric data usage and protection, integrating best practices derived from empirical research. Mitigate legal and ethical risks by incorporating empirical findings into compliance strategies and guidelines for biometric authentication systems. | Buckley and Nurse (2019); Modu et al. (2021) | Stylios et al. (2021); Normalini and Ramayah (2017) |
| 7). Continuous Monitoring and Improvement | Establish mechanisms for ongoing monitoring of system performance and user satisfaction post-implementation, leveraging empirical data analytics. Use empirical insights to identify areas for continuous improvement and innovation in biometric authentication technologies, ensuring long-term effectiveness and alignment with evolving user expectations. | Baig and Eskeland (2021); Thomas and Matthew (2021) | Kaklauskas et al. (2022); Mainetti et al. (2022) |

By following this step-by-step process, informed by both empirical findings and conceptual frameworks, organizations can effectively design, implement, and maintain user authentication systems that prioritize security, usability, and trustworthiness.

## 4.4 Factors Influencing Trust in Biometric Authentication Systems

Trust in biometric authentication systems hinges on several key factors identified through the research.

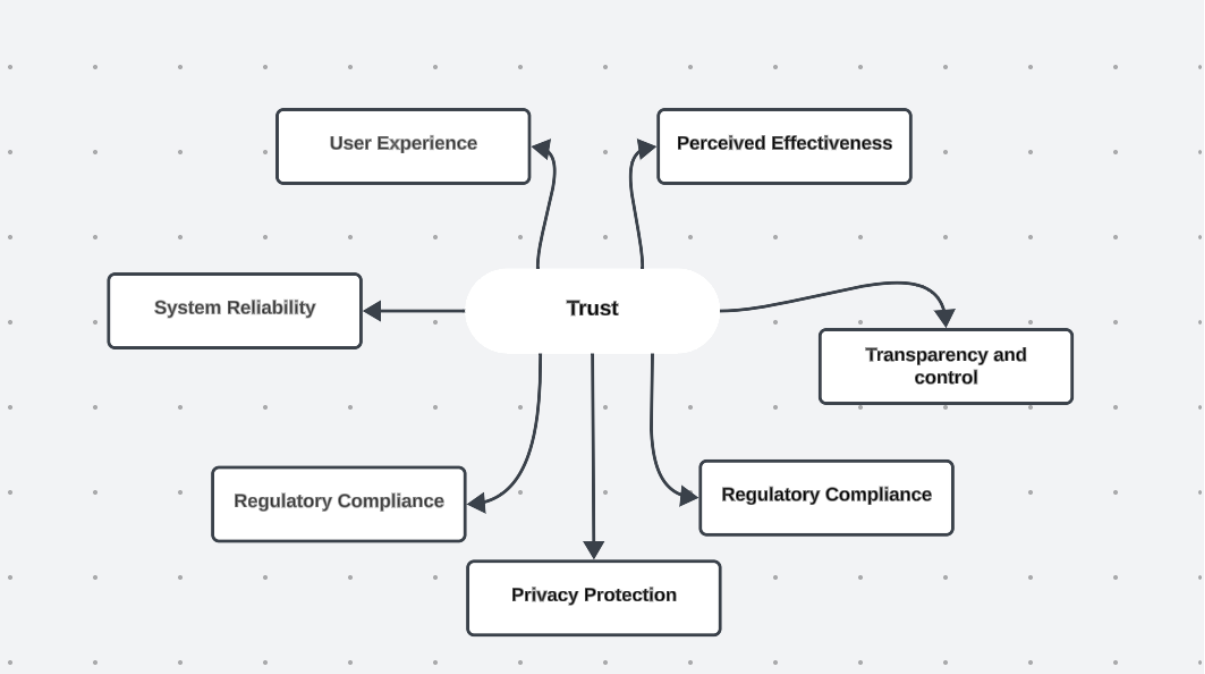
Users' perception of the effectiveness of these systems in accurately verifying identities, as highlighted by Normalini & Ramayah (2017), is foundational. Additionally, the perceived security against fraud and unauthorized access, emphasized by Khan et al. (2023), plays a critical role. User experience, including factors like ease of use and integration into daily routines, has been shown by Trivedi (2019) to significantly influence trust levels. Transparency and control over biometric data, as discussed by Solano et al. (2021), are crucial for user confidence. Privacy protection measures, as advocated by Baig (2023), are essential in mitigating concerns about data misuse. Furthermore, the reliability of biometric systems across different conditions, as studied by Shi et al. (2023), contributes to building trust. Finally, regulatory compliance with legal standards, as addressed by Garcia et al. (2022), reinforces trust among users and stakeholders. These factors collectively shape user perceptions and attitudes towards biometric authentication systems, underscoring their importance in fostering trustworthiness and widespread adoption.

**Thematic Overview**

The thematic analysis of both conceptual and empirical research revealed several key themes that address the research question: "What factors influence user acceptance and trust in the security of biometric authentication systems?"

1. **Trust in Biometric Authentication Systems:** Both research types emphasize the importance of trust, with empirical evidence showing that robust security measures and intuitive interfaces significantly enhance user trust.
2. **Diversity and Innovations of Biometric Authentication Systems:** Continuous technological advancements and innovative solutions are crucial for maintaining user trust and acceptance. Conceptual research explores potential future directions, while empirical studies validate these innovations in real-world scenarios.
3. **User Conditioning:** The emphasis on user-centred design and convenience is common across both conceptual and empirical research. Positive user experiences are vital for widespread acceptance.
4. **Technological Advancements:** Both research types highlight the role of emerging technologies in shaping biometric systems. Empirical studies provide practical insights into the effectiveness of these technologies.
5. **Data Security in Behavioural Authentication:** Protecting biometric data through robust security measures and transparent privacy policies is essential for user trust. Both conceptual and empirical research underscore the importance of addressing ethical considerations.
6. **Personalization Strategies in Biometric Authentication Systems:** Personalized authentication processes can positively impact user behaviour and attitudes. Empirical studies show that tailored approaches enhance user acceptance.

*Figure 2: Trust Factors in Behavioural Biometrics*


User Experience
Perceived Effectiveness
System Reliability
Trust
Transparency and control
Regulatory Compliance
Regulatory Compliance
Privacy Protection

# Chapter 5: Discussion

## 5.1 Interpretation of findings

Based on the comprehensive review of biometric authentication systems across various industries and applications, several key findings emerge. First, biometric technologies are increasingly recognized for their pivotal role in enhancing security measures while improving user experience and operational efficiency. Studies consistently highlight the effectiveness of biometric modalities, such as physiological and BB, in providing robust authentication solutions that mitigate traditional vulnerabilities like password breaches and unauthorized access attempts (Escobar et al., 2021; Almohamade et al., 2021; Shanakraiah, 2022).

Moreover, the integration of biometric systems in diverse sectors—from healthcare to mobile technology—underscores their versatility and transformative impact. For instance, in healthcare, biometric authentication facilitates secure access to electronic health records (EHRs) and enhances patient data protection, addressing critical security concerns in telehealth and medical device applications (Alexandrou & Chen, 2022; Hazratifard, 2022). Similarly, in mobile technology, continuous authentication methods utilizing deep learning algorithms and smartphone sensors demonstrate exceptional accuracy and usability, setting new benchmarks for mobile security standards (Gattuli et al., 2023; Shende et al., 2024).

However, the findings also reveal significant challenges, particularly concerning ethics and sustainability. The near absence of ethical considerations and sustainability frameworks in biometric technology deployment poses risks to privacy and societal trust (Gralha et al., 2020; Nasser et al., 2022). Addressing these gaps is crucial for ensuring responsible implementation and long-term viability of biometric systems across industries.

### Interdisciplinary Integration

The study by E. Kadena, L. C. R. Salvador, and Z. Rajnai (2022) suggests that biometric authentication systems could greatly benefit from interdisciplinary integration. Collaborations across fields such as psychology, sociology, and law could provide a comprehensive understanding of user behaviour, societal trust, and privacy regulations. For example, psychologists could shed light on how users react to biometric systems, while legal scholars could evaluate the implications for privacy laws. By incorporating these interdisciplinary perspectives, biometric technologies could be designed with a broader awareness of human and societal impacts, ensuring they are not only secure but also aligned with ethical and social norms.

### Public Health and Safety Preparedness

Despite significant investments in electronic medical record systems, a notable gap persists between usual and evidence-based clinical practice, leading to inefficiencies and high costs in healthcare. Clinical decision support tools are crucial for translating evidence-based recommendations into practice, yet poor provider adoption often limits their effectiveness. Addressing provider attitudes and fostering adoption are essential for implementing these tools successfully. Biometric authentication systems could play a pivotal role in public health and safety, particularly in pandemic preparedness, by ensuring secure access to sensitive areas like hospitals and laboratories while minimizing physical contact. In healthcare settings, biometrics could effectively track and verify the identities of patients and providers and manage the distribution of vaccines and medical supplies, thereby reducing fraud and ensuring accountability. The recent global health crises have highlighted the need for

touchless solutions, and biometric authentication offers a way to manage access in high-security areas without physical interaction, thus mitigating the spread of pathogens. Sean M. et al (2019)

**Globalization and International Relations**

The widespread adoption of biometric authentication systems has significant implications for globalization and international relations. These technologies can enhance cross-border collaboration by facilitating secure identification in international travel, immigration, and trade. For example, biometric passports and identity verification systems could streamline border crossings, ensuring more efficient and secure travel. In addition, global cooperation on security issues, such as shared biometric databases, could aid in combating international crime and terrorism. However, differences in privacy laws and regulations across regions may require harmonization to fully realize the potential of biometric technologies on a global scale. E. Kadena et al (2022)

**Education and Workforce Reskilling**

The findings underscore the need for education and workforce development as biometric systems become more integrated into various industries. Educational institutions will need to incorporate training programs to equip the next generation with the skills required to develop, implement, and maintain these systems. Additionally, there will be a need for workforce reskilling, particularly for those in industries that are increasingly reliant on biometric technologies. Employees may need to transition into roles that involve overseeing biometric systems, while those displaced by automation might require new skills in adjacent fields. Investment in reskilling programs will be essential to ensure that the workforce adapts to the rapid adoption of these technologies. Naaz et al. (2022)

**User-Centred Design and Accessibility for Special Needs**

Biometric authentication systems must evolve to address the needs of all users, including individuals with special needs. Ensuring accessibility is crucial for creating inclusive systems that everyone can use effectively. For example, biometric systems relying on visual input may exclude visually impaired individuals, while those dependent on fingerprint or voice recognition might not work for users with physical disabilities. Future research should explore how biometric systems can be designed with accessibility in mind, offering alternative modalities or adaptive technologies that cater to a wide range of users. User-centred design principles should prioritize ease of use, minimizing error rates, and enhancing user confidence, ensuring that these systems are both secure and inclusive. Segal et al. (2022) and Garcia et al. (2022)

**Economic and Market Development**

The findings have notable economic implications, particularly for industries that rely on biometric authentication to reduce operational costs and prevent fraud. The financial sector, for example, could benefit significantly from the enhanced security that biometric systems offer, reducing instances of identity theft and fraud. However, the initial cost of implementing biometric systems may be prohibitive for smaller businesses, creating potential market gaps. This could lead to the development of new business models, such as biometric authentication services offered on a subscription basis, allowing smaller businesses to access these technologies without the high upfront costs. As the market for biometric solutions grows, businesses will need to navigate both the benefits and the challenges of widespread implementation. Trivedi (2019).

**Security Evolution and Resilience to Emerging Threats**

As biometric systems continue to evolve, they must be resilient against emerging security threats. Biometric authentication systems face the risk of sophisticated attacks, such as biometric spoofing and deepfakes, which can compromise their effectiveness. Future systems will need to incorporate advanced technologies, such as behavioural analytics or contextual data, to strengthen security. For example, combining biometrics with real-time user behaviour analysis could create hybrid authentication methods that are more difficult to bypass. Additionally, as new threats emerge, biometric systems will need to evolve quickly to stay ahead of attackers, incorporating machine learning and artificial intelligence to detect and respond to potential breaches in real-time. This ongoing evolution will be essential for maintaining trust and security in biometric authentication systems. Umoren et al. (2022)

**Influence on Practice**

The findings suggest several strategies for organizations to effectively implement biometric authentication systems. Healthcare providers, for example, can enhance patient identity verification through the adoption of biometric systems, while simultaneously addressing challenges such as provider resistance. This could involve creating tailored training programs that not only teach staff about the technical aspects of these systems but also emphasize the ethical considerations surrounding user privacy and data protection. Additionally, organizations can establish best practices for integrating biometric systems into existing workflows, ensuring that they enhance efficiency without disrupting established processes. Hazratifard (2022)

**Policy Implications**

The research findings also have significant implications for policy development. Policymakers should consider establishing regulatory frameworks that balance the need for security with the protection of individual privacy rights. This could involve advocating for standardized policies that govern the collection, storage, and usage of biometric data, ensuring that user information is adequately safeguarded while promoting innovation in biometric technologies. Furthermore, the findings highlight the necessity for international cooperation in harmonizing privacy laws related to biometric data. This approach would facilitate smoother cross-border collaboration and enhance the effectiveness of biometric systems in addressing global security challenges. S. Eskeland (2021)

By addressing these additional areas, the research findings can have a far-reaching impact on various sectors, encouraging responsible, secure, and accessible use of biometric authentication systems across different industries and contexts.

## 5.2 Comparison with previous research

The comparison between the new findings on biometric authentication systems and prior research addresses the research question of how trust is cultivated in these technologies. The studies highlight the pivotal role of biometric technologies in enhancing security measures and user experience across various sectors, while also exploring the factors that influence trust. The emphasis is that trust in biometric systems is cultivated through effective integration into user workflows, transparent communication about security measures, and that they demonstrable reliability in authentication processes. Furthermore, the findings identify the importance of ethical considerations and sustainability frameworks in building and maintaining trust, advocating for responsible practices that safeguard user privacy and ensure societal acceptance. Theoretical perspectives from the studies expand upon how continuous authentication models and multimodal biometric systems contribute to trust by offering

enhanced security and usability, thereby shaping future advancements in digital identity management. Practical implications showed the necessity for interdisciplinary collaboration and strategic planning to successfully implement biometric systems while addressing complex challenges and fostering widespread trust among users and stakeholders alike.

## 5.3 Theoretical implications

Theoretical research into biometric authentication systems across diverse industries yields profound implications. It illuminates the evolution of security paradigms, shifting from traditional methods to advanced biometric technologies. The integration of physiological and BB in sectors like banking, healthcare, and IT challenges existing theories on user authentication and security, expanding frameworks to include continuous authentication models and biometric usability's impact on trust and acceptance. Multimodal biometric systems suggest integrated security solutions, prompting theoretical explorations into the intersection of privacy, usability, and effectiveness in digital authentication.

Theoretical implications for biometric authentication systems are critical. Robust frameworks spanning psychology, sociology, and computer science guide system design, implementation, and evaluation across industries. Ethically, the research emphasizes privacy, consent, and data protection, advocating for ethical guidelines on biometric data usage. A user-centric approach prioritizes usability and user experience, enhancing system effectiveness. Security advances in cryptography and protocols are essential for building user trust, while technological innovations like advanced algorithms improve system reliability. Theoretical perspectives also address societal and legal frameworks, balancing technological progress with safeguarding user rights and ensuring societal acceptance. Overall, these implications highlight biometric authentication research's interdisciplinary nature and its role in advancing technology while addressing complex challenges.

## 5.4 Practical implications

The practical implications of research on biometric authentication systems are extensive and impactful. They highlight the need for practical implementation strategies that integrate user-centred design principles, ensuring systems are intuitive and foster widespread acceptance. Emphasizing data security and privacy, the research highlights the necessity for robust encryption protocols and transparent data management practices to build user trust. Technological advancements advocate for adopting cutting-edge algorithms to enhance system reliability and performance. From a governance standpoint, adherence to regulatory standards and ethical frameworks is crucial to mitigate legal risks and promote responsible innovation. Overall, interdisciplinary collaboration and strategic planning are essential for successfully implementing biometric systems across sectors, enhancing security and user experience while shaping the future of digital identity management.

# Chapter 6: Conclusion

## 6.1 Summary of key findings

The research findings of biometric authentication systems reveal several key findings across diverse industries. Biometric technologies, encompassing physiological and behavioural modalities, are pivotal for enhancing security, improving user experience, and optimizing operational efficiency. They effectively mitigate traditional vulnerabilities such as password breaches and unauthorized access attempts. These technologies are versatile, securing sensitive data in sectors like healthcare and supporting applications in mobile technology and telehealth.

Trust in biometric authentication systems hinges on several key factors identified through the research. Users' perception of the effectiveness of these systems in accurately verifying identities is foundational. Additionally, the perceived security against fraud and unauthorized access plays a critical role. User experience, including factors like ease of use and integration into daily routines, significantly influences trust levels. Transparency and control over biometric data are crucial for user confidence. Privacy protection measures are essential in mitigating concerns about data misuse. Furthermore, the reliability of biometric systems across different conditions contributes to building trust. Finally, regulatory compliance with legal standards reinforces trust among users and stakeholders. These factors collectively shape user perceptions and attitudes towards biometric authentication systems, emphasizing their importance in fostering trustworthiness and widespread adoption.

Practically, integrating user-centred design principles is crucial for intuitive and widely accepted biometric systems. Emphasizing data security, robust encryption, and transparent data management practices builds user trust. Technological advancements enhance system reliability, while regulatory compliance mitigates legal risks.

Theoretically, the shift to biometric technologies challenges existing security paradigms and expands theoretical frameworks, particularly in sectors like banking, healthcare, and IT. Multimodal biometric systems offer integrated security solutions, prompting insights into privacy, usability, and effectiveness in digital authentication.

In conclusion, interdisciplinary collaboration and strategic planning are essential for effective implementation of biometric systems. These systems not only enhance security and operational efficiencies but also shape future digital identity management practices, emphasizing ethical considerations and regulatory compliance in technological innovation."

## 6.2 Contributions to knowledge

The analysis of existing literature underscores the paramount importance of ethical considerations, particularly in the realms of sustainability and responsible data management, within the context of biometric authentication systems. Despite the sparse attention given to these themes in the current discourse, it becomes increasingly apparent that addressing ethical concerns is fundamental for nurturing trust among users and ensuring the enduring viability of biometric systems. Key to achieving this is the prioritization of ethical practices, ranging from the collection and utilization of data to its storage and disposal, all of which

necessitate robust policies and regulations to uphold user confidence and sustain the integrity of biometric systems.

In terms of contributions to knowledge, this dissertation brings to light the disparity between the ongoing discussions surrounding biometric authentication systems and the pressing need for ethical and sustainable practices within this domain. By identifying this gap, the research underscores the imperative for academia, policymakers, and industry stakeholders to place ethical considerations at the forefront of system design, implementation, and regulation.

Moreover, the dissertation offers insights into the potential ramifications of neglecting ethical and sustainable practices in the context of biometric authentication. It underscores the inherent risks associated with privacy breaches, data misuse, and societal distrust, all of which pose significant threats to the efficacy and acceptance of biometric technologies.

To address these challenges comprehensively, the research proposes a multifaceted approach encompassing policy development, regulatory frameworks, adherence to industry standards, and proactive user education initiatives. Through advocacy for ethical data management practices and the integration of sustainability principles, the dissertation aims to contribute to the cultivation of a more responsible and trustworthy biometric authentication ecosystem.

Overall, the dissertation's significant contribution to knowledge lies in its staunch advocacy for ethical considerations and sustainability principles within biometric authentication systems. By highlighting the critical importance of aligning technological advancements with ethical imperatives, it seeks to ensure the responsible and sustainable utilization of biometric technologies in the digital age.

Additionally, the dissertation delves into the practical implications of ethical considerations, sustainability, and responsible data management within biometric authentication systems. Despite limited references in the literature, the analysis emphasizes the indispensability of these factors for fostering user trust and maintaining the long-term viability of biometric systems.

**Ethical Considerations**

*User Trust and Confidence:* Foundational to fostering trust and confidence among users are ethical data collection, usage, and storage practices. Operating biometric systems ethically enhances transparency and accountability, essential elements for user acceptance and adoption.

*Privacy Protection:* Central to ethical considerations is protecting user privacy through policies prioritizing privacy-preserving measures such as data anonymization, encryption, and consent-based data sharing. These measures safeguard user rights and interests.

*Fairness and Equity:* Ethical data management promotes fairness and equity within biometric authentication systems. Ensuring equal access and treatment for all users, irrespective of demographic or socio-economic factors, is vital for building trust and maintaining public confidence.

**Sustainability**

*Environmental Impact:* Sustainable practices in biometric systems mitigate environmental impact. This includes energy-efficient algorithms, responsible sourcing of materials, and reducing electronic waste to lessen the carbon footprint of biometric technologies.

*Long-Term Viability*: Ethical and sustainable practices contribute to the long-term viability of biometric systems. Addressing environmental concerns and societal expectations for corporate responsibility enhances resilience and ensures continued relevance.

**Responsible Data Management**

*Data Security and Integrity:* Fundamental to responsible data management are robust encryption, access controls, and data governance frameworks to protect against unauthorized access, breaches, and misuse.

*Compliance with Regulations:* Adhering to regulations and standards for data management is essential for legal compliance and maintaining user trust. Organizations must stay updated on evolving legal requirements and industry best practices.

**Policy and Regulatory Implications**

*Development of Ethical Guidelines:* Policymakers and regulatory bodies are pivotal in developing and enforcing ethical guidelines for biometric authentication systems. Clear policies prioritizing user privacy, fairness, and sustainability provide a framework for responsible system development.

*Enforcement Mechanisms*: Effective enforcement mechanisms, including regular audits and oversight bodies, are necessary to ensure compliance with ethical and sustainability standards. These mechanisms hold organizations accountable and maintain public trust.

*Stakeholder Collaboration:* Collaboration across stakeholders facilitates the development of holistic approaches to ethical and sustainable biometric authentication. Multi-stakeholder dialogues aid in consensus-building and effective regulatory frameworks.

**Future Research Directions**

To address the limitations identified in this study, future research should consider several key directions:

*Empirical Studies in Real-World Settings*: Conduct empirical research that validates the identified factors influencing user acceptance and trust in biometric systems within real-world contexts. These studies should encompass various sectors, such as banking, healthcare, and education, to capture a broader spectrum of experiences and challenges.

*Diverse User Groups and Cross-Cultural Studies*: Future research should involve diverse user demographics and incorporate cross-cultural perspectives. This approach will help elucidate how cultural differences impact the trust and acceptance of biometric authentication technologies, facilitating the development of more tailored solutions.

*Longitudinal Studies*: Implement longitudinal studies to track the evolution of user trust over time. These studies can provide insights into how user conditioning, technological advancements, and ethical considerations affect trust. By examining trends over an extended period, researchers can better understand how external factors—such as data breaches and policy changes—impact user confidence.

*Ethical and Privacy Considerations*: As biometric technologies gain prominence; studies should delve into user perceptions of privacy and the effectiveness of consent mechanisms. Research should explore the ethical implications of biometric data use in surveillance and law enforcement. Further research is needed to develop comprehensive ethical frameworks for biometric authentication systems, addressing complex ethical considerations and evaluating

existing regulations. Proposing new frameworks will be essential to tackle emerging ethical challenges.

*Sustainability Metrics:* Future studies should establish standardized metrics for assessing the environmental impact of biometric technologies. These metrics are crucial for measuring and improving sustainability performance in the deployment of biometric systems.

*Assessment of Regulatory Impact*: Investigate how regulatory and policy changes influence user trust in biometric systems. Comparative studies across regions with varying regulatory environments can reveal insights into the effectiveness of policy measures in fostering user confidence. Additionally, examining the role of industry standards and certifications in assuring users of system security and reliability is necessary.

*Impact Assessments*: Conducting impact assessments to evaluate the ethical, environmental, and social implications of biometric systems is critical for informed policy decisions and industry practices. These assessments can inform the development of responsible data management practices.

In conclusion, ethical considerations, sustainability, and responsible data management are integral to building and maintaining user trust in biometric authentication systems. Prioritizing ethical practices enhances transparency, accountability, and user confidence. Collaboration among policymakers, regulatory bodies, and industry stakeholders is essential for developing and enforcing ethical guidelines. By focusing on these comprehensive frameworks, standardized metrics, and informed impact assessments, future research can advance the development of ethical and sustainable biometric authentication systems, ultimately fostering a safer and more trustworthy digital environment.

### 6.3 Limitations and future research directions

Despite the valuable insights gained from this study and the comparison with prior research, several limitations must be acknowledged. Firstly, the review's scope was confined to existing literature, potentially missing emerging trends and developments in biometric authentication. For instance, advancements in multimodal biometrics—which combine various biometric inputs, such as facial recognition and fingerprint scanning—may not be fully represented in all the reviewed studies. Similarly, newly developed authentication methods that leverage BB, such as keystroke dynamics or gait analysis, might also be overlooked across the studies.

Additionally, the generalizability of findings may be constrained by the specific contexts and methodologies of included studies, often conducted in controlled environments rather than real-world scenarios. For example, many studies rely on laboratory settings where participants may behave differently than they would in actual usage situations, such as banking transactions or healthcare access, where urgency and stress levels can influence user interactions with biometric systems. This limitation could lead to a lack of representation of recent innovations and challenges, such as how biometric systems perform in diverse environmental conditions or across different demographic groups, including age, socioeconomic status, and cultural background.

Several other factors may further limit the comprehensiveness of the review. Access to studies may be restricted by paywalls, preventing researchers from accessing relevant literature that could provide valuable insights into biometric authentication. Additionally, some important research might not have been considered due to being region-locked, focusing only on specific geographical areas while ignoring the diverse challenges and opportunities present in other regions. Similarly, language barriers can restrict access to significant studies published in

languages other than English, leading to a skewed understanding of global trends in biometric technologies.

There is also a concern regarding grey literature bias, where unpublished or non-peer-reviewed studies might provide alternative insights but are often overlooked. Furthermore, research funded by private companies may present a bias toward positive outcomes, potentially downplaying negative aspects of biometric systems to promote their products. This bias can influence the objectivity of findings and limit a comprehensive understanding of the user acceptance and trust issues surrounding biometric authentication.

Moreover, existing studies may not adequately account for the integration of biometric technologies with other security measures, such as two-factor authentication or encryption protocols, which can significantly affect user acceptance and trust. The lack of longitudinal studies assessing the long-term effects of user familiarity and changing societal attitudes toward privacy and security could further limit the insights gained from this research.

## 6.4 Conclusion

In the intricate landscape of biometric authentication systems, trust emerges as the cornerstone upon which user acceptance and adoption hinge. Users, rightfully so, demand assurance that their biometric data will be handled with the utmost care, securely stored, processed, and utilized while preserving their privacy and confidentiality. This trust, however, is not bestowed lightly but is rather a delicate interplay of multifaceted factors. It is nurtured by the unwavering reliability and accuracy of the technology, bolstered by the transparency of system operations, and fortified by robust security measures crafted to safeguard sensitive data. Yet, beyond the technical realm, trust finds its roots intertwined with the ethical fabric of the system, where fairness and ethicality are paramount. Users seek alignment between the system's objectives and their own values and expectations, yearning for a symbiotic relationship founded on principles of integrity and accountability.

At its core, trust in biometric authentication systems reflects ethical considerations meticulously woven into their fabric. Data privacy becomes not just a checkbox to mark but a fundamental principle guiding every interaction, every decision made within the system. Consent emerges not as a mere formality but as a sacred pact between user and system, a cornerstone of mutual respect and understanding. Accountability, likewise, ceases to be an afterthought but becomes the bedrock upon which trust is built, fostering a culture of responsibility and transparency.

Moreover, sustainability emerges as an indispensable pillar supporting the edifice of trust. Responsible data management practices, coupled with unwavering compliance with regulatory frameworks, lay the groundwork for trust to flourish over the long term. In a world where the digital landscape evolves at breakneck speed, sustainability becomes not just an aspiration but a necessity—a commitment to the future generations who will inherit the fruits of our technological endeavours.

By embracing these ethical and sustainable practices, biometric authentication systems can transcend mere functionality, becoming beacons of trust in an increasingly interconnected world. They can bridge the chasm between apprehension and acceptance, between scepticism and embrace, paving the way for widespread adoption and ushering in an era were trust reigns supreme. In this convergence of ethics and technology, lies the promise of a future where biometric authentication systems not only safeguard our identities but also safeguard the very essence of trust itself.

## References


Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioural biometrics. *IEEE Communications Surveys & Tutorials, 18*(3), 1998-2026. https://doi.org/10.1109/COMST.2016.2537748

Angulo, J., & Wästlund, E. (2021). Designing Usable and Secure Biometric Systems. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-13). https://doi.org/10.1145/3411764.3445435

Anwar, S., & Rahman, M. (2018). A Comprehensive Study on Biometric Authentication: Advances, Trends, and Challenges. Future Internet, 10(5), 45. https://doi.org/10.3390/fi10050045

Bhardwaj, I., Londhe, N. D., & Kopparapu, S. K. (2017). A novel behavioural biometric technique for robust user authentication. IETE Technical Review, 34(5), 478-490. https://doi.org/10.1080/02564602.2016.1203271

Bhatti, M. H., Shafqat, M., & Younis, M. S. (2021). A deep learning approach for multimodal biometric authentication. *IEEE Access, 9*, 7386-7397. https://doi.org/10.1109/ACCESS.2021.3049499

Bianchi, T., Piva, A., & Piva, F. (2020). Secure Biometric Authentication: A Comprehensive Overview. Journal of Cryptographic Engineering, 10(2), 107-121. https://doi.org/10.1007/s13389-020-00224-0

Biggio, B., Fumera, G., & Roli, F. (2013). Security Evaluation of Biometric Authentication Systems under Realistic Spoofing Attacks. IEEE Transactions on Information Forensics and Security, 8(3), 451-463. https://doi.org/10.1109/TIFS.2012.2236677

Bojkovic, Z. S., Bakmaz, B. M., & Kocovic, P. (2017). Security issues in biometric systems. In 2017 25th Telecommunications Forum (TELFOR) (pp. 1-4). https://doi.org/10.1109/TELFOR.2017.8249312

Bose, R., & Frew, L. (2005). Health Insurance Portability and Accountability Act (HIPAA) for biomedical researchers. Scientific World Journal, 5, 536-546. https://doi.org/10.1100/tsw.2005.68

Bowyer, K. W., Hollingsworth, K. P., & Flynn, P. J. (2008). A Survey of Iris Biometrics Research: 2008-2010. In 2010 20th International Conference on Pattern Recognition (pp. 912-917). https://doi.org/10.1109/ICPR.2010.223

Brady, G., & Lim, E. (2022). Privacy-preserving biometric authentication. IEEE Security & Privacy, 20(1), 40-47. https://doi.org/10.1109/MSEC.2022.3156931

Camacho, S., & Best-Rowden, L. (2022). Deep learning for multi-biometric authentication: An overview. ACM Computing Surveys, 55(3), 54:1-54:35. https://doi.org/10.1145/3495243

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008

De Marsico, M., Nappi, M., & Wechsler, H. (2018). Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols. Pattern Recognition Letters, 57, 1-6. https://doi.org/10.1016/j.patrec.2014.03.004

Derawi, M. O., Nickel, C., Bours, P., & Busch, C. (2010). Unobtrusive user-authentication on mobile phones using biometric gait recognition. In 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (pp. 306-311). https://doi.org/10.1109/IIH-MSP.2010.147

Diaz-Santana, J. F., Benitez, C., & Lorente, M. (2015). Biometrics and Privacy: On the Relevance of Balancing Security, Privacy and Usability in Biometric Systems. IEEE Security & Privacy, 13(6), 82-85. https://doi.org/10.1109/MSP.2015.138

Dinesha, H. A., & Agrawal, V. K. (2015). Multimodal Biometric System: A Review. International Journal of Computer Applications, 120(2), 15-21. https://doi.org/10.5120/21258-4052

Dunn, J. (2021). Biometric Authentication Using ECG Signals: A Survey. IEEE Access, 9, 116303-116320. https://doi.org/10.1109/ACCESS.2021.3105006

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioural Biometrics for Continuous Authentication: Challenges and Metrics. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 386-399). https://doi.org/10.1145/3133956.3134049

Eshratifar, A. E., & Pedram, M. (2018). IoT Device Fingerprinting Using Deep Learning. In 2018 IEEE 39th Sarnoff Symposium (pp. 1-6). https://doi.org/10.1109/SARNOF.2018.8421402

Fairhurst, M., Li, C., & Da Costa-Abreu, M. (2017, July 13). Predictive biometrics: A review and analysis of predicting personal characteristics from biometric data. IET Biometrics. https://doi.org/10.1049/iet-bmt.2016.0169Faundez-Zanuy, M., & Elizondo, D. (2019). Human activity recognition for mobile biometrics. Applied Sciences, 9(21), 4628. https://doi.org/10.3390/app9214628

Giesing, I. (2003). User perceptions related to identification through biometrics within electronic business (master's dissertation). University of Pretoria, Pretoria. Retrieved from http://hdl.handle.net/2263/29139

Gimpel, J., & Winkler, S. (2019). Privacy-Preserving Biometric Authentication: Techniques and Challenges. IEEE Security & Privacy, 17(5), 74-81. https://doi.org/10.1109/MSEC.2019.2922693

Grosz, B., & Klein, D. (2016). Improving the Usability of Biometric Authentication. In 2016 IEEE Symposium on Security and Privacy (pp. 1-12). https://doi.org/10.1109/SP.2016.45

Gupta, P., & Garg, D. (2020). Privacy-Preserving Biometric Authentication in Cloud Computing Environment: A Comprehensive Survey. IEEE Access, 8, 72819-72835. https://doi.org/10.1109/ACCESS.2020.2985647

Hildebrandt, M., & Gutwirth, S. (Eds.). (2008). Profiling the European Citizen: Cross-Disciplinary Perspectives. In S. van der Hof & C. Prins (Eds.), Chapter 6: Personalisation and its Influence on Identities, Behaviour and Social Values (p. 134). Springer Science + Business Media B.V. Link

Jain, A. K., Deb, D., & Engelsma, J. J. (2022, July). Biometrics: Trust But Verify. IEEE Transactions on Biometrics, Behaviour, and Identity Science, 4(3), 303-323. https://doi.org/10.1109/TBIOM.2021.3115465

Jain, A. K., Flynn, P., & Ross, A. A. (2008). Handbook of Biometrics. Springer Science & Business Media. https://doi.org/10.1007/978-0-387-71041-9

Jain, S., & Rathod, V. (2021). Biometric Authentication Using Electromyography Signals: A Comprehensive Review. Sensors, 21(4), 1128. https://doi.org/10.3390/s21041128

Johnson, P., & Duberley, J. (2000). *Postmodernist epistemology - Relativism unleashed?* In *Understanding management research* SAGE Publications Ltd. https://doi.org/10.4135/9780857020185

Kanawattanachai, P., & Yoo, Y. (2002). Dynamic nature of trust in virtual teams. The Journal of Strategic Information Systems, 11(3–4), 187-213. https://doi.org/10.1016/S0963-8687(02)00019-7

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. Technical Report, EBSE 2007-001. Software Engineering Group, School of Computer Science and Mathematics, Keele University.

Lai, K., Oliveira, H. C. R., Hou, M., Yanushkevich, S. N., & Shmerko, V. P. (2020). Risk, trust, and bias: Causal regulators of biometric-enabled decision support. IEEE Access, 8, 148779-148792. https://doi.org/10.1109/ACCESS.2020.3015855

Li, C., & Jain, A. K. (2009). Moorish et al.: Exploring Age, Gender, and Ethnicity Factors in Fingerprint Recognition. IEEE Transactions on Information Forensics and Security, 5(3), 420-432. https://doi.org/10.1109/TIFS.2010.2049715

Li, Y., & Chen, Z. (2022). A survey of multimodal biometric authentication: Challenges and trends. Information Fusion, 79, 88-108. https://doi.org/10.1016/j.inffus.2021.08.011

Li, Z., Zhang, L., & Zhao, H. (2021). Secure and Efficient Multi-Factor Authentication Scheme Using Biometrics in Cloud Computing. IEEE Transactions on Cloud Computing. Advance online publication. https://doi.org/10.1109/TCC.2021.3097568

Lockwood, C., Munn, Z., & Porritt, K. (2015). Qualitative research synthesis: methodological guidance for systematic reviewers utilizing meta-aggregation. Int J Evid Based Healthc, 13(3), 179–187

Lu, X., & Jain, A. K. (2005). Integrating Range and Texture Information for 3D Face Recognition. In Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05) - Volume 1 (pp. 156-163). https://doi.org/10.1109/ACV.2005.48

Mahmood, S., & Tyrer, B. (2017). A Study on the Security of Biometric Authentication in Cloud Computing. Journal of Cloud Computing, 6(1), 1-16. https://doi.org/10.1186/s13677-017-0094-0

Malik, M. I., & Khan, A. (2020). Biometric Recognition: A Modern Era of Forensic Science. In Forensic Science and Humanitarian Action (pp. 157-174). Elsevier. https://doi.org/10.1016/B978-0-12-815395-1.00009-5

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

Morandi, C., & Pari, P. (2018). Biometric authentication and IoT: Trends, challenges, and future directions. Future Internet, 10(8), 64. https://doi.org/10.3390/fi10080064

Moustafa, N., & Slay, J. (2013). Biometric Authentication System for the Internet of Things Using Mobile Devices. IEEE Transactions on Consumer Electronics, 59(4), 664-671. https://doi.org/10.1109/TCE.2013.6689683

Nambisan, S., Agarwal, R., & Tanniru, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. MIS Quarterly, 23(3), 365–395. https://doi.org/10.2307/249468

Nguyen, H. T., & Jain, A. K. (2021). Synthetic Fingerprint Generation: Survey, Analysis, and Evaluation. IEEE Transactions on Pattern Analysis and Machine Intelligence. Advance online publication. https://doi.org/10.1109/TPAMI.2021.3074528

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Sprouts: Working Papers on Information Systems, 10(26). Retrieved from http://sprouts.aisnet.org/10-26

Olade, T., Subramanian, R., & Ratha, N. (2018). A Comprehensive Survey on Biometric Template Protection. ACM Computing Surveys, 51(3), 57:1-57:36. https://doi.org/10.1145/3177850

Oloyede, M. O., & Hancke, G. P. (2016). Unimodal and multimodal biometric sensing systems: A review. IEEE Access, 4, 7532-7555. https://doi.org/10.1109/ACCESS.2016.2628162

Oteng, P. A., & Lai, R. (2016). Evaluating the Usability of Biometric Authentication on Mobile Devices. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (pp. 1279-1284). https://doi.org/10.1145/2968219.2971441

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., & Flynn, P. J. (2013). The Human Identification at a Distance (HID) Challenge. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(5), 585-593. https://doi.org/10.1109/TPAMI.2003.1190577

Raja, K. B., & Rathgeb, C. (2015). Multi-modal face and ear biometrics fusion in image domain. Pattern Recognition Letters, 36, 92-100. https://doi.org/10.1016/j.patrec.2014.09.005

Rankin, A., & Locke, A. (2016). A study of the challenges and security measures of biometric authentication in mobile devices. Journal of Information Security and Applications, 26, 35-45. https://doi.org/10.1016/j.jisa.2015.11.004

Rathgeb, C., Uhl, A., & Busch, C. (2011). On the application of hill-climbing attacks to iris biometrics. IET Biometrics, 1(1), 19-27. https://doi.org/10.1049/iet-bmt.2011.0003

Sasse, M. A., & Brostoff, S. (2001). Evaluating the Usability of a Biometric Authentication System. In Proceedings of the 2001 CHI Conference on Human Factors in Computing Systems (pp. 89-94). https://doi.org/10.1145/365024.365047

Schmidt, H., & Uellenbeck, S. (2017). Exploring the Performance of Behavioural Biometrics for Continuous Authentication. In 2017 IEEE International Conference on Identity, Security and Behaviour Analysis (ISBA) (pp. 1-8). https://doi.org/10.1109/ISBA.2017.7947694

Singh, R., Vatsa, M., & Noore, A. (2005). Biometric Classifiers: Are They Secure? In Proceedings of the 2005 IEEE International Conference on Electro Information Technology (pp. 1-5). https://doi.org/10.1109/EIT.2005.1627001

Tankard, C. (2012). Cultural issues in security and privacy. Network Security, 2012(11), 5-8. https://doi.org/10.1016/S1353-4858(12)70102-2

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews in information systems research. MIS Quarterly, 39(3), 541-564. https://doi.org/10.25300/MISQ/2015/39.3.02

Tondi, B., Bertolazzi, P., de Carvalho, A. C. P. L. F., Spolaôr, N., & Lambert-Torres, G. (2019). A Framework for Sensor-Based Healthcare Monitoring in the Context of IoT: Particularities and Challenges. Sensors, 19(5), 1050. https://doi.org/10.3390/s19051050

Turgeman, A., & Zelazny, F. (2017). Invisible challenges: The next step in behavioural biometrics? Biometric Technology Today, 2017(6), 5-7. https://doi.org/10.1016/S0969-4765(17)30114-5

Tyagi, A., & Singh, S. (2020). Robust biometric watermarking technique based on singular value decomposition and quaternion wavelet transform. Multimedia Tools and Applications, 79(29-30), 21133–21156. https://doi.org/10.1007/s11042-020-09139-2

Vasconcelos, A., Santos, G., & Kofuji, S. T. (2023). Forensic investigation using Multimodal Biometrics and Machine Learning techniques. Journal of Forensic Sciences & Criminal Investigation, 23(1), 555979. https://doi.org/10.19080/JFSCI.2023.23.555979

Verma, A., Moghaddam, V., & Anwar, A. (2022). Data-Driven Behavioural Biometrics for Continuous and Adaptive User Verification Using Smartphone and Smartwatch. Sustainability, 14, 7362. https://doi.org/10.3390/su14127362

Virdi, A., & De Mola, R. (2021). Advances in Biometric Authentication and Privacy Protection. In Proceedings of the 2021 International Conference on Security, Privacy, and Applied Cryptography Engineering (pp. 1-20). https://doi.org/10.1007/978-3-030-83463-4_1

Wang, Y., & Zhao, Y. (2021). A Secure and Efficient Multimodal Biometric Authentication System Using Quantum Cryptography. Quantum Information Processing, 20(2), 58. https://doi.org/10.1007/s11128-021-03049-5

Wang, Z., & Bhargava, B. (2014). User Authentication on Mobile Devices: Approaches, Threats and Solutions. In 2014 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 1-8). https://doi.org/10.1109/TrustCom.2014.9

Wayman, J. L. (2001). Fundamentals of biometric authentication technologies. International Journal of Image and Graphics, 1(1), 93-113. https://doi.org/10.1142/S0219467801000063

Wen, F., & Guo, G. (2019). A Comprehensive Review of Computational Intelligence Techniques in Biometric Systems. ACM Computing Surveys, 52(2), 32:1-32:35. https://doi.org/10.1145/3316485

Xiao, L., & Watson, M. (2019). Guidance on conducting a systematic literature review. Journal of Planning Education and Research, 39(1), 93-112. https://doi.org/10.1177/0739456X17723971

Xu, Z., & Wang, X. (2015). Privacy-Preserving Biometric Authentication Systems. ACM Computing Surveys, 47(3), 41:1-41:38. https://doi.org/10.1145/2676890

Yampolskiy, R. V., & Govindaraju, V. (2008). Behavioural biometrics: A survey and classification. International Journal of Biometrics, 1(1), 81-113. https://doi.org/10.1504/IJBM.2008.018665

Yang, H., & Bourlai, T. (2013). Iris recognition in the presence of ocular disease. Image and Vision Computing, 31(3), 250-262. https://doi.org/10.1016/j.imavis.2012.10.003

Yang, Y., & Qu, Y. (2020). Challenges and Countermeasures for Biometric Authentication Systems in the Era of Artificial Intelligence. IEEE Access, 8, 151678-151690. https://doi.org/10.1109/ACCESS.2020.3016260

Yang, Z., & Wang, Y. (2020). A survey of biometric authentication using electroencephalogram signals. Neurocomputing, 410, 70-82. https://doi.org/10.1016/j.neucom.2020.06.013

Yousefnezhad, M., & Arabnia, H. R. (2019). A Survey of Biometric Identification Based on Deep Learning. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 1308-1315). https://doi.org/10.1109/CSCI49370.2019.00243

Zhang, D., & Zhu, H. (2021). A Survey of Biometric Authentication Systems. Computers & Security, 103, 102174. https://doi.org/10.1016/j.cose.2021.102174

Zhang, Z., & Wu, Z. (2015). An Overview of Biometric Authentication. In 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity) (pp. 129-133). https://doi.org/10.1109/SmartCity.2015.53

Zhang, Z., & Xie, S. (2022). A Comprehensive Survey on Multimodal Biometrics Fusion and Recognition. ACM Computing Surveys, 54(3), 51:1-51:30. https://doi.org/10.1145/3415732

Zhang, Z., & Zuo, W. (2016). On the Security of Biometric Authentication Systems. In 2016 IEEE Symposium on Security and Privacy (pp. 399-414). https://doi.org/10.1109/SP.2016.32

Zhou, L., & Jain, A. K. (2021). Advances in Biometric Systems and Privacy Protection. Information Fusion, 79, 88-108. https://doi.org/10.1016/j.inffus.2021.08.011

Ziółkowski, A., & Loba, J. (2017). Biometric-based continuous authentication in mobile devices. Future Generation Computer Systems, 76, 168-176. https://doi.org/10.1016/j.future.2016.06.013

Zhu, Y., & Tang, W. (2020). Secure and Efficient Biometric Authentication Using Homomorphic Encryption. In 2020 IEEE Symposium on Security and Privacy (pp. 121-136). https://doi.org/10.1109/SP40000.2020.00032

Zhu, Y., & Zhang, W. (2022). Privacy-Preserving Biometric Authentication Using Secure Multiparty Computation. In 2022 IEEE Symposium on Security and Privacy (pp. 89-103). https://doi.org/10.1109/SP46215.2022.00089

Zhu, Z., & Yin, Z. (2021). A Survey of Biometric Authentication for Mobile Devices. ACM Computing Surveys, 54(3), 57:1-57:35. https://doi.org/10.1145/3416487

Ziółkowski, K., & Loba, P. (2019). Biometric Authentication and Blockchain Technology: Trends and Future Directions. Sensors, 19(5), 1040. https://doi.org/10.3390/s19051040

Zupan, B., & Donati, E. (2019). A Review of Biometric Authentication Methods for Mobile Devices. In Proceedings of the 2019 ACM Conference on Human Factors in Computing Systems (pp. 1-13). https://doi.org/10.1145/3290605.3300611

## Appendices

### Appendix A: List of Articles used for Literature Review

| DATABASE | TITLE | AUTHOR | YEAR | METHOD | THEMES | NOTES | EMPIRICAL/ CONCEPT | INDUSTRY |
|---|---|---|---|---|---|---|---|---|
| Dimensions | OdorTAM: Technology Acceptance Model for Biometric Authentication System Using Human Body Odor | Sameena Naaz, Sarah Ali Khan, Farheen Siddiqui, Shahab Saquib Sohail, Dag Øivind Madsen, Asad Ahmad | 2022 | Quantitative | Diversity & Innovations in B.A.S, Trust in B.A.S, Data Security in B.A, User Conditioning | Very high-quality article of great applicability to the research question, useful in quantitative nature | Empirical | Biometric Technology |
| Dimensions | Security, Privacy, and Usability in Continuous Authentication: A Survey | Ahmed Fraz Baig, Sigurd Eskeland | 2021 | Qualitative | Diversity & Innovations in B.A.S, User Conditioning, Data Security in B.A | Another high-quality article, however, it is qualitative in nature capturing the human essence | Empirical | Identity Verification |
| Dimensions | Human Micro-Expressions in | Zaman Wahid, A S M Hossai | 2023 | Quantitative | Diversity & Innovations in | very clear methodology | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Multimodal Social Behavioural Biometrics | n Bari, Marina Gavrilova | | | B.A.S, Trust in B.A.S, User Conditioning, Personalisation Strategies in B.A.S | presented, extremely useful to research question for all the wrong reasons. Only one sentence in the 21-page article mentioned user privacy or rather "anonymity" | | |
| Dimensions | Perceived security of BYOD devices in medical institutions | Alex Alexandrou, Li-Chiou Chen | 2022 | Mixed Methods | Trust in B.A.S, Technological Advancements | Highly useful mixed methods rich resource. Will be applicable at all stages of SLR | Empirical | Healthcare |
| Dimensions | Periocular Data Fusion for Age and Gender Classification | Carmen Bisogni, Lucia Cascone, Fabio | 2022 | Quantitative | Diversity & Innovations in B.A.S, Technological Advance | Suitable for potential trust and user recommendat | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Narducci | | | ments, Personalisation Strategies in B.A.S, Data Security in B.A. | ions, groundbreaking research therefore limited in policy. | | |
| Dimensions | Techniques and countermeasures for preventing insider threats | Rakan A. Alsowail, Taher Al-Shehari | 2022 | Qualitative | Diversity & Innovations in B.A.S | useful for building a policy narrative and explaining what types of biometrics exist | Conceptual | Information Security |
| Dimensions | The effects of anthropomorphism and multimodal biometric authentication on the user experience of voice intelligence | Mels de Kloet, Shengyun Yang | 2022 | Quantitative | User Conditioning, Personalisation Strategies in B.A.S, Technological Advancements, Trust in B.A.S | This reference is all about the user's condition. Useful mainly for the second factor/ challenge, somewhat touches trust | Empirical | Identity Verification |
| Dimensions | Digital onboarding in finance: a novel model and related | Miren Karmele García, Eliseo Venegas, SOTER | 2022 | Qualitative | Diversity & Innovations in B.A.S, Personalisation strategie | Minor relevance to paper yet may be used in first factor/ | Conceptual | Information Security |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | cybersecurity risks | , Esther Aguilera, José Manuel Panizo, Charlotte Kelly, Diego Serrano | | | s in B.A.S | challenge. Cyber security solution that addresses Privacy and Transparency risks in finance. | | |
| Dimensions | Supporting schools to use face recognition systems: a continuance intention perspective of elementary school parents in China | Jon-Chao Hong, Yushun Li, Shuo-Ying Kuo, Xin An | 2022 | Quantitative | Trust in B.A.S, User conditioning, Technological Advancements. | The more educated a parent is of Biometric Authentication the more likely they would express an intention to engage with the service. Directly correlates with research question | Empirical | Identity Verification |
| Dimensions | A broad review on non-intrusive active user | Princy Ann Thomas, K. Preetha Mathew | 2021 | Qualitative | Diversity &innovations of B.A.S, Data | would be useful at start of literatur | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | authentication in biometrics | | | | Security in B.A | e review as an overview reference to explain the different types of Biometric authentication methods | | |
| Dimensions | A Review of AI Cloud and Edge Sensors, Methods, and Applications for the Recognition of Emotional, Affective and Physiological States | Arturas Kaklauskas, Ajith Abraham, Ieva Ubarte, Romualdas Kliukas, Vaida Luksaite, Arune Binkyte-Veliene, Ingrida Vetloviene, Loreta Kaklauskiene | 2022 | Quantitative | User conditioning, Technological Advancements | may use AFFECT to build a narrative around the human conditioning in the reliability of Biometric authentication. Absence of trust. | Empirical | Identity Verification |
| Dimensions | Touch events and human activities for continu | Vincenzo Gattulli, Donato Impedovo, Giusep | 2023 | Quantitative | Data security in B.A. | very bare bones resource, however | Empirical | Mobile Technology |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ous authentication via smartphone | pe Pirlo, Francesco Volpe | | | | describes in detail security for smartphones. May use to support a narrative in either the first or third challenge | | |
| Dimensions | Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain | Otuekong Umoren, Raman Singh, Zeeshan Pervez, Keshav Dahal | 2022 | Quantitative | Data Security in B.A., Diversity & Innovations in B.A.S, Technological Advancements. | use for transparency and privacy risks | Conceptual | Identity Verification |
| Dimensions | WoX+: A Meta-Model-Driven Approach to Mine User Habits and Provide Continuous Authentication | Luca Mainetti, Paolo Panarese, Roberto Vergallo | 2022 | Mixed Methods | Trust in B.A.S, Diversity & Innovations of B.A.S, Personalisation strategies in B.A.S | use for trust as the study not just did quantitative analysis of systems, but also interviewed | Empirical | Technology-IOT |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | in the Smart City | | | | | users for their feedback | | |
| Dimensions | Deep Residual Networks for User Authentication via Hand-Object Manipulations | Kanghae Choi, Hokyoung Ryu, Jieun Kim | 2021 | Quantitative | Data Security in B.A. | use in overview to differentiate between implicit and explicit behavioural authentication. Absence of trust, may also be used to address privacy concerns and personalisation. | Empirical | Identity Verification |
| Dimensions | Biometric applications in education | Marcela Hernandez-de-Menendez, Ruben Morales-Menendez, Carlos A. Escobar, Jorge Arinez | 2021 | Lit review | Diversity & innovations of B.A.S, Trust in B.A.S | a conceptual paper, however very strong in its recommendations. A solid general overview of B.A. and | Empirical | Educational |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | may use to support a trust narrative. | | |
| Dimensions | BioTouch: Reliable Re-Authentication via Finger Bio-Capacitance and Touching Behaviour | Chong Zhang, Songfan Li, Yihang Song, Qianhe Meng, Li Lu, Mengshu Hou | 2022 | Quantitative | User Conditioning | may use for user state impact, barely. | Empirical | Identity Verification |
| Dimensions | Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial | Mehdi Hazratifard, Fayez Gebali, Mohammad Mamun | 2022 | Qualitative | Diversity & innovations of B.A.S, Data Security in B.A | use for the first and second challenges | Conceptual | Healthcare |
| Dimensions | Encouraging gender-inclusive acceptance of multipurpose national-identity smart cards | Yuen Yee Yen, P. H. P. Yeow, Loo Wee Hong | 2022 | Quantitative | Trust in B.A.S,, User Conditioning, Technological Advancements. | Directly correlates with research question | Empirical | Public sector |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| EBSCO | Integrating Information Technology and Marketing to increase e-Book consumption | Liao, Hsiu-Li; Liu, Su-Houn | 2023 | Quantitative | Diversity & innovations of B.A.S., Trust in B.A.S, User Conditioning | Directly correlates with research question | Empirical | Publishing, E-Books |
| EBSCO | When Humans Using the IT Artifact Becomes IT Using the Human Artifact. | Demetis, Dionysios S.; Lee, Allen S. | 2018 | Qualitative | Trust In B.A.S., User Conditioning, Technological Advancements | Directly correlates with research question | Conceptual | IT and Data Management |
| EBSCO | Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach. | Breward, Michael; Hassanein, Khaled; Head, Milena | 2017 | Mixed Methods | Trust in B.A.S., User Conditioning, Technological Advancements, Diversity and innovations of B.A.S | Directly correlates with research question | Empirical | Banking and Finance |
| EBSCO | The Critical Role of Health Information Technol | Segal, Mark; Giuffrida, Patricia; Possan | 2022 | Mixed Methods | Personalisation Strategies in B.A.S. | A theoretically heavy reference that may be | Conceptual | Healthcare |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ogy in the Safe Integration of Behavioural Health and Primary Care to Improve Patient Care. | za, Lorraine; Buccifero, David | | | | used support a healthcare narrative in discussion, but ultimately does not address the trust in BB | | |
| EBSCO | Data Leakage Prevention for Secure Cross-Domain Information Exchange. | Kongsgard, Kyrre Wahl; Nordbotten, Nils Agne; Mancini, Federico; Haaseth, Raymond; Engelstad, Paal E. | 2017 | Mixed Methods | Trust in B.A.S., User Conditioning, Technological Advancements, Diversity and innovations of B.A.S, Personalisation strategies in B.A.S | If constructing a policy argument this reference may be used to identify commonalities found in drafting one | Empirical | Information Security |
| EBSCO | Factors Affecting the Accessibility of IT Artifacts: A Systematic Review. | Mäkipää, Juho-Pekka; Norrgård, Johanna; Vartiainen, Tero | 2022 | Qualitative | Trust in B.A.S., Diversity and innovations of B.A.S, , User Conditioning, Personalisation Strategie | An exceptional reference that addresses many critical factors in research questio | Empirical | IT and Data Management |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | s in B.A.S | n, use this. | | |
| EBSCO | Advanced security and privacy in connected vehicles. | Kitayama, Hiroyuki; Muneto h, Seiji; Ohnishi, Katsumi; Uramoto, Naohiko; Watanabe, Yuji. | 2014 | Qualitative | Technological Advancements, User Conditioning, Data Security in B.A., Diversity and innovations of B.A.S | An obscure reference that can be used in a policy narrative | Empirical | Automotive |
| EBSCO | Behavioural Health Information Technology: From Chaos To Clarity. | Ranallo, Piper A.; Kilbourne, Amy M.; Whatley, Angela S.; Pincus, Harold Alan. | 2016 | Qualitative | Trust in B.A.S., Personalisation Strategies in B.A.S, Technological Advancements | Mainly addresses the third challenge | Conceptual | Healthcare |
| EBSCO | Examining the Customer Experience of Using Banking Chatbots and Its Impact on Brand | Trivedi, Jay. | 2019 | Quantitative | Trust in B.A.S.,Technological Advancements, Personalisation Strategies in B.A.S. | Directly correlates with research question | Empirical | Banking and Finance |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Love: The Moderating Role of Perceived Risk. | | | | | | | |
| EBSCO | Leveraging Health Information Technology in the Quest to Improve Health Care Value. | Genies, Marquita C.; Biondi, Eric A.; Berenholtz, Sean M. | 2019 | Qualitative | Personalisation Strategies in B.A.S., Technological Advancements, Trust in B.A.S. | The issues highlighted in key findings may be used to support a narrative where trust in BB is affected by inconsistencies during nascent stages of policy development | Conceptual | Healthcare |
| EBSCO | Using 'Big Data' for analytics and decision support. | Power, Daniel J | 2014 | Qualitative | Technological Advancements, User Conditioning, Data Security in B.A., Trust in B.A.S | user perspective of trust | Conceptual | IT and Data Management |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Google Scholar | Behavioural Biometrics for more (dis) trust and security | E. Kadena, L. C. R. Salvador, Z. Rajnai | 2022 | Qualitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A | Directly correlates with research question | Conceptual | Information Security |
| Google Scholar | Trust and Voice Biometrics Authentication for Internet of Things | Alec Wells, Aminu Bello Usman | 2023 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | Directly correlates with research question, fantastic high value source | Empirical | Technology I.O. T |
| Google Scholar | BioTAM: a technology acceptance model for biometric authentication systems | Kanak, A. and Sogukpinar, I. | 2017 | Qualitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A | Directly correlates with research question | Conceptual | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Google Scholar | Behaviour-Based Biometrics for Continuous User Authentication to Industrial Collaborative Robots | Shurook S. Almohamma, John A. Clark, and James Law | 2021 | Mixed Methods | Data Security in B.A, Technological Advancements, Personalisation Strategies in B.A.S. | does not address trust in BB, however, indicates users perceived risk, and strong policy implications. | Empirical | Robotics |
| Google Scholar | The language of biometrics: Analysing public perceptions | Oliver Buckley a,Jason R.C. Nurse | 2019 | Quantitative | Trust in B.A.S, User Conditioning | Reference highlights general public knowledge of what exactly BB is, this may be used to build a narrative around educating users to build trust in BB | Empirical | Biometric Technology |
| Google Scholar | Energy-efficient multi-biometric system for Internet of | Falmata Modu,Faroq, Aliyu, Tarek Sheltami, | 2021 | Quantitative | Diversity and innovations of B.A.S | Useful for highlighting the robustness of BB, how it can be | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Things using trust manag ement | Mahdi Musa | | | | trusted by users for enhanc ed security | | |
| Google Scholar | Users' Privacy Attitude s towards the Use of Behavi oural Biometr ics Continu ous Authent ication (BBCA) Technol ogies: A Protecti on Motivati on Theory Approa ch | Skalkos A, Stylios I, Karyda M, Kokola kis S | 2021 | Quantitat ive | Trust in B.A.S, Diversity and innovatio ns of B.A.S, Personali sation Strategie s in B.A.S. | Directly addres ses researc h questio n | Empirical | Mobile Technology |
| Google Scholar | Trust in Internet Bankin g in Malaysi a and the Modera ting Influenc e of Perceiv ed Effectiv eness of Biometr | Normali ni M.K, T. Ramay ah | 2017 | Quantitat ive | Trust in B.A.S, Diversity and innovatio ns of B.A.S | Directly addres ses researc h questio n | Empirical | Banking and Finance |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ics Technology on Perceived Privacy and Security | | | | | | | |
| Springer Link | Privacy-preserving continuous authentication using behavioural biometrics | Baig, A.F., Eskeland, S. & Yang, B. | 2023 | Quantitative | Data Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | While not focusing on user's trust, the paper emphasises preventative measures to ensure the privacy of users | Empirical | Information Security |
| Springer Link | Analytical study on users' awareness and acceptability towards adoption of multimodal biometrics (MMB) mechanism in online transactions: a two- | Purohit, H., Dadhich, M. & Ajmera, P.K | 2022 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S | Directly correlates with research question | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | stage SEM-ANN approach | | | | | | | |
| Springer Link | Cryptography and Tay-Grey wolf optimization based multimodal biometrics for effective security | Arora, A., Miri, R. | 2022 | Mixed Methods | Diversity and innovations of B.A.S, Personalisation Strategies in B.A.S. | a technically sound paper, however, does not address trust at all | Conceptual | Biometric Technology |
| Springer Link | Combining behavioural biometrics and session context analytics to enhance risk-based static authentication in web applications | Solano, J., Camacho, L., Correa, A. et al. | 2020 | Qualitative | Trust in B.A.S, Diversity and Technological Advancements, Personalisation Strategies in B.A.S. | A good paper for policy making, yet no focus on user trust or perceptions | Conceptual | Information Security |
| Springer Link | Social behavioural biometric multimodal union to evade | P, S., Shankaraiah | 2022 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data | Paper focuses on explaining HOW algorithms are identifie | Empirical | Social media |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | fake account creation in Facebook | | | | Security in B.A | d, and which ones are most useful in a social media setting, not useful for trust | | |
| Springer Link | Analytical outlook on customer awareness towards biometrics mechanism of unimodal and multimodal in online transactions | Gokulkumari, G. | 2020 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | Directly correlates with research question | Empirical | E-commerce |
| Springer Link | Adversarial attacks against mouse- and keyboard-based biometric authentication: black- | López, C., Solano, J., Rivera, E. et al. | 2023 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S | Can be used to identify how users trust can be challenged if attackers were aware of potenti | Conceptual | Information Security |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | box versus domain-specific techniques | | | | | al security risks in BB systems | | |
| Springer Link | New soft biometrics for limited resource in keystroke dynamics authentication | Chang, TY., Tsai, CJ., Yeh, JY. et al. | 2020 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Personalisation Strategies in B.A.S. | The study aims to educate users in adopting keystroke authentication-in doing so building trust in BB, albeit it is not the KEY focus of this research | Conceptual | Identity Verification |
| Springer Link | Investigating of nodes and personal authentications utilizing multimodal biometrics for medical application of | El-Bendary, M.A.M., Kasban, H., Haggag, A. et al. | 2020 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, | Robust examination of authentication, however null on trust | Conceptual | Healthcare |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | WBANs security | | | | Personalisation Strategies in B.A.S. | | | |
| Springer Link | A novel algorithm to model the neuromuscular system from the eye to fingers to authenticate individuals through a typing process | Kavusi, H., Maghooli, K. & Haghipour, S. | 2022 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining. | A useful reference that may be used to highlight how a user's condition/ state/ fatigue levels may affect the accuracy of BB authentication | Empirical | Biometric Technology |
| Springer Link | Implementation of quaternion mathematics for biometric security | Khallaf, F., El-Shafai, W., El-Rabaie, ES.M. et al. | 2024 | Quantitative | Data Security in B.A | A loosely applicable source, however, may be used to build a narrative around how BB can build on the security for enterprises | Empirical | Information Security |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Springer Link | Deep learning-based authentication schemes for smart devices in different modalities: progress, challenges, performance, datasets and future directions | Shende, S.W., Tembhurne, J.V. & Ansari | 2024 | Qualitative | Personalisation Strategies in B.A.S. | a very robust source, answers challenges one and three of the three challenging factors- (1) privacy/ transparency risks and (3) privacy concerns/ personalisation | Empirical | Mobile Technology |
| Springer Link | User authentication method based on keystroke dynamics and mouse dynamics using HAD | Shi, Y., Wang, X., Zheng, K. et al. | 2022 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S | Use to build a narrative around how BB may enable users | Empirical | IT and Data Management |
| IEEE Xplore | Implementing Behavioural Biometrics With TRUST | J. Killoran, Y. G. Cui, A. Park, P. v. Esch, A. Dabiria | 2023 | Qualitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data | Addresses research question, provides a neat | Conceptual | IT and Data Management |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | n and J. Kietzmann. | | | Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | acronym to use in narrative | | |
| IEEE Xplore | A Biometrics-Based Behavioural Trust Framework for Continuous Mobile Crowd Sensing Recruitment | R. Nasser, R. Mizouni, H. Otrok, S. Singh, M. Abououd and M. Kadadha | 2022 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | Examines trust in users and how an enterprise may develop a system that may best enable them | Empirical | Mobile crowd sensing platforms |
| IEEE Xplore | It's All in the Touch: Authenticating Users with HOST Gestures on Multi-Touch Screen | C. Wu et al. | 2024 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, | Directly addresses research question | Empirical | IT and Data Management |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Devices | | | | Technological Advancements, Personalisation Strategies in B.A.S. | | | |
| IEEE Xplore | CASTRA: Seamless and Unobtrusive Authentication of Users to Diverse Mobile Services | D. M. Shila and K. Srivastava | 2018 | Mixed Methods | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, Personalisation Strategies in B.A.S. | Examines risk in systems, their security benefits and how this may influence how a user may accept their model | Empirical | Identity Verification |
| IEEE Xplore | Technology Acceptance Model: A Case Study of Palm Vein Authentication Technology | B. Nakisa, F. Ansarizadeh, P. Oommen and S. Shrestha. | 2022 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditining, Technological Advancements, Personali | Directly correlates with research question, use this reference | Empirical | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | sation Strategies in B.A.S. | | | |
| IEEE Xplore | Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis | H. U. Khan, M. Z. Malik, S. Nazir and F. Khan, | 2023 | Mixed Methods | Data Security in B.A. | Unfortunately, very vague generalised source, however, does support a narrative that adopting BB may enable security in the financial sector | Conceptual | Banking and Finance |
| IEEE Xplore | Secure, Fast, and Energy-Efficient Outsourced Authentication for Smartphones | P. Gasti, J. Šeděnka, Q. Yang, G. Zhou and K. S. Balagani | 2016 | Quantitative | Data Security in B.A. | Good for the first and third challenges. | Empirical | Mobile Technology |
| IEEE Xplore | TBIOM Special Issue on Trustworthy Biometrics–Editorial | W. Deng, T. Hassner, X. Liu and M. Pantic | 2022 | Qualitative | Trust in B.A.S, Personalisation Strategies in B.A.S. | Addresses research question, use this reference | Conceptual | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Scopus | Trustworthy interaction model: continuous authentication using time–frequency joint analysis of mouse biometrics | Zhang, YiGong, Yi, Qian, Yi Q, Yi, ShuPing a, Zhang, XiaoLong, Li, JiaJia. | 2022 | Quantitative | Data Security in B.A, User Conditining. | supports a narrative of how a user can be enabled by BB | Conceptual | Information Security |
| Scopus | PanAf20K: A Large Video Dataset for Wild Ape Detection and Behaviour Recognition | Brookes, Otto, et al | 2024 | Quantitative | rust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A, User Conditioning, Technological Advancements, Personalisation Strategies in B.A.S. | Interestingly, the first resource that is primarily ethical in nature | Empirical | Conservation |
| Scopus | An insider user authentication method based on improv | Tao, Xiaoling, Tao X, Yu, Yuelin, Fu, Lianyou, | 2023 | Quantitative | Diversity and innovations of B.A.S, Data Security in B.A, User | Through the lens of an enterprise and how they conduct | Conceptual | Identity Verification |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ed temporal convolutional network | Liu, Jianxiang, Zhang, Yunhao. | | | Conditioning, | business as a whole- how technology forces them to adapt, in turn may be used to bounce the 'trust' narrative off | | |
| Scopus | Multimedia Identification and Analysis Algorithm of Piano Performance Music Based on Deep Learning | Y. Jing, Z. Ying, L. Yuwei. | 2023 | Qualitative | Technological Advancements | Innovation', to sum this up in one word. May be used as well to build upon the second challenge identified | Empirical | Identity Verification |
| Scopus | Key factors driving the adoption of behavioural biometrics and continuous authentication | Stylios. I, Kokolakis. S, Thanou. O, Chatzis. S | 2022 | Quantitative | Trust in B.A.S, Diversity and innovations of B.A.S, Data Security in B.A. | directly correlates with research question. Excellent source | Empirical | IT and Data Management |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | technology: empirical research | | | | | | | |
| Scopus | Are there gender differences when interacting with social goal models: A quasi-experiment | Gralha. C, Goulão. M, Araujo. J | 2020 | Quantitative | Technological Advancements, Personalisation Strategies in B.A.S. | An interesting perspective stated here, the narrative suggests that gender plays a significant role in how users approach social interaction. With some work can be linked to willingness of trust in BB | Empirical | Social Science |
| Scopus | A context-aware system to secure enterprise content: | Oluwatimi. O, Damiani. M.L., Bertino. E | 2018 | Qualitative | Personalisation Strategies in B.A.S. | once key trust factors are identified, use this source as a | Empirical | Information Security |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Incorporating reliability specifiers | | | | | building block to support the narrative | | |