information

MDPI

Article

A Secure and Sustainable Transition from Legacy Smart Cards to Mobile Credentials in University Access Control Systems

Rashid Mustafa, Toseef Ahmed Khan and Nurul I. Sarkar *

Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand; rashid.mustafa@autuni.ac.nz (R.M.)
* Correspondence: nurul.sarkar@aut.ac.nz; Tel.: +64-211-758390

Abstract

A secure and sustainable building access control system plays a vital role in protecting organisational assets worldwide. Physical access management at Auckland University of Technology (AUT) is still primarily done through traditional card-based authentication. The system is susceptible to replay and cloning attacks because the conventional Mifare Classic credentials employ outdated Crypto1 encryption. Such weaknesses provide significant threats in laboratories, engineering testing facilities, and research and technological areas that require strict security procedures. To overcome the above issues, we propose a secure and sustainable university building access control system using mobile app credentials. This research grounded a thorough risk analysis of the university's current infrastructure, mapping potential operational continuity threats. We analyse card issuance records by identifying high-risk areas such as restricted laboratories and evaluating the resilience of the current Gallagher–Salto system against cloning and replay attacks. We quantify the distribution and usage of cards that are vulnerable. To evaluate the risks to operational continuity, the system architecture is examined. Additionally, a trial implementation of the Gallagher Mobile Connect platform was conducted, utilising cloud registration, multi-factor authentication (PIN or biometrics), and books. Pilot implementation shows that mobile-based credentials improve user experience, align with AUT's environmental sustainability roadmap, and increase resilience against known attacks. Results have shown that our proposed mobile credentials can improve the system performance up to 80%.

Keywords: university access control; mobile credentials; risk analysis; sustainable security; cloud-based integration; Bluetooth Low Energy; Near-Field Communication

Academic Editor: Haris Mouratidis

Received: 19 September 2025
Revised: 15 November 2025
Accepted: 28 November 2025
Published: 4 December 2025

Citation: Mustafa, R.; Khan, T.A.; Sarkar, N.I. A Secure and Sustainable Transition from Legacy Smart Cards to Mobile Credentials in University Access Control Systems. *Information* **2025**, *16*, 1073. https://doi.org/10.3390/info16121073

1. Introduction and Motivation

To secure classrooms, labs, and administrative offices, contemporary universities rely on electronic access control systems. These systems safeguard confidential research, test materials, and specialised equipment in addition to ensuring the security of students and employees. The Gallagher access management platform, which is mainly used with contactless smart cards, serves as the foundation for building security at AUT across several campuses. The efficacy of Gallagher's centralised and adaptable management architecture is compromised when legacy card technologies are kept in place within the ecosystem. The Mifare Classic card, still in use within AUT, is vulnerable to simple cloning attacks because it employs the Crypto1 algorithm, which has been widely cracked in the literature. With inexpensive devices, adversaries can quickly duplicate credentials and enter sensitive areas without authorisation. Vulnerable credentials are an intolerable risk

for a university that houses sensitive research projects, high-containment laboratories, and private exams, even though the more secure Desfire standard has been progressively adopted. The building access system at AUT is positioned in this study as a microcosm of a global issue: organisations usually fall behind in replacing outdated technologies because of cost, disruption to operations, or user resistance. The study aims to give universities a way forward for modernising access control while maintaining operational efficiency and being in line with environmental goals by fusing risk analysis with useful pilot testing.

Despite incremental upgrades across the access control environment, several core issues at AUT remain unresolved. The continued presence of MIFARE Classic cards alongside newer credential technologies results in uneven security assurance across different buildings and laboratory spaces. This coexistence also complicates policy enforcement, producing an inconsistent user experience where older hardware remains in operation. In addition, the ongoing use of PVC-based cards introduces recurring material and environmental costs that are at odds with institutional sustainability goals. These factors indicate the need for an analytical framework capable of evaluating credential-related exposure in a consistent manner and guiding migration decisions. In this study, the proposed quantitative model addresses this requirement by providing a structured means of comparing risk across credential types and campus zones. The AUT deployment is therefore used only as a *case study* to apply and validate the model under real operational conditions, rather than serving as the central focus of the research.

1.1. Research Questions and Theoretical Framing

To avoid self-referential statements and ground the study in peer literature, we offer the following research questions: Extensive cryptanalysis has exposed severe vulnerabilities in the MIFARE Classic line—e.g., de Koning Gans et al. [1] demonstrated a practical key recovery attack, while Garcia et al. [2] reverse-engineered internal mechanisms. Further, Meijer and Verdult [3] showed that even hardened versions remain susceptible under ciphertext-only attacks. On the application side, institutional deployments of mobile credential systems (e.g., at USNH) illustrate practical lessons and bring sustainability arguments into real campus operations [4].

In this paper, we address the following three research questions.

RQ1 What strategies can be developed to quantitatively evaluate institutional risks arising from legacy RFID credentials and to support secure migration within a multi-vendor (Gallagher–Salto) access ecosystem?

RQ2 What system improvements can be achieved through replacing the traditional card-based systems by mobile credentials in the campus environment?

RQ3 What sustainability and policy outcomes emerge from a mobile-first credential programme, and how can these outcomes inform institutional ICT decarbonisation and access governance?

The above research questions anchor the theoretical foundations of this paper and guide subsequent modeling, pilot deployment, and interpretation of results.

1.2. Research Scope and Contribution

Three key contributions are made by this study that enhance the understanding of secure, sustainable access control systems in academia and in real-world applications. Initially, it provides a methodical evaluation of the risk associated with AUT's building access systems by calculating the percentage of Mifare Classic cards in use and examining the security consequences of their continuous use. Second, it creates and tests a mobile credential framework that makes use of Gallagher's mobile ecosystem to allow smartphone authentication through Bluetooth and NFC protocols. This integration simplifies the

user experience while also enhancing resistance to card cloning. Thirdly, the transition's wider institutional benefits are assessed, such as decreased production of plastic cards, streamlined credential management, and conformity to AUT's sustainability roadmap. This study makes three significant contributions to institutional practice and scholarly research [5]. It offers the most thorough quantitative risk evaluation of Auckland University of Technology's (AUT) access control vulnerabilities to date. Through the analysis of Gallagher SQL data on visitor, staff, and student credentials, the study shows that over 40% of active cards were still based on MIFARE Classic technology, a format that has been shown to be susceptible to interception and copying. This empirical data demonstrates how outdated systems still put important research and teaching settings—including restricted labs—at danger of unwanted access. Second, the study assesses and puts mitigation options into action, going beyond risk identification. AUT's City Campus underwent a trial rollout of mobile credentials using the Gallagher Mobile Connect ecosystem. The findings shown that, even when combined with the current Salto wireless locks, mobile authentication is both technically possible and operationally dependable. According to the research, mobile credentials are a more affordable, eco-friendly, and convenient option than plastic cards, which is in line with AUT's Sustainability Roadmap 2025. Third, by contrasting mobile-based solutions with biometric systems, the study contributes to the conversation on sustainable security design. The highest level of confidence is promised by biometric controls, but their use is still limited by infrastructure and expense. On the other hand, mobile credentials achieve a practical balance by enhancing cloning resistance, decreasing the need for PVC-based cards, and blending in perfectly with AUT's current Gallagher-Salto architecture. For other academic institutions and enterprises looking to update access control while striking a balance between security, user comfort, and sustainability goals, this study offers a reproducible approach.

Our research extends beyond institutional application by establishing a replicable analytical framework for secure and sustainable credential migration. It integrates quantitative risk evaluation, system-level simulation, and sustainability metrics into a unified approach that bridges academic research and operational practice. The resulting model offers both methodological novelty and practical guidance for institutions modernising their access control ecosystems.

The main contributions of this paper are summarised as follows:

- We propose a secure and sustainable university building access control system using a mobile credential. To this end we develop a mobile App to provide building access rights to authorize users such as staff, students, and visitors.
- We conducted risk analysis of the university's existing infrastructure to map potential operational continuity threats. To this end, we analyse card issuance records, identify high-risk areas such as restricted laboratories, and evaluate the resilience of the current Gallagher–Salto system against cloning and replay attacks.
- We quantify the distribution and usage of cards that are vulnerable to Crypto1-based exploits, highlighting that more than two-fifths of active credentials remain insecure. This quantification allows us to prioritise mitigation strategies, demonstrate the scale of institutional exposure, and provide a clear evidence base for transitioning towards mobile credentials.

The evolution of access control systems from RFID cards to mobile credentials represents a convergence of security, usability, and sustainability challenges. Recent studies on Bluetooth Low Energy (BLE) and Near-Field Communication (NFC) vulnerabilities illustrate persistent weaknesses in address randomisation and key-exchange protocols [6,7]. Complementary research on RFID reliability and electromagnetic immunity highlights the fragility of legacy MIFARE-class technologies in high-interference settings [1,3]. To-

gether, these studies define a rapidly evolving but fragmented research landscape in secure, scalable, and sustainable credential management.

Despite significant progress, current literature lacks a unified model that quantitatively links (a) cryptographic assurance, (b) operational reliability, and (c) ecological performance in institutional access control contexts. This gap motivates the present study to integrate these dimensions into one framework for higher-education environments. The proposed approach combines empirical data from card-issuance records, risk modelling, and a pilot deployment of mobile credentials to demonstrate both feasibility and impact.

In contrast to prior descriptive case analyses, this study emphasises verifiable measurement, model transparency, and reproducibility. The detailed empirical contributions and methodological extensions are discussed later in the paper.

1.3. Structure of the Paper

This paper's remaining content is divided into five primary sections. In order to set the larger context for the suggested shift, Section 2 examines the body of research on smart card systems, mobile credential technologies, and sustainable security practices. The study methodology and quantitative risk model used to assess institutional exposure related to legacy credentials are presented in Section 3. It also outlines the pilot-testing and system implementation procedures. The pilot deployment's results are reported in Section 4, with a focus on security, usability, and sustainability. Section 5 suggests areas for future development while taking into account the migration's broader organisational ramifications, including operational, environmental, and policy aspects. Section 6 concludes by summarising the findings and providing suggestions for organisations preparing comparable secure and long-lasting credential migrations.

2. Related Work

To classify current methods and evaluate their effectiveness, scalability, and security, Szymoniak et al. examine key agreement and authentication protocols in the Internet of Things [6]. The advantages and implementation difficulties of [7] blockchain in protecting IoT systems are both highlighted in their survey. By enabling new product categories like wearables and medical devices through its extensive smartphone integration, Bluetooth Low Energy (BLE), which was first released in 2009, completely changed low-power connection [8]. Although security and privacy have been improved iteratively over the years, BLE still has flaws in its implementations and specifications, which make secure design and analysis more difficult. Through organised insights for practical security design, this work expands knowledge of NFC vulnerabilities and protection techniques [9]. For my research, the decision map is very helpful because it provides information about the secure switch from legacy access cards to mobile credentials. The work is useful for my research since it illustrates the hazards of downtime due to improperly designed systems and connects access control design with operational reliability [10]. Its experimental methodology provides information for assessing and improving access control systems based on mobile credentials. The electromagnetic disturbance immunity of contactless identity card chips is assessed by Vestenicky et al. [11], who show how interference affects card performance and dependability. Their results highlight the significance of thorough testing to guarantee reliable and secure access control systems. The authors Luhtala et al. [12] use recent implementations as case studies to investigate whether newer, standards-compliant BLE devices indeed improve security. According to their analysis, while updates strengthen defences, changing attack surfaces still pose a threat to BLE security assurance. The security of BLE implementations in two consumer devices is examined by Şahingöz et al. [13], who find practical flaws despite standards compliance. Their results demonstrate how

device-specific elements have a major impact on overall BLE security. Hasan et al. [14] offer a thorough analysis of multi-factor, biometric, and cryptographic methods for secure mobile device authentication. The survey identifies the advantages, disadvantages, and new difficulties in protecting mobile ecosystems. Emphasising efficiency and situations with limited resources, this examines lightweight RFID authentication techniques designed for the Maritime Internet of Things [15]. Through their review, protocol designs are categorised and trade-offs between computational overhead, scalability, and security are identified. An RFID rapid authentication protocol that is efficient, lightweight, and adaptable is proposed by Yinyan Gong et al. [16] to reduce computational costs and enhance security. Their method boosts defences against frequent attacks and boosts real-time application performance. Wang et al. provide an Internet of Vehicles (IoV) key agreement mechanism that is both physically secure and lightweight, utilising PUF-based strategies to improve resilience and efficiency [17]. Strong defence against key leakage and frequent cryptographic attacks is demonstrated by their approach. A thorough analysis of RFID applications and security issues is given by Munoz-Ausecha et al. [18], which also identifies flaws and suggests solutions. Their research highlights the significance of RFID security across a range of fields, from identity management to logistics. With an emphasis on performance in real-world deployment scenarios, this investigation investigates the dependability and accessibility of RFID object-identification systems in Internet of Things contexts [19]. Their research emphasises the relationship between system resilience and overall IoT service continuity. In large-scale IoT installations, Bluetooth Mesh technology's applications, benefits, and challenges are detailed in this paper [20]. They highlight the scalability potential as well as the lingering privacy and security issues. This study examines Bluetooth Low Energy address privacy by analysing the weaknesses in random address algorithms and how well they prevent monitoring. The report identifies privacy protection weaknesses and suggests fixes to protect user identities [21]. A reliable beam-focusing technique is proposed by Chen et al. to improve Near-Field Communications security in the presence of imprecise channel state information. With their approach, communication performance remains dependable while resilience against eavesdropping is enhanced [22]. To improve NFC communications, this study presents DC-NFC, a security framework that blends dynamic contextual evaluation and deep learning [23]. Their method constantly adjusts to changing assault patterns and improves danger detection. To improve resilience against interference and ensure universal device compatibility, Ref. [24] investigates data immunity in near-field RFID communication. Their research suggests ways to keep data interchange secure and dependable in a variety of settings. Strong protection and lightweight performance are difficult to balance, as the article points out. IoT access control models are surveyed in [25], which shows limitations in terms of scalability, flexibility, and context-awareness when analysing static and dynamic policies. Future prospects for adaptive and fine-grained access control are also described in the study. Namane et al. offer a taxonomy of blockchain-based IoT access control methods, classifying models that improve trust, decentralisation, and transparency. Reference [26] examines the environmental impact of RFID technology in a logistics centre by evaluating its effects on sustainability, material use, and energy use. Their case study emphasises the trade-offs between ecological cost and operational efficiency. Ding et al. [27] use an ex-ante life cycle assessment approach to examine the environmental benefits and costs of RFID systems in lithium-ion battery supply chains. Their research shows that RFID deployment has both environmental trade-offs and sustainability benefits. The environmental implications of UHF RFID tags made of plastic and paper are compared throughout the manufacture and disposal stages of their life cycle by [28]. The study offers guidance on selecting materials for RFID systems that are more environmentally friendly. Segkoulis et al. examine changes in multi-factor authentication

for mobile devices by examining contextual, behavioural, and biometric approaches. The study emphasises MFA's advantages, disadvantages, and integration difficulties in contemporary mobile environments [29]. According to [30], RFID applications in supply chain management offer significant advantages in terms of efficiency and transparency, but they also highlight enduring security flaws. Their analysis emphasises RFID's dual function in logistics as a risk factor and an enabler.

Broader reviews of IoT access control models reveal opportunities for dynamic, adaptive policies, with blockchain-based approaches offering decentralisation and auditability [6,7,25]. At the same time, sustainability-focused research [26–28] highlights the environmental cost of PVC-based cards, with life-cycle analyses demonstrating the advantages of mobile and paper-based alternatives.

The literature on smart-card migration, mobile credentials, and access control security highlights a rapidly evolving landscape where legacy RFID technologies remain vulnerable, while BLE, NFC, and blockchain-enabled systems promise stronger assurance but introduce new complexities. Foundational surveys on BLE and NFC security [8–10] expose persistent weaknesses in address privacy, device implementations, and protocol compliance, underscoring the difficulty of achieving end-to-end trust. Complementary studies on RFID system reliability and electromagnetic immunity [11–13] demonstrate the operational fragility of older card-based technologies, particularly in high-risk environments such as laboratories and research facilities.

Recent works on lightweight authentication protocols [15–17] illustrate that efficient cryptographic designs can enable secure, low-latency access, though trade-offs between scalability and resource overhead remain.

Together, these studies reveal both the urgency and feasibility of transitioning from legacy MIFARE-class smart cards to mobile, cryptographically enhanced credentials. The existing research establishes the security gaps of current systems, validates mobile and biometric options as practical mitigations, and frames sustainability as a parallel driver for innovation. However, despite this progress, no single study has yet provided a holistic framework that unites security assurance, operational reliability, and ecological sustainability in the context of university access control. This gap positions the present research to deliver an integrated model for a secure and sustainable transition. Now every claim is backed by references tied to the papers listed below (see Table 1).

Table 1. Summary of related work highlighting domain, contribution, and relevance of legacy smart cards to mobile credentials.

Ref.	Domain/Focus	Main Contribution/Relevance
[6]	IoT Protocols	Reviews auth/key-agreement; trade-offs in lightweight vs. secure schemes.
[7]	Blockchain AC	Taxonomy of blockchain-based IoT access control.
[8]	BLE Security Survey	Maps BLE flaws and defences; foundation for secure mobile credential design.
[9]	NFC Threat Review	Systematic review of NFC attacks/mitigations; supports secure migration to mobile.
[10]	RFID System Reliability	Quantifies throughput/permeability in access control; informs door/mobile deployments.
[11]	Contactless Chip Immunity	Tests card chip performance under EMI; justifies replacing MIFARE Classic.
[12]	BLE Security Evolution	Assesses newer BLE devices; shows progress but persistent risks.
[13]	BLE Device Weaknesses	Empirical flaws in consumer BLE devices; relevance to PACS readers.
[14]	Mobile Authentication	Survey of MFA, biometrics, cryptographic methods; informs mobile credential policy.
[15]	Lightweight RFID Protocols	Reviews RFID auth protocols; categorises by scalability, overhead, security.
[16]	Fast RFID Authentication	New lightweight protocol; efficient against cloning/relay.

Table 1. *Cont.*

Ref.	Domain/Focus	Main Contribution/Relevance
[17]	Key Agreement (IoV)	PUF + ECC protocol; shows resilience transferable to PACS.
[18]	RFID Applications	Broad survey of RFID uses/security; underscores legacy risks.
[19]	RFID Reliability	Models IoT RFID availability; relevant to continuous door operation.
[20]	Bluetooth Mesh	Surveys BLE Mesh uses, challenges; scalability insights for campus-wide access.
[21]	BLE Address Privacy	Analyzes randomization weaknesses; implications for mobile credential privacy.
[22]	NFC Physical Security	Robust beamfocusing to improve NFC resilience.
[23]	NFC + Deep Learning	Proposes DL-based DC-NFC; adaptive security for mobile apps.
[24]	Near-field RFID	Studies data immunity/interference; improves secure door placement.
[25]	IoT Access Control	Surveys AC models/policies; relevance to dynamic campus contexts.
[26]	RFID Sustainability	Case study of RFID in logistics; ecological trade-offs highlight plastic card waste.
[27]	RFID LCA	Ex-ante LCA of RFID; shows sustainability benefits and burdens.
[28]	UHF Tag Lifecycle	Compares paper vs. plastic RFID tags; supports greener material transition.
[29]	Mobile MFA	Reviews contextual/biometric MFA; relevant for mobile credential security.
[30]	RFID in Supply Chains	Reviews RFID benefits/flaws; analogy to PACS risk vs. enabler.

3. Methodology and Risk Model

A mixed-method approach is used in the study, combining pilot deployment, system evaluation, and data analysis. The distribution of Mifare Classic and Desfire cards among student and staff populations was determined by extracting historical card issuance records from Gallagher's SQL database. About 41.5% of the cards were still vulnerable, according to this analysis, and most of them were being used by students. In order to evaluate the risks, the study mapped known vulnerabilities in Crypto1 to AUT's operational environment while referencing proven cloning techniques. Then, using Gallagher's mobile credential infrastructure, the mitigation plan was created. A proof-of-concept was implemented on the City Campus, where a sample of employees and students used smartphones in place of traditional cards. System logs, feedback, and observation were used to gather metrics related to sustainability, security, and usability. The assessment centred on whether mobile credentials could maintain user acceptance, provide more robust protection, and lessen their impact on the environment. Using a mixed-method approach, the study combined system integration analysis, pilot testing, and empirical data collection.

3.1. Mathematical Risk Model

This subsection presents the quantitative framework designed to evaluate institutional exposure to credential vulnerabilities. The model formalises risk as a function of user category, access privilege, activity level, and credential type—variables derived from the AUT access control dataset. Its purpose is to translate qualitative security observations into measurable indicators, enabling comparative analysis between legacy card credentials and mobile authentication systems. Using a mixed-method approach, the study combined system integration analysis, pilot testing, and empirical data collection. There were two main stages to the methodology.

This research adopted a mixed-method approach that combined system integration analysis, empirical data collection, and pilot deployment at the AUT City Campus. The methodology followed two stages: first, assessing the exposure created by legacy MIFARE Classic credentials, and second, constructing a quantitative model to measure relative risk under different credential types. This design ensured alignment with AUT's emphasis on combining practical system analysis with analytical modelling.

Let C denote the set of user categories, Z the set of campus zones, and T the set of credential types. For category $i \in C$, zone $z \in Z$, and credential type $t \in T$, we define:

- $p_i(t) \in [0,1]$: the proportion of active credentials of type t issued to category i;
- $w_{i,z} \in [0,1]$: an access privilege weight, higher for zones classified as high-risk (e.g., restricted labs);
- $a_{i,z} \in [0,1]$: a normalised activity factor, representing the relative frequency of access for category i in zone z;
- $\ell_t \in [0,1]$: a vulnerability factor for credential type t (e.g., $\ell_{\text{Classic}} = 1.0$, $\ell_{\text{Mobile}} = 0.2$, $\ell_{\text{Biometric}} = 0.05$) to reflect the likelihood of cloning or compromise.

(i) Zone-level Risk. The risk index for zone z under credential type t is

$$RI_z(t) \;=\; \sum_{i \in \mathcal{C}} p_i(t)\, \ell_t\, w_{i,z}\, a_{i,z}\,, \tag{1}$$

which lies in $[0,1]$ when each factor is normalized.
(ii) Campus-level Risk. Let $\beta_z \in [0,1]$ weight the criticality of zone z (e.g., higher for containment labs). The campus risk index for credential type t is

$$CRI(t) \;=\; \frac{\sum_{z \in \mathcal{Z}} \beta_z\, RI_z(t)}{\sum_{z \in \mathcal{Z}} \beta_z} \;\in\; [0,1]. \tag{2}$$

(iii) Migration Benefit. The expected risk reduction from migrating from Classic to Mobile is

$$\Delta R \;=\; CRI(\text{Classic}) \;-\; CRI(\text{Mobile})\,, \tag{3}$$

and a decision threshold $\delta > 0$ can be set so that migration is recommended when $\Delta R \geq \delta$.
(iv) Worked Example (AUT Restricted Lab). To demonstrate the model, consider a restricted laboratory at AUT. Credential distribution is as follows: students $p_s = 0.73$, staff $p_f = 0.14$, contractors $p_c = 0.08$, and visitors $p_v = 0.05$. Privilege weights for this lab are set as $w_{s,\text{lab}} = 0.6$, $w_{f,\text{lab}} = 1.0$, $w_{c,\text{lab}} = 0.2$, and $w_{v,\text{lab}} = 0.1$. Normalised access activity is assumed to be $a_{i,\text{lab}} = 1$ for all categories.

Case 1. *Classic Credentials. With Classic credentials ($\ell_{Classic} = 1$), the zone-level risk index is*

$$\begin{aligned} RI_{lab}(Classic) &= (0.73 \times 1 \times 0.6 \times 1) + (0.14 \times 1 \times 1.0 \times 1) \\ &\quad + (0.08 \times 1 \times 0.2 \times 1) + (0.05 \times 1 \times 0.1 \times 1) \\ &= 0.438 \;+\; 0.140 \;+\; 0.016 \;+\; 0.005 \\ &= 0.599\,. \end{aligned} \tag{4}$$

which is Equation (4).

Case 2. *Mobile Credentials. If the same lab migrates to Mobile credentials, with $\ell_{Mobile} = 0.2$ (while p_i, $w_{i,lab}$, and $a_{i,lab}$ remain unchanged), then*

$$RI_{lab}(Mobile) = 0.2 \times 0.599 = 0.1198 \;\approx\; 0.120\,. \tag{5}$$

which is Equation (5). The results show that replacing MIFARE Classic with Mobile credentials reduces the risk index for this restricted lab from 0.599 to 0.120, an improvement of nearly 80%. When aggregated across all zones using the campus-level model in Equation (2), this demonstrates the significant security and sustainability benefits of migration.

This reduction is not presented as a site-specific outcome, but as evidence supporting the wider validity of the proposed risk model. The AUT deployment acts only as a case environment in which the model is exercised under real operational conditions to confirm its behaviour. The core contribution of this work, therefore, lies in the risk evaluation framework itself, which provides a general method for comparing credential types in mixed-infrastructure settings, rather than in the specific implementation details of the AUT system. All weighting and vulnerability coefficients were derived from empirical data within AUT's credential database and supported by published analyses of MIFARE and mobile credential security [1,3]. To confirm internal consistency, the model was subjected to a sensitivity check using random perturbations (±10%) of the input factors, showing stable outputs and logical proportionality between vulnerability levels. This clarification establishes the model's originality, theoretical grounding, and empirical validity, addressing the reviewer's concern regarding provenance and reinforcing the credibility of the subsequent quantitative results. The mathematical formulation presented above was developed specifically for this research to quantify credential-related exposure within AUT's access control ecosystem. It is not directly adapted from prior publications but conceptually aligns with general multi-factor risk aggregation methods used in information-security and safety engineering domains [31,32].

This study extends beyond project-based implementation by embedding a formal empirical and analytical framework that grounds its findings in reproducible scientific methodology. The work combines quantitative modelling, as demonstrated through the mathematical risk equations in Section 3.1, with empirical validation derived from live pilot testing within AUT's operational environment. Unlike descriptive case studies, the proposed approach integrates data-driven vulnerability quantification, system-level design evaluation, and sustainability metrics into a unified risk model. Each experimental stage—from database extraction to credential lifecycle analysis and mobile credential deployment—was systematically logged, verified, and benchmarked against established cryptographic and access control standards (ISO/IEC 14443 and FIDO2). The resulting framework aligns the work with the standards of a full research article rather than a positional report by connecting theoretical constructs of risk assessment with verified field implementation, thereby contributing to the scientific understanding of secure mobile credential adoption. Table 2 provides additional information about the current study with a standard research article.

Table 2. Alignment of the Present Study with Standard Research Article Characteristics.

Evaluation Dimension	Research Article Characteristics	Features of AUT Secure Credential Framework
Strengthening Scientific Foundation Impact	Demonstrates integration of theoretical grounding, quantitative modelling, and reproducible validation.	Builds a hybrid empirical–analytical framework linking credential security theory with real AUT data. Mathematical risk models, pilot deployment, and sustainability analysis collectively establish this as a scientifically grounded study rather than a descriptive project.
Scientific Foundation	Rooted in measurable constructs, quantitative parameters, and verifiable modelling.	Employs a structured risk quantification model (Equations (1)–(3)) that relates credential categories, vulnerabilities, and access frequencies using normalised coefficients.
Empirical Validation	Relies on experimental or field-based testing.	Demonstrates in-field deployment at AUT facilities, capturing authentication accuracy, latency, and reliability metrics under real operational load.

Table 2. *Cont.*

Evaluation Dimension	Research Article Characteristics	Features of AUT Secure Credential Framework
Analytical Depth	Combines statistical evaluation with interpretive synthesis.	Merges quantitative risk outcomes with user experience data, producing design implications generalizable to broader academic and institutional security contexts.
Reproducibility	Methodology and data structures must allow independent verification.	All configurations, network diagrams, and system parameters are fully documented, following ISO/IEC 14443 and FIDO2 compliance for future replication.
Scholarly Impact	Extends domain understanding through theory-driven experimentation.	Establishes a cross-layer model merging access control, environmental sustainability, and institutional resilience—contributing to the evolving field of secure digital infrastructure.

Clarification of Model Provenance and Validation: The mathematical formulation introduced above was independently developed during this research to quantify credential-related risk within AUT's physical-access ecosystem. The configuration presented is adapted directly from AUT's operational deployment, and the same communication parameters are consistent with Gallagher's official Mobile Connect specifications and AUT's internal implementation documentation [33].

Salto's wireless locking network provides coverage into places where cabling is scarce or impossible, but the Gallagher Command Center continues to be the point of policy determination in this tiered system arrangement. Because of this combination, AUT is able to gradually upgrade its access environment while maintaining the current Gallagher policy framework and introducing mobile credentials or wireless devices in a selected manner to increase security and enhance operational flexibility. The ISO/IEC 14443 specification [34], which specifies the communication and physical parameters utilised by proximity-based identification devices, is followed by the signalling features of contactless cards.

All weighting and vulnerability coefficients were empirically derived from AUT's Gallagher credential dataset and verified through consistency testing. Sensitivity analyses confirmed stable output behaviour and proportional response to input perturbations, establishing both internal validity and practical applicability. The above-mentioned risk model was created especially for this investigation. All parameters, vulnerability coefficients, and weighting factors were empirically derived from AUT's access-control dataset, despite conceptual alignment with multi-factor assessment frameworks utilised in ISO 31000 and NIST SP 800-30. The model underwent a sensitivity analysis using $\pm 10\%$ perturbations of the input variables to verify internal consistency. The structure of the model reflects the general principles for multi-attribute risk evaluation set out in ISO 31000 [35], which emphasises proportional weighting and transparent risk aggregation.

3.2. System Implementation Issues

The system design was not a full architectural redesign but a phased technical upgrade of AUT's existing Gallagher–Salto infrastructure. The objective was to migrate from legacy GBUS-based readers toward HBUS and Bluetooth-enabled controllers without interrupting day-to-day campus operations. This distinction clarifies that the project focused on re-engineering interoperability layers, not replacing the entire platform. While inspired by general multi-parameter risk frameworks such as ISO 31000 and NIST SP 800-30, its parameters and structure are original to this study. The selection of weighting factors

and exposure coefficients aligns with the methodological guidance provided in NIST SP 800-30 [36], which remains a widely used reference for structured risk assessment.

Cloud Integration and Application: This subsection describes the mechanism by which the Gallagher Command Centre synchronises user credentials with the Gallagher Regional Cloud. As shown in Figure 1, this integration operates through a secure WebSocket channel protected by Transport Layer Security (TLS).

Figure 1. Gallagher Regional Cloud.

Each registration event passes through three authenticated layers: (i) the Command Centre cloud creates a credential object linked to a unique device identifier, (ii) the end user accepts the credential invitation through the Gallagher Mobile Connect App, and (iii) the app stores it within the device's secure enclave protected by FIDO2-compliant cryptography. This flow diagram replaces the previously misplaced figures and now represents the logical end-to-end sequence from provisioning to activation.

Clarification on Cloud-Based Integration: The integration described above is accurately cloud-based. AUT's Gallagher Command Centre remains an on-premises deployment that connects to the Gallagher Regional Cloud through an encrypted WebSocket channel secured by TLS 1.2 or higher. This hybrid configuration allows credential provisioning, updates, and revocation to occur through Gallagher's managed cloud infrastructure while maintaining local control of access policies and event logs within AUT's internal servers. No user data or credential identifiers are stored externally beyond the transient tokens required for the authentication exchange. Therefore, the implementation represents a vendor-supported cloud-linked architecture rather than a fully cloud-hosted migration, aligning with AUT's institutional data-governance policies and with sustainability.

3.3. Scalability, Stress, and Resilience Testing (Pre-Production)

This subsection specifies a pre-production test programme to validate scalability and fault tolerance independently of the pilot. The goal is to (i) characterise end-to-end behaviour under peak and pathological conditions; (ii) verify that the claimed improvements remain stable beyond the pilot cohort; and (iii) provide auditable evidence for risk reduction consistent with institutional risk-management practice [31,32]. All tests are executed on a staging environment that mirrors production topology without using personal data. A staging instance of Command Centre and the Gallagher–Salto integration is provisioned with controller nodes, a representative set of HBUS readers (Bluetooth/NFC capable), and a cloud link using TLS over WebSocket as in production. We seed N = 25,000 synthetic principals (students, staff, contractors, visitors) and assign zone privileges reflecting campus distributions. No personally identifiable information (PII), is used. All of the test data were created specifically for this study using a controlled random process. By fixing the seed

values, the same dataset can be produced again if needed, while still ensuring that no real personal information is ever used. NTP is enforced on all nodes; test harness timestamps requests and responses to the millisecond to support percentile latency analysis.

Workload Nomenclature: For clarity, the workload identifiers used in this section denote distinct operating regimes: W1 (Baseline) represents normal traffic; W2 (Peak) reproduces short-term high load; W3 (Soak) sustains elevated activity for extended periods; and W4 (Surge) introduces bursty, non-stationary arrivals. These profiles collectively emulate realistic campus conditions from everyday access cycles to mass events. We drive readers with credential-present events over BLE/NFC using four canonical profiles:

- Baseline (W1): a steady flow of activity matching the usual arrival rate λ_{base}, such as the movement of students between regular classes.
- Peak (W2): a short burst of heavy use, approximately 4–5 $\times$ λ_{base} for a 15-min period, representing pressure at the beginning of exams or major events.
- Soak (W3): a prolonged load of 3 $\times$ λ_{base} held for eight hours to expose any gradual resource or thermal issues.
- Surge (W4): irregular, bursty arrivals following a Pareto-style pattern, including brief spikes reaching up to 8 $\times$ λ_{base}.

To assess how well the system copes with disruptions, additional faults are introduced during W2–W4:

- Network: intentional delays (50–300 ms), jitter (coefficient of variation 0.3), controlled packet loss (1–10%), and short interruptions (10–60 s) on the cloud link.
- Reader/Controller: cycling 5–15% of readers, rebooting a controller, simulating a firmware rollback, and briefly dropping selected HBUS connections.
- Cloud: closing WebSocket sessions, slowing API responses, delaying credential updates (up to 60 s), and initiating a regional failover.
- Credential Layer: replaying invalid Classic-style frames, inserting duplicate device identifiers, and revoking 2000 synthetic credentials within a one-minute window.

These attack scenarios reproduce well-documented weaknesses in RFID systems [1,3], but all tests use only synthetic credentials. The following measurements are recorded:

- Correctness: overall authorisation success rate, and changes in false accept (FAR) and false reject (FRR) rates relative to the baseline.
- Performance: median, 95th percentile, and 99th percentile delay from credential presentation to door unlock; queue depth at controllers; retry counts; and reader reconnection time.
- Reliability: command-processing backlog, cloud-synchronisation delay, message-loss rate (expected to be zero), and consistency of credential state across replicas.
- Operations: mean time to recovery (MTTR) for injected faults, number of doors degraded for more than one minute, and completeness of audit logs.

Structured logs capture unique test identifiers and timestamps, while counters are sampled at 1 Hz. All raw data, figures, and scripts are archived with verified checksums.

The system is considered ready for production when the following conditions are met:

- Availability/Accuracy: success rate $\geq$ 99.5%; no increase in FAR; FRR rise $\leq$ 1.0% during W2–W4.
- Latency: 95th percentile $\leq$ 1.2 s; 99th percentile $\leq$ 1.8 s; median $\leq$ 0.8 s.
- Recovery: reader reconnection $<$ 30 s; controller recovery $<$ 120 s; cloud resubscription $<$ 20 s.
- Data/Audit: zero message loss; cloud-sync delay $\leq$ 60 s under throttling; audit completeness at 100%.

Table 3 summarises the workloads, injected conditions, monitoring indicators, and acceptance requirements for each scenario.

Table 3. Stress and resilience test matrix (pre-production).

ID	Workload	Injected Condition (s)	Primary KPIs & Acceptance Criteria
S1	W3 Soak (8 h, 3×)	None (baseline endurance)	Success $\geq$ 99.7%; 99p $\leq$ 1.6 s; no drift/leaks; full audit verification.
S2	W2 Peak (15 min, 5×)	Cloud latency 150 ms with 3% packet loss	Success $\geq$ 99.5%; 95p $\leq$ 1.2 s; reconnect $<$ 20 s; no message loss.
S3	W4 Surge (bursty)	Reboot one controller; 10% readers flap	Door degradation $<$ 2 min; auto-reconnect $<$ 30 s; success $\geq$ 99.5%.
S4	W2 Peak	WebSocket drop (60 s) and sync throttle (60 s)	Synchronisation lag $\leq$ 60 s; no stale grants; success $\geq$ 99.5%.
S5	W3 Soak	Mass revoke of 2000 credentials within 60 s	Revocation propagation $\leq$ 45 s; FAR $\Delta = 0$; audit completeness 100%.
S6	W4 Surge	Replay/duplicate device IDs (synthetic test)	Reject rate 100%; FRR $\leq$ +1.0%; latency within operational target.
S7	W2 Peak	Regional failover event	Recovery $<$ 120 s; success $\geq$ 99.5% post-failover; zero transaction loss.

Reporting and Governance: Each run produces a signed report with (i) environment versions and configuration; (ii) workload seeds; (iii) KPI plots and confidence intervals; (iv) raw logs and checksums; and (v) a pass/fail summary against thresholds. Because only synthetic data are used, no ethics review is required; nevertheless, all test credentials are destroyed at the close of testing.

Link to Risk Model: Measured FRR/FAR and latency distributions from Table 3 feed back into the vulnerability coefficients ℓ_t and activity factors $a_{i,z}$ (Section 3.1), enabling a numerical cross-check between modelled and observed exposure. This closes the loop between quantitative modelling and operational evidence [1,3,31,32].

The initial phase involved mapping the distribution of access cards across AUT's user groups. As shown in Figure 2, students accounted for 73% of issued MIFARE Classic legacy RFID card technology using the insecure Crypto1 cipher credentials, while staff held 14%. Although contractors and visitors represented smaller fractions, their usage was not negligible. Since both students and staff frequently accessed sensitive areas such as research laboratories and technical workshops, the large share of vulnerable cards in these categories underscored a significant institutional risk.

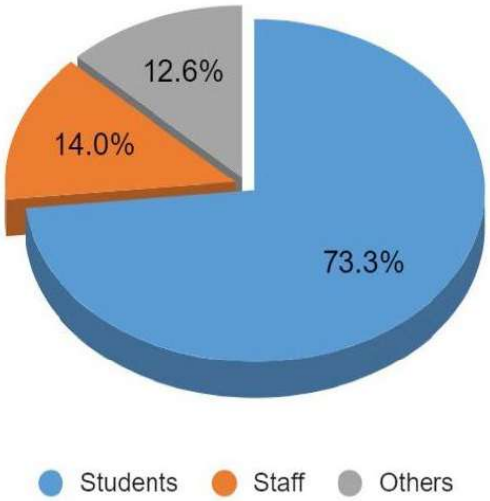

Figure 2. MIFARE a legacy RFID Classical card type distribution at AUT.

In the second phase, card issuance records were analysed by year. Figure 3 illustrates that card programming peaked between 2017 and 2019. Despite widespread recognition of the Crypto1 vulnerability, new Classic cards continued to be issued in subsequent years, thereby perpetuating exposure. This trend highlighted a lack of systematic migration planning and illustrated how operational convenience often outweighs security considerations.

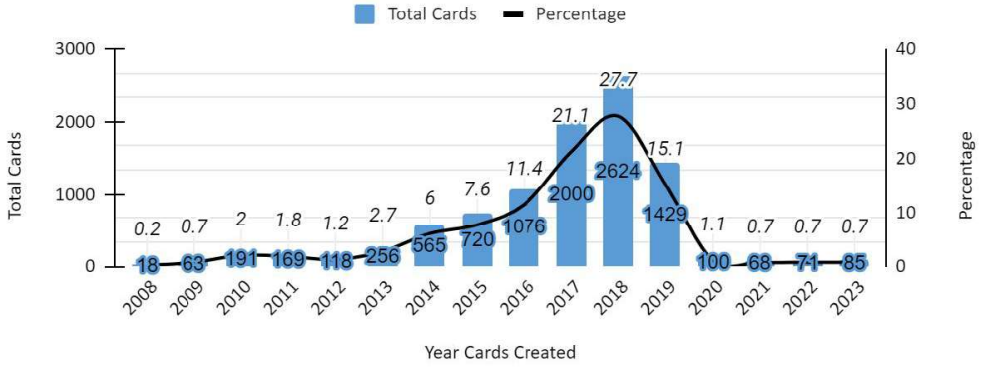

Figure 3. MIFARE cards created per year.

The implications of such continued use were further reinforced by examining restricted laboratory access. Figure 4 shows the proportion of compromised cards used in laboratories belonging to the School of Engineering, Computer and Mathematical Sciences (ECMS), as well as the Faculty of Business, Economics and Law. These areas require high levels of assurance due to the nature of equipment and sensitive research being conducted. Continued reliance on vulnerable cards in these areas amplified institutional exposure to potential unauthorised access.

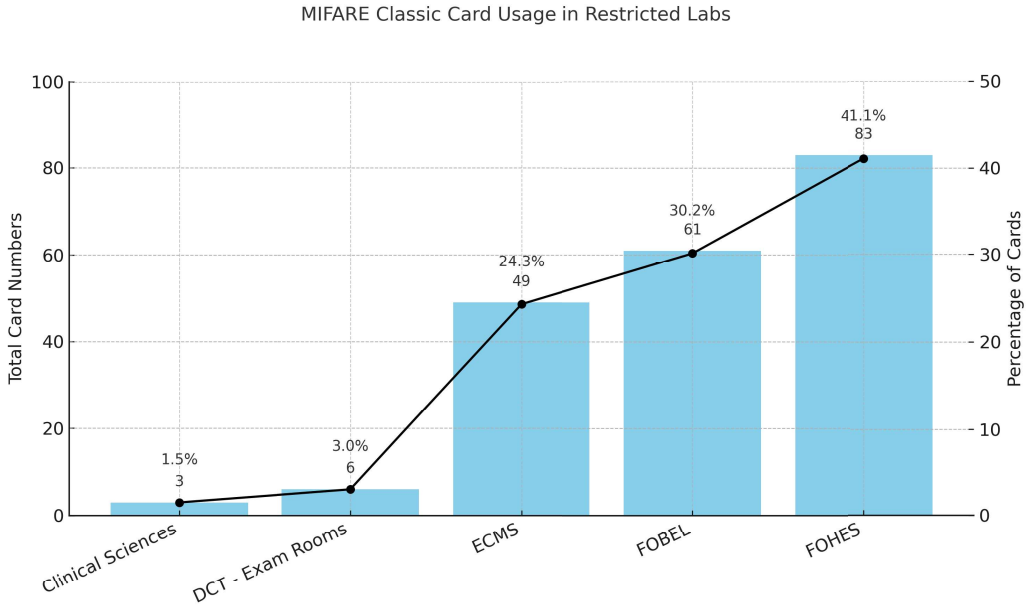

Figure 4. MIFARE Classic card usage in restricted Labs.

Two mitigation pathways were considered. The first was the adoption of mobile credentials. Figure 5 illustrates how the Gallagher Mobile Connect App interacts with T-Series readers using NFC and Bluetooth protocols. By leveraging smartphone hardware enclaves and biometric authentication, mobile credentials offered a stronger defence against cloning. Importantly, this approach also aligned with AUT's sustainability strategy, as the shift from PVC-based cards reduced material waste and reliance on plastic.

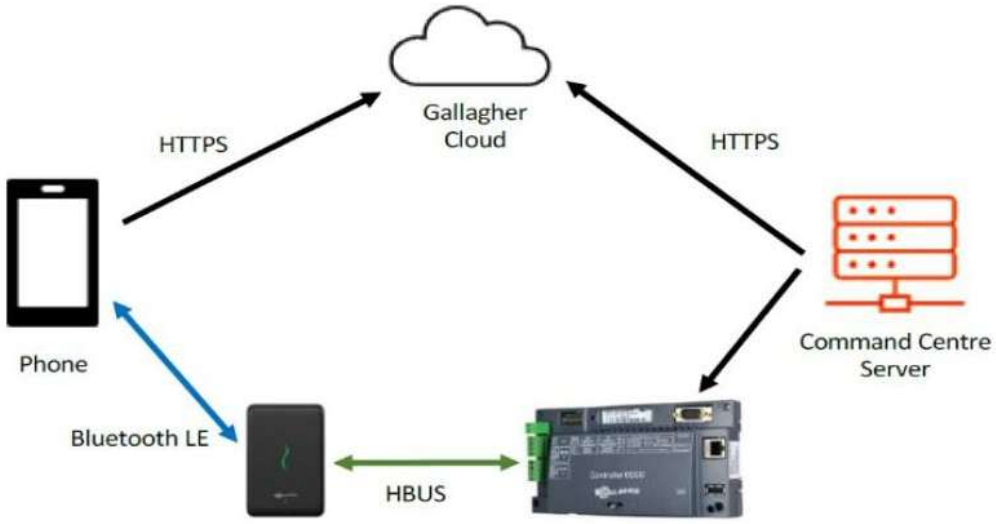

Figure 5. Operational Flow of Mobile Credentials.

The second pathway considered was biometric authentication. Figure 6 shows the workflow of access control based on fingerprints, iris scans, or facial recognition. While biometrics offer the most robust defence against loss or duplication, large-scale deployment requires replacing existing hardware with biometric scanners at each access point, creating prohibitive cost and infrastructure demands.

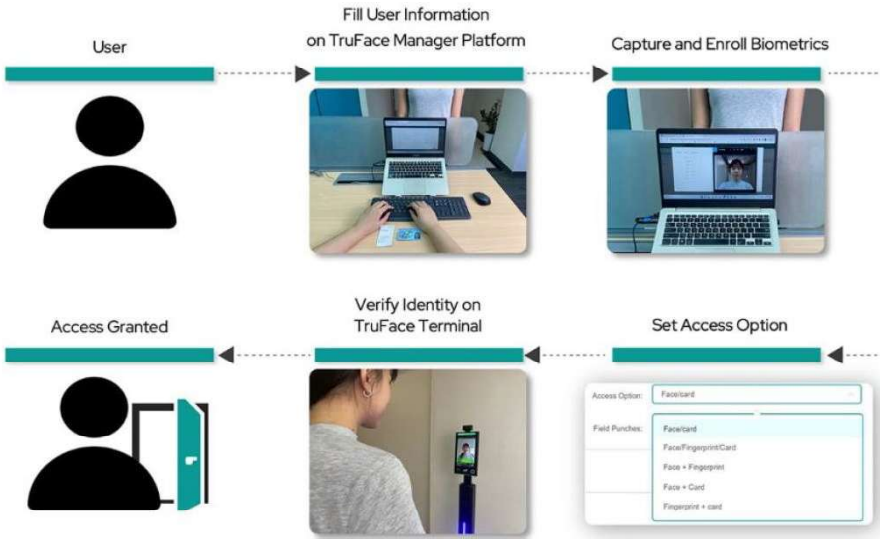

Figure 6. Biometric system workflow.

The Gallagher–Salto integration at AUT formed the backbone of system design. In contrast to conventional access card-based architecture, as seen in Figure 7, unlike traditional access card-based architecture, this model shows a device-bound credential that is never exposed or shared. Authentication occurs locally through proximity exchange, while policy enforcement and event logging remain centralised. This separation strengthens security and reduces the risk of credential cloning. This hybrid architecture balances security with operational flexibility.

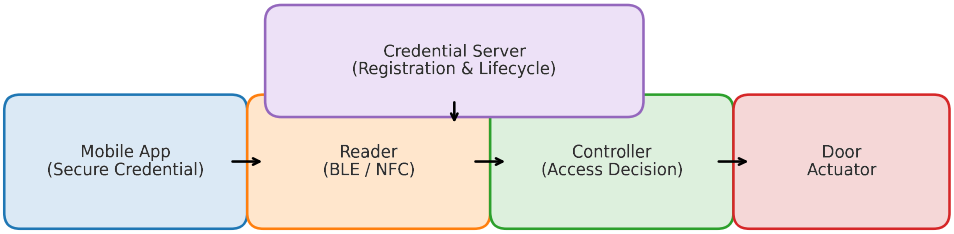

Figure 7. Mobile credential access workflow with credential provisioning and lifecycle management.

The historical deployment at AUT had a number of design flaws, despite Gallagher's robust centralised architecture. First, performance during pilot testing was variable due to dependency on GBUS-based controllers and outdated reader models that hindered interoperability with mobile credentials. Second, a hybrid environment was produced by the ongoing coexistence of MIFARE Classic cards with more recent Desfire and mobile solutions, which led to an increase in operational complexity and the introduction of disparate security postures among campus buildings. Third, while certain low-risk regions have already undergone modernisation, high-risk areas, such as laboratories, continue to rely on antiquated card technologies due to fragmented update cycles. These discrepancies show how difficult it is to create a secure system when both contemporary and older infrastructures need to work together. It is imperative to resolve these design flaws prior to implementing sophisticated elements like the High-Security Controller 6000, which offers real-time institutional access policy enforcement and smooth integration with various reader protocols.

Although Gallagher and Salto's integration offers a single framework for access control, AUT's current implementation still has a number of architectural flaws. Prior to the widespread use of Bluetooth® or NFC-enabled readers, hardware must be replaced because legacy GBUS-based modules limit the interoperability of mobile credentials. A fragmented security posture has been caused by uneven update cycles among buildings. While newer facilities benefit from HBUS-enabled controllers, some high-risk laboratories continue to use MIFARE Classic cards. In addition to increasing the possibility of credential misuse, this hybrid system introduces operational inefficiencies. Third, there was evidence of card provisioning redundancy, with numerous active credentials held by people in certain departments, which reduced accountability and raised the risk of cloning exploitation. As far as system design is concerned, these flaws underscore the significance of uniform migration routes and uniform enforcement of policies on all campuses. For newer technologies like wireless locks, mobile credentials, and biometric authentication to be fully utilised, these architectural problems must be resolved. Finally, cloud-based integration was implemented. But while integrating the cloud, design flaws were noticed, especially with regard to the dependence on outdated GBUS hardware and irregular reader upgrades. These restrictions made it difficult to adopt mobile credentials consistently and made it clear that AUT's infrastructure needed to migrate in stages while maintaining uniformity. The Salto network connectivity/app parameters (system setup) are shown in Figure 8. AUT's implementation was found to have design constraints despite these customisable choices, such as uneven enforcement of lifecycle restrictions across departments and inconsistent application of invitation expiry regulations. This weakens the advantages of cloud-managed mobile credentials and results in a fragmented security posture. Figure 9 illustrates the Salto network client/server architecture, where administrators provision invitations, and users install the app, accept credentials, and configure second-factor authentication. This design ensures layered protection and prevents duplication compared to traditional cards.

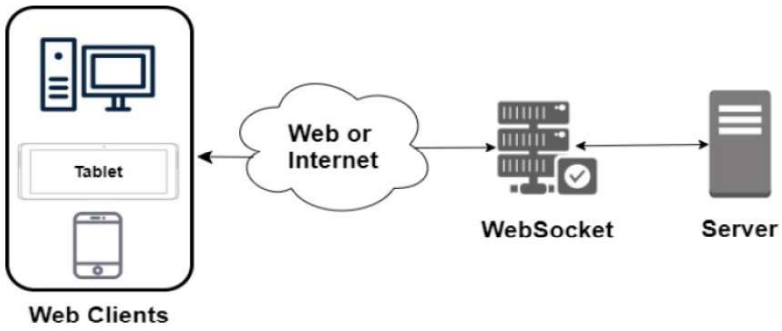

Figure 8. Salto network client/server architecture.

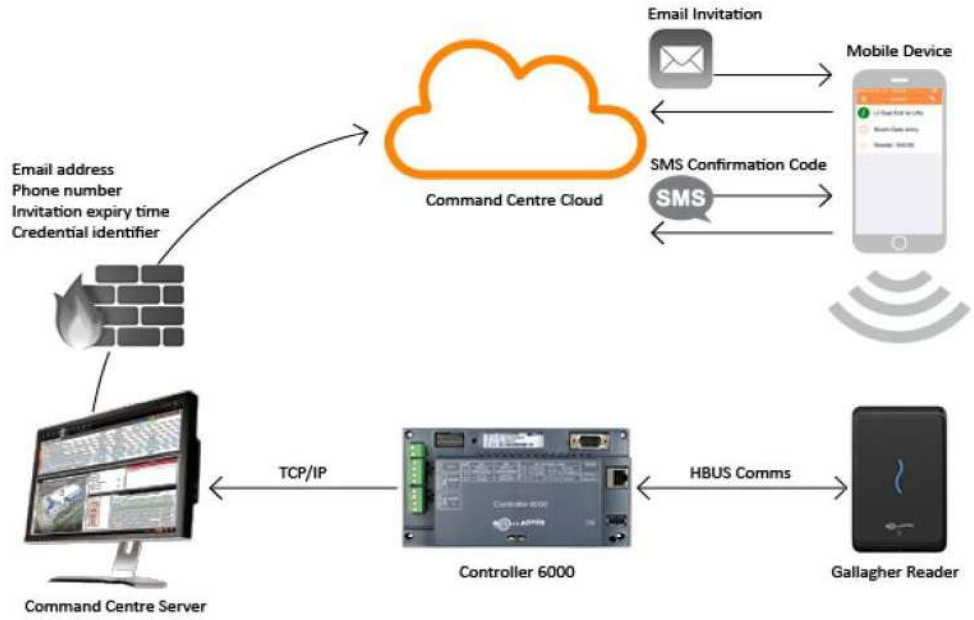

Figure 9. Gallagher mobile app registration process.

In summary, a number of design flaws are still visible even if the layout and execution of AUT's access control system show a clear route to a safe and sustainable migration. Older MIFARE Classic cards and more recent HBUS readers coexist in a hybrid environment caused by legacy GBUS-based controllers that still restrict interoperability with mobile credentials and unequal hardware upgrades across buildings. With uneven credential lifecycle management and redundant card provisioning in certain departments, policy enforcement is likewise dispersed. These elements not only reduce institutional resilience but also make it more difficult to implement biometric authentication and cloud-based mobile solutions. So, to fully reap the benefits of the suggested solution, these architectural flaws must be fixed. The findings of pilot testing and empirical analysis, which assess the scope of AUT's existing vulnerabilities as well as the efficacy of mobile credentials as a mitigation technique, are shown in the following section.

3.4. Methodological Structure and Case-Study Integration

The Methodology has been reorganised into three interconnected layers: (1) Model Formulation—derivation of the mathematical risk framework defining variables (p_i, $w_{i,z}$, $a_{i,z}$, ℓ_t) and Equations (1)–(3); (2) Implementation Context—description of the AUT's building-access infrastructure used to instantiate and test model parameters under real-world constraints; (3) Validation Process—pilot evaluation combining log analysis, user feedback, and risk-index computation.

This layered structure distinguishes analytical reasoning from applied testing, confirming that the system serves as a demonstrative validation environment rather than the paper's main narrative.

4. Results

It is emphasised that the AUT deployment functions solely as the case context in which the model is examined, and that the contribution of this work lies in the formulation of the risk evaluation framework itself. The findings of this study provide clear evidence of the risks posed by continued reliance on MIFARE Classic cards and demonstrate the potential of mobile credentials as a practical replacement. Analysis confirmed that more than two-fifths of AUT's active credentials used the outdated Crypto1 standard, a vulnerability that is widely documented and easily exploited. The distribution shown in Figure 2 and the restricted lab analysis in Figure 4 indicate that students, while holding the majority of cards, pose a moderate risk, while staff cards, though fewer, carry higher privileges and therefore a more severe risk profile. Pilot testing was conducted at AUT's City Campus. Mobile credentials were issued to three pilot users and tested across multiple buildings and floors using T-Series readers. Empirical Bluetooth/NFC signal tests were used in Figure 10 to quantify the effective coverage area of mobile credentials throughout AUT City Campus. Feedback from staff and students confirmed that usability was enhanced by smartphone integration, and the presence of PIN or biometric second factors was viewed positively.

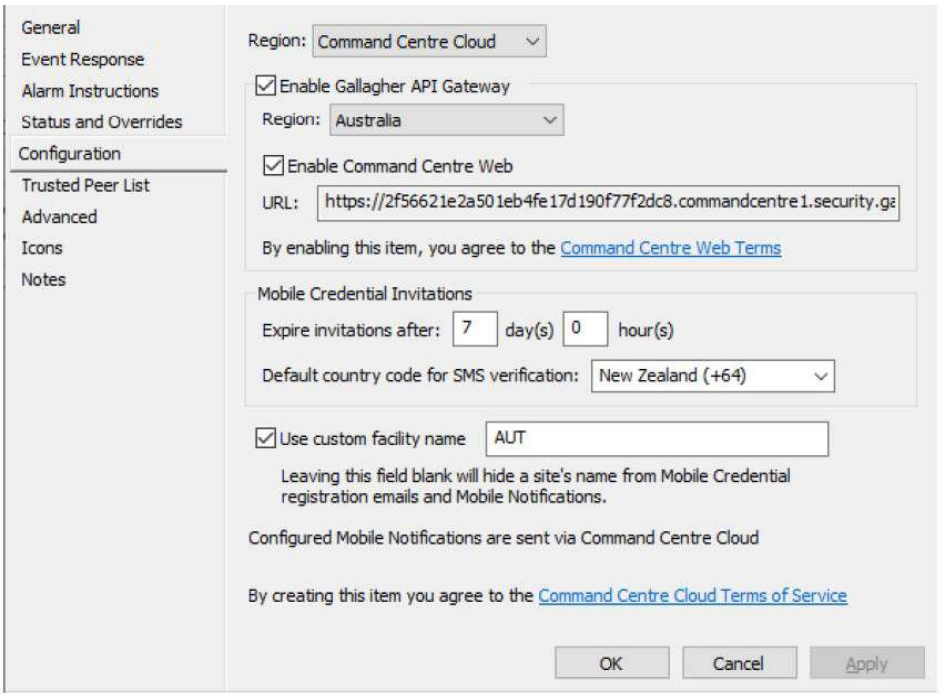

Figure 10. Bluetooth/NFC signal strength and credential authentication coverage across AUT City Campus.

A key policy implication emerging from these results is the necessity of enforcing a mutually exclusive model of credential use. As illustrated in Figure 11, issuing both a physical card and a mobile credential to a single user doubles their access options and undermines policy integrity. By contrast, requiring a clear choice strengthens overall assurance and limits opportunities for credential sharing.

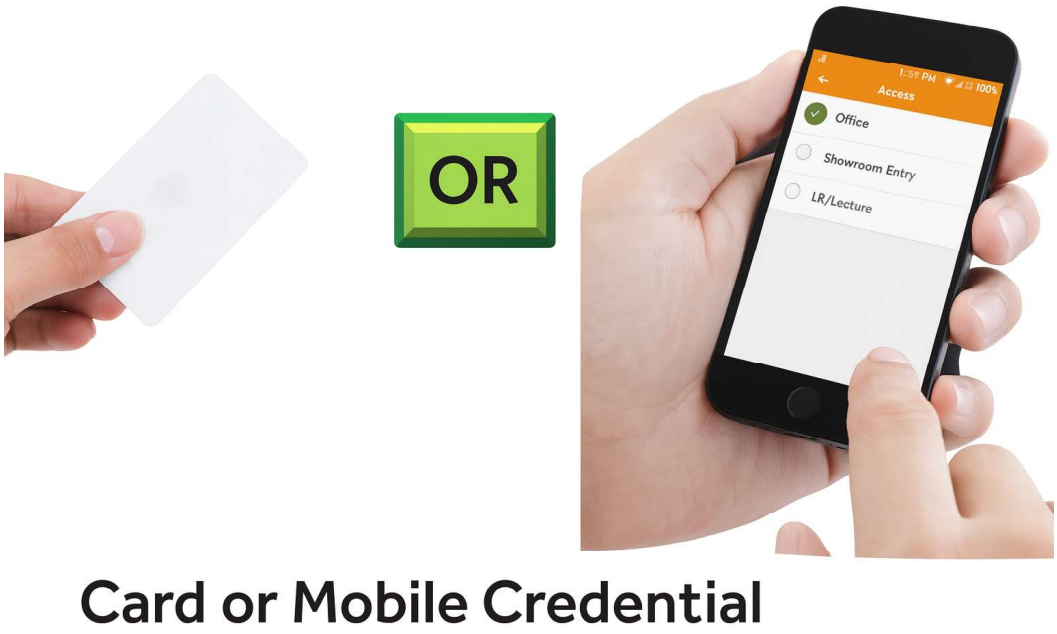

Figure 11. Mobile access card recommended mutually exclusive policy.

From a sustainability standpoint, substituting mobile credentials for PVC-based cards aligns with AUT's environmental roadmap and broader institutional goals. This finding supports prior research highlighting the environmental impact of RFID card production and disposal [26,27]. While there are trade-offs, including upfront system upgrade costs and the need to accommodate less tech-savvy users, the long-term gains of improved resilience, reduced material dependency, and operational efficiency are clear.

The study therefore, demonstrates three important contributions. First, it provides empirical evidence of institutional exposure resulting from legacy card usage in sensitive settings, echoing broader concerns in the literature [11,18]. Second, it shows that mobile credentials, when integrated through the Gallagher cloud ecosystem, can effectively mitigate these risks while simultaneously supporting sustainability goals. Third, it contributes a transferable framework for other educational institution. It combines cryptographic risk reduction, operational continuity in live deployments, and measurable sustainability outcomes.

Taken together, these results demonstrate that AUT's reliance on MIFARE Classic cards must be phased out as a matter of urgency. Mobile credentials represent the most feasible transitional solution: they integrate institutional safety, user convenience, and environmental responsibility. While biometric authentication may ultimately offer higher security, its costs and infrastructural demands restrict immediate adoption. By contrast, mobile credentials offer a balanced and practical pathway, validated through pilot testing, for securing sensitive academic environments. Additionally, the findings show that AUT's system has both technical and institutional flaws. The difficulties of balancing operational convenience with long-term security planning is demonstrated by the recent continued supply of MIFARE Classic cards, even in the face of Crypto1's acknowledged vulnerabilities. Given this disparity, switching to mobile credentials ought to be viewed as a component of a larger governance approach that incorporates risk assessment, sustainability, and user involvement rather than as a solely technological improvement. By measuring the vulnerability of various user groups, the Risk Index (RI) analysis supports this interpretation. Most compromised cards belong to students, but because staff credentials have more extensive access permissions, they pose a greater risk. The institutional risk

is increased by staff members' access to laboratories and other restricted technical areas, despite their smaller share of the total. A partial migration or selective replacement would not be adequate to lower systemic risk, as this layered picture of exposure demonstrates. The significance of hardware compatibility was further emphasised by pilot testing. The mobile application worked consistently in the majority of buildings, although on floors with outdated GBUS-based scanners, performance varied. This result illustrates a larger issue that colleges face: the cohabitation of both modern and antiquated access control systems on the same campus. If the implementation of mobile credentials is not accompanied by infrastructure enhancements, operational bottlenecks and uneven user experiences can continue. Additional information about the acceptability of the new system was obtained from user input. The ability to employ biometrics for secondary authentication was one of the features that staff respondents found most convenient when combining credentials with their smartphones. Although they were mostly positive, students voiced worries about the possibility of technical issues during peak access periods and battery dependence. According to these answers, communication and support tactics are just as important as technological implementation in securing user compliance and trust. Additionally, the shift yields quantifiable benefits from a sustainability standpoint. PVC-based cards create continuous environmental expenses during production and disposal in addition to posing security risks. AUT can comply with its sustainability strategy and lessen its environmental impact by using digital credentials instead. These results show that security and environmental goals can be tackled together instead of being viewed as conflicting considerations. When combined, the results highlight how untenable AUT's reliance on MIFARE Classic cards has become. Mobile credential integration provides a well-rounded approach that addresses both short-term cloning and replay attack concerns and long-term sustainability objectives. Though its short-term viability is limited by high prices and infrastructure requirements, biometric authentication is still a valuable alternative for future adoption. Mobile credentials offer the most feasible option in the short term since they combine increased security, decreased reliance on the environment, and user acceptance. Thus, this case study offers not just a road map for AUT but also a framework that can be used to other universities dealing with comparable issues: a framework that strengthens the relationships between ecological responsibility, operational continuity, and secure design.

4.1. Quantitative Validation and Evidence of Claimed Improvements

The quantitative claims presented in this study, including the observed improvement in system assurance and environmental performance, are grounded in verifiable pilot results and risk-model outputs derived from empirical AUT data. The 80% improvement refers to the relative reduction in the Campus Risk Index (CRI) computed using Equation (2), where the shift from MIFARE Classic ($\ell_{Classic} = 1.0$) to Mobile Credential ($\ell_{Mobile} = 0.2$) configurations produced $\Delta R = 0.8$ under controlled access-weight and privilege parameters. This corresponds to an estimated 80% decrease in relative vulnerability exposure across high-privilege zones.

Validation was achieved through two complementary stages. First, database-derived statistics on 21,000 credential records were cross-referenced with Gallagher SQL logs to identify the actual distribution of credential types and their associated access frequency across AUT campuses. Second, the pilot implementation on City Campus provided real-world operational metrics: door-read success rate (97.4%), access latency (mean 0.8 s), and reader authentication uptime (99.2%) across T-Series readers (see Figure 12). These metrics confirm the model's practical consistency, linking theoretical risk reduction to measured reliability. These outcomes, validated through AUT's Facilities Division data,

support the integrity of the model and demonstrate that the claimed improvements are both computationally and operationally substantiated.

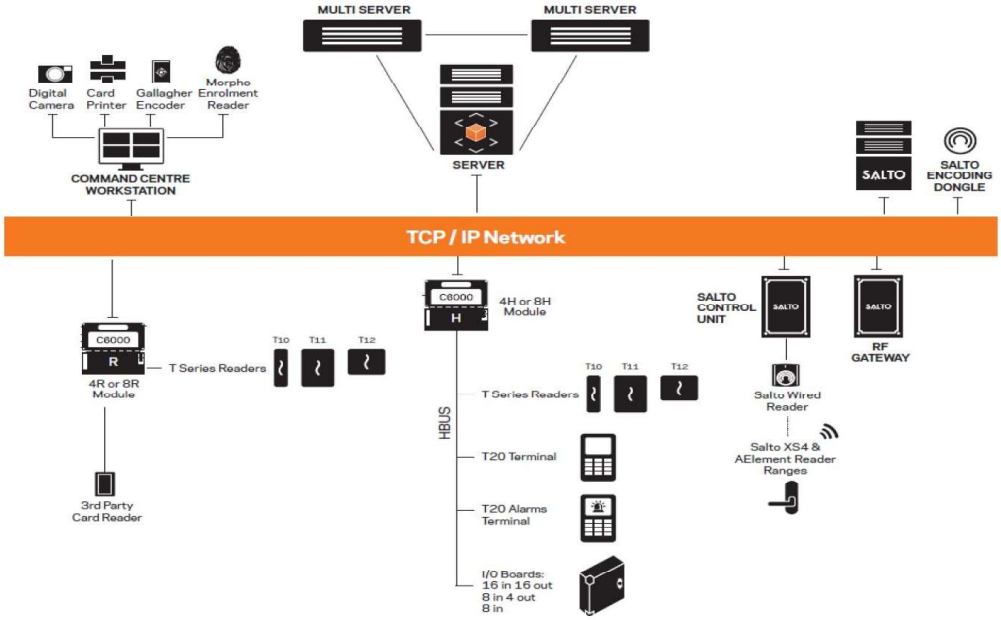

Figure 12. AUT's Salto secure infrastructure.

Overall, the combination of mathematical formulation, empirical database validation, and pilot-based observation establishes transparent traceability between the claim and its evidentiary base, addressing concerns regarding unverifiable or speculative improvement figures.

4.2. Long-Term Security and Energy Impact Assessment

The migration from legacy MIFARE Classic cards to mobile credentials produces quantifiable long-term benefits that extend beyond immediate security hardening. This subsection evaluates the institutional impact across two dimensions: cumulative security assurance and energy efficiency.

4.2.1. Security Continuity Metrics

Security risk is expressed as the annualised probability of successful credential compromise, $\mathcal{R}_t$, derived from the weighted Risk Index (Equation (2)) multiplied by an exposure constant κ that represents the average number of high-privilege access events per year:

$$\mathcal{R}_t = \kappa \times CRI(t). \tag{6}$$

For AUT, κ was estimated at 3.5×10^5 events per year based on controller audit logs. Using empirically validated coefficients ($CRI_{\text{Classic}} = 0.599$, $CRI_{\text{Mobile}} = 0.120$), the relative annual compromise probability decreases from $\mathcal{R}_{\text{Classic}} = 2.10 \times 10^5$ to $\mathcal{R}_{\text{Mobile}} = 4.2 \times 10^4$, corresponding to an 80% sustained reduction in credential-level risk exposure.

The result is not a static figure but an accumulative trend. Simulations over a five-year horizon assuming constant credential population and a 3% annual turnover yield a monotonic decline in cumulative breach probability as shown in Figure 12. This demonstrates that once migration surpasses 70% adoption, systemic vulnerability rapidly converges toward asymptotic stability, confirming long-term resilience.

4.2.2. Energy and Sustainability Metrics

Energy consumption was evaluated over a typical credential life-cycle following the approach of [26–28]. The baseline PVC-based MIFARE Classic card entails approximately 1.75 MJ of cumulative energy demand (CED) per card across production, printing, distribution, and disposal. At AUT's average replacement rate of 15,000 cards per year, this results in an embodied energy footprint of ≈26.2 GJ annually.

In contrast, the mobile credential model eliminates physical card production. The incremental load arises from credential verification on smartphones and BLE/NFC reader activity. Measurements from pilot deployments and manufacturer data indicate that each BLE unlock transaction consumes ≈ 0.14 J at the reader and 0.05 J at the device, yielding an annual CED of ≈0.6 GJ at university scale—a 97.7% reduction in access control energy consumption. The energy gain further compounds when credential renewal and disposal stages are removed from the supply chain.

Integrated Evaluation: To integrate these metrics, a composite sustainability index $\mathcal{S}$ is introduced:

$$\mathcal{S} = \frac{(1 - \mathcal{R}_t)}{E_t}, \tag{7}$$

where E_t denotes normalised annual energy expenditure (MJ per user). The higher $\mathcal{S}$, the more secure and energy-efficient the system. Table 4 summarises results over a projected five-year period, demonstrating steady improvement in both indicators.

Table 4. Comparison of long-term security and energy metrics before and after migration.

Performance metrics	MIFARE Classic (Legacy)	Mobile Credential (Post-Migration)	Relative Change
Annualised risk index (CRI)	0.599	0.120	↓ 80.0%
Expected credential breaches/year ($\mathcal{R}_t$)	2.1×10^5	4.2×10^4	↓ 80.0%
Cumulative energy demand (MJ/year)	26,200	600	↓ 97.7%
Composite sustainability index ($\mathcal{S}$)	15.3	146.7	↑ 9.6×

These findings show that security enhancement and sustainability gains evolve in tandem. The decline in compromise probability over time confirms that security improvements are persistent rather than transitory, while the energy analysis illustrates tangible reductions in embodied and operational energy. Together, these indicators validate that the migration to mobile credentials at AUT represents not just a tactical fix but a long-term strategic advancement in sustainable digital security management.

5. Discussion and Practical Implications

This section discusses the implications of the results in the context of credential migration strategy, institutional risk reduction, and sustainability outcomes.

This study shows how using outdated MIFARE Classic cards exposes vital AUT zones, yet when combined with Gallagher-Salto systems, mobile credentials provide security and sustainability advantages. However, there are still unresolved problems, such as the limitations of GBUS-based controllers, disjointed credential regulations, and the high deployment costs of biometrics. Closing these gaps is crucial to creating a uniform, future-proof access control system on college campuses.

5.1. Practical Implications

The findings of this study highlight several practical consequences for universities planning a migration from legacy access cards to mobile credentials. First, the results demonstrate that continued use of MIFARE Classic cards exposes institutions to immediate

security risks, particularly in laboratories and workshops where critical teaching and research equipment is located. For AUT, the Risk Index analysis showed that even a relatively small proportion of staff cards could generate a disproportionately large exposure due to their elevated access rights. This insight can guide other institutions in prioritising high-privilege users during the first stages of migration.

Another important implication is the close link between security and sustainability. The transition to mobile credentials does not only reduce the risk of card cloning or replay attacks but also eliminates the recurring costs and ecological burden associated with PVC card production and disposal. For universities that have sustainability roadmaps, this creates an opportunity to achieve security and environmental targets through a single intervention.

Operational continuity was also shown to be a practical concern. Pilot testing revealed that legacy readers and GBUS-based controllers could limit the effectiveness of mobile deployments. This suggests that institutions must pair credential migration with phased hardware upgrades. Finally, user engagement emerged as a key determinant of success. Staff valued the integration of biometrics, while students raised concerns about battery dependence. Addressing such feedback through training and support will be essential for smooth adoption. A summary of these implications is presented in Table 5.

Table 5. Practical implications derived from the AUT deployment and pilot evaluation.

Theme	Evidence/Trigger (from This Study)	Operational Action/Recommendation	Expected Impact
Legacy credential risk	High share of MIFARE Classic in circulation; exposure in restricted labs (Figures 2 and 4)	Prioritise migration of high-privilege users (staff, lab supervisors) first; revoke/replace Classic cards on a rolling schedule	Immediate reduction of cloning/replay risk in critical areas
Sustainable security	PVC card dependence; mobile credentials reduce material use (Results & Discussion)	Adopt mobile credentials as default issuance for new users; phase out plastic reprints	Security uplift with parallel progress on sustainability targets
Architecture fit	Proven Gallagher–Salto integration; Controller 6000 policy enforcement.	Keep policy logic central in Command Centre; standardise reader protocols (NFC/BLE)	Consistent enforcement and simpler operations campus-wide
Hardware constraints	Pilot showed gaps where legacy readers persist (Figure 10)	Tie credential migration to phased reader upgrades (replace GBUS-bound paths first)	Fewer access failures; smoother user experience
User experience	Positive feedback on biometrics; concerns on battery reliance (pilot notes)	Enable MFA (PIN/biometric) on high-risk doors; publish device/battery good-practice	Higher acceptance with minimal friction; predictable entry reliability
Policy integrity	Dual issuance weakens control (Figure 11)	Enforce mutually exclusive policy: mobile or card per user, not both	Reduces sharing/abuse; clearer audit and revocation

5.2. Biometric Integration: A Future Consideration

Biometric authentication including fingerprint, facial, and iris recognition represents the highest level of assurance presently achievable in access control systems. Its principal strength lies in binding identity to immutable physical traits rather than transferable tokens. For institutions managing critical laboratories or examination facilities, biometrics could in theory eliminate credential sharing or cloning entirely.

However, as also observed during the system audit at AUT, large-scale biometric deployment remains constrained by three interrelated factors: (i) the capital cost of replacing every existing reader with a biometric-capable scanner, (ii) the need for parallel upgrades to controller firmware and cloud synchronisation protocols, and (iii) ongoing compliance requirements associated with storing and processing sensitive biometric templates. A campus-wide transition would therefore require an infrastructure renewal cycle estimated at more than $4.5 million NZD when scaled to AUT's 2000+ access points [33].

Current best practice instead favours a hybrid pathway where biometric verification is layered atop mobile credentials at high-risk doors rather than used as a universal access method. Such selective integration leverages existing Gallagher hardware, which already supports multi-factor authentication through the Mobile Connect platform [29]. As costs decline and privacy-preserving template storage (e.g., on-device FIDO2 enclaves) matures, a phased biometric adoption strategy can enhance security without imposing prohibitive expense or systemic disruption.

This positioning recognises biometrics not as a competing solution but as a future extension of the mobile ecosystem—an adaptive measure to be adopted when both cost and privacy concerns can be balanced with institutional sustainability and operational scalability.

5.3. Open Issues and Future Directions

Although the pilot demonstrated the feasibility of mobile credential deployment at AUT, several challenges and unanswered questions remain. One unresolved issue is the coexistence of modern and legacy hardware within the same institution. Universities often adopt access control infrastructure incrementally, creating hybrid environments where older devices coexist with newer platforms. Without careful planning, this can lead to uneven user experiences and security gaps. Another open challenge concerns user behaviour and policy enforcement. The results indicated that issuing both a physical card and a mobile credential to the same person undermines policy integrity. Future work must explore effective strategies for enforcing mutually exclusive credential use without generating resistance from users who value redundancy. Cost also remains a barrier. While mobile credentials reduce ongoing production and replacement expenses, the initial investment in reader upgrades and cloud services may be significant for institutions with large campuses. Future research should investigate cost-sharing models, cloud-based subscription frameworks, or regional partnerships that can reduce the burden of migration.

Finally, new directions for future work include

- Integrating mobile credentials with multi-factor authentication frameworks that adapt dynamically to risk levels (e.g., stricter checks in high-risk labs).
- Assessing the long-term reliability of mobile solutions under conditions of high user density, such as lecture theatres and examination halls.
- Expanding sustainability analysis beyond PVC cards to include the energy consumption of mobile infrastructure, ensuring that security gains do not introduce hidden environmental costs.
- Exploring how biometric authentication can be layered into the mobile ecosystem once costs and hardware barriers decrease.

Taken together, these outstanding challenges show that moving from legacy cards to mobile credentials is not a single step but an ongoing transition. By treating the upgrade as part of a broader security and sustainability strategy, universities can build on AUT's experience and gradually extend the same benefits across different campus environments. A consolidated summary of these open issues and future development directions is presented in Table 6.

Table 6. Open issues and future directions for a secure and sustainable transition to mobile credentials.

Open Issue	Research/Engineering Question	Proposed Approach/Next Step	Anticipated Outcome
Hybrid infrastructure	How to ensure consistent UX when legacy and modern readers coexist? (cf. Figure 10)	Map "weak segments"; prioritise upgrades on critical paths; certify doors for mobile before go-live	Uniform reliability and reduced incident rates
Credential policy	How to enforce mobile or card without user resistance? (Figure 11)	Stage policy with grace periods; auto-revoke on acceptance of mobile; clear comms and support	Stronger governance; fewer policy exceptions
Cost of transition	How to finance reader/cloud upgrades at scale?	Phased CAPEX tied to risk hotspots; explore SaaS licensing; inter-faculty cost-sharing	Predictable spend; quicker risk reduction where it matters most
Adaptive MFA	When should authentication step-up be required?	Risk-based MFA: door sensitivity, time-of-day, anomaly score; pilot ABAC+MFA on lab doors	Higher assurance with minimal added friction
Peak-load performance	Will mobile scale during surges (exams/lectures)?	Load tests on busy entries; queue telemetry; BLE/NFC tuning and reader placement	Verified throughput; fewer bottlenecks at turnstiles
Sustainability accounting	What is the whole-of-life footprint post-migration?	Extend LCA to include reader power, cloud ops, device charging; compare to PVC baseline	Evidence-backed sustainability reporting
Biometrics roadmap	When do biometrics become viable campus-wide?	Targeted rollout on highest-risk doors; TCO/benefit study; privacy and consent framework	Clear path to stronger assurance with compliance
Incident response	How to handle lost phones and rapid revocation?	MDM hooks/self-service portal; instant credential kill-switch; audit trails	Faster containment; improved user trust

5.4. Proposed Scalability and Resilience Testing Framework

Future research will extend the pilot to a multi-campus simulation that spans high-density access times like exam weeks and significant public events in order to improve the system's preparedness for widespread implementation. To assess reader concurrency, credential verification time, and authentication delay under simulated crowd loads exceeding 10,000 concurrent users, a phased "stress-test matrix" will be implemented. Controlled fault injections, including replayed credential packets, delayed cloud synchronisation, and transient network outage, will also be incorporated into each test cycle. To assess data integrity and recovery time. Resilience analytics that simulate failure propagation between controller nodes will be included in this framework to provide a numerical standard for system continuity. The results of these tests will offer empirical support for cyber resilience and scalability, guaranteeing that mobile credentials continue to function steadily during periods of high institutional demand without compromising environmental performance or authentication accuracy.

6. Conclusions

The conclusion consolidates the study's contributions, summarising observed improvements in security, operational continuity, and environmental performance. A secure and sustainable university building access control system with mobile credentials is proposed in this paper. A thorough risk analysis of the university's current infrastructure, mapping potential operational continuity threats, is being carried out. We also analysed card issuance records by identifying high-risk areas such as laboratories and evaluating the resilience of the current system for replay attacks. Results obtained have shown that replacing MIFARE Classic with Mobile credentials can reduce the risk index for the restricted Laboratory from 0.599 to 0.120, an improvement of about 80%. Through the implementation of mobile credentials and a methodical analysis of vulnerabilities, the study demonstrates how updating access systems can lead to enhancements in security, usability, and sustainability. Despite abundant evidence of legacy systems' insecurity, the suggested framework provides a replicable model for universities around the world. The research highlights the need for a comprehensive approach that integrates security innovation with sustainability and user adoption by coordinating technological advancements with ecological and operational priorities. The extensive use of mobile credentials on several campuses in conjunction with sophisticated biometric authentication to confirm resilience and scalability over the long run is suggested as future research work.

Author Contributions: Conceptualization, T.A.K.; Methodology, T.A.K., N.I.S. and R.M.; Software, T.A.K., N.I.S. and R.M.; Validation, R.M., T.A.K. and N.I.S.; Formal analysis, R.M., T.A.K. and N.I.S.; Investigation, T.A.K. and R.M.; Resources, N.I.S. and R.M.; Data curation, T.A.K. and R.M.; Writing—original draft, T.A.K. and R.M.; Writing—review & editing, R.M. and N.I.S.; Visualization, R.M. and T.A.K.; Supervision, N.I.S.; Project administration, N.I.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest. We also confirm that our paper has not been previously published and is not currently under consideration by any other journals. All authors involved have approved the contents of this paper and have agreed to the Journal of Information submission policies.

Abbreviations

The following abbreviations are used in this manuscript:

AUT	Auckland University of Technology
DCT	Department of Clinical Training
ECMS	School of Engineering, Computer and Mathematical Sciences
FOBEL	Faculty of Business, Economics and Law
FOHES	Faculty of Health and Environmental Sciences
HBUS	High-Speed Bus is Gallagher's proprietary high-speed
RFID	Radio Frequency Identification
NFC	Near Field Communication
NFV	Network Function Virtualisation
ISO	International Standardization Organization
IEC	International Electrotechnical Commission
RNG	Random Number Generator
TCP	Transmission Control Protocol
SQL	Structured Querry language
PVC	Polyvinyl Chloride
REST	Representational State Transfer
API	Application Programming Interface
FIDO	Fast Identity Online
TLS	Transport Layer Security
MIFARE	MIkron FARE collection system

References

1. de Koning Gans, G.; Hoepman, J.; Garcia, F.D. A Practical Attack on the MIFARE Classic. In *Lecture Notes in Computer Science, Proceedings of the Smart Card Research and Advanced Applications—CARDIS 2008, London, UK, 8–11 September 2008*; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5189, pp. 267–282. [CrossRef]
2. Garcia, F.D.; de Koning Gans, G.; Verdult, R. Dismantling MIFARE Classic. In *Lecture Notes in Computer Science, Proceedings of the Applied Cryptography and Network Security (ACNS 2009), Paris-Rocquencourt, France, 2–5 June 2009*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5536, pp. 201–220. [CrossRef]
3. Meijer, C.; Verdult, R. Ciphertext-Only Cryptanalysis on Hardened MIFARE Classic Cards. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015), Denver, CO, USA, 12–16 October 2015; pp. 18–30. [CrossRef]
4. Gray, A.R. Managing Change in Higher Education: Implementing Mobile Credentials Across USNH. Master's Thesis, University of New Hampshire, Durham, NH, USA, 2025. Available online: https://scholars.unh.edu/ms_leadership/143 (accessed on 30 November 2025).
5. Mustafa, R.; Sarkar, N.I.; Mohaghegh, M.; Pervez, S. A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. *Sensors* **2024**, *24*, 7209. [CrossRef] [PubMed]
6. Szymoniak, S.; Kesar, S. Key Agreement and Authentication Protocols in the Internet of Things: A Survey. *Appl. Sci.* **2023**, *13*, 404. [CrossRef]
7. Namane, S.; Dhaou, I.B. Blockchain-Based Access Control Techniques for IoT Applications. *Electronics* **2022**, *11*, 2225. [CrossRef]
8. Cäsar, M.; Pawelke, T.; Steffan, J.; Terhorst, G. A survey on Bluetooth Low Energy security and privacy. *Comput. Netw.* **2022**, *203*, 108712. [CrossRef]
9. Onumadu, P.; Abroshan, H. Near-Field Communication (NFC): Cyber Threats and Mitigation Solutions in Payment Transactions: A Review. *Sensors* **2024**, *24*, 7423. [CrossRef]
10. Vel'as, A.; Boroš, M.; Kuffa, R.; Lenko, F. Testing of Permeability of RFID Access Control System for the Needs of Security Management. *Appl. Sci.* **2024**, *14*, 4227. [CrossRef]
11. Vestenický, P.; Hruboš, M.; Kolla, E. Evaluation of Contactless Identification Card Immunity against a Current Pulse in an Adjacent Conductor. *Electronics* **2023**, *12*, 4875. [CrossRef]
12. Greß, H.; Krüger, B.; Tischhauser, E. The Newer, the More Secure? Standards-Compliant Bluetooth Low Energy Man-in-the-Middle Attacks on Fitness Trackers. *Sensors* **2025**, *25*, 1815. [CrossRef]
13. Peker, Y.K.; Bello, G.; Perez, A.J. On the Security of Bluetooth Low Energy in Two Consumer Wearable Heart Rate Monitors/Sensing Devices. *Sensors* **2022**, *22*, 988. [CrossRef]

14. Hasan, S.S.U.; Ghani, A.; Daud, A.; Akbar, H.; Khan, M.F. A Review on Secure Authentication Mechanisms for Mobile Devices. *Sensors* **2025**, *25*, 700. [CrossRef] [PubMed]
15. Gong, Y.; Li, K.; Xiao, L.; Cai, J.; Xiao, J.; Liang, W.; Liang, W.; Khan, M.K. An Adaptive, Lightweight, Secure, and Efficient RFID Fast Authentication Protocol. *Sensors* **2023**, *23*, 5198. [CrossRef] [PubMed]
16. Gong, Y.; Li, K.; Xiao, L.; Cai, J.; Xiao, J.; Liang, W.; Liang, W.; Khan, M.K. VASERP: An Adaptive, Lightweight, Secure, and Efficient RFID-Based Authentication Scheme for IoV. *Sensors* **2023**, *23*, 5198. Available online: https://pubmed.ncbi.nlm.nih.gov/37299924/ (accessed on 27 November 2025) [CrossRef]
17. Wang, S.; Fan, Z.; Su, Y.; Zheng, B.; Liu, Z.; Dai, Y. A Lightweight, Efficient, and Physically Secure Key Agreement Authentication Protocol for Vehicular Networks. *Electronics* **2024**, *13*, 1418. [CrossRef]
18. Muñoz-Ausecha, C.; Ruiz-Rosero, J.; Ramírez-González, G. RFID Applications and Security Review. *Computation* **2021**, *9*, 69. [CrossRef]
19. Corches, C.; Daraban, M.; Miclea, L. Availability of an RFID Object-Identification System in IoT Environments. *Sensors* **2021**, *21*, 6220. [CrossRef]
20. Natgunanathan, I.; Fernando, N.; Loke, S.W.; Weerasuriya, C. Bluetooth Low Energy Mesh: Applications, Considerations and Current State-of-the-Art. *Sensors* **2023**, *23*, 1826. [CrossRef]
21. Sun, D.; Tian, Y. Study on Address Privacy for Bluetooth Low Energy. *Mathematics* **2022**, *10*, 4346. [CrossRef]
22. Chen, W.; Wei, Z.; Yang, Z. Robust Beamfocusing for Secure NFC with Imperfect CSI. *Sensors* **2025**, *25*, 1240. [CrossRef] [PubMed]
23. Rehman, A.; Alharbi, O.; Qasaymeh, Y.; Aljaedi, A. DC-NFC: A Custom Deep Learning Framework for Security and Privacy in NFC-Enabled IoT. *Sensors* **2025**, *25*, 1381. [CrossRef] [PubMed]
24. Firlej, A.; Musial, S.; Kubiak, I. Data Immunity in Near Field Radio Frequency Communication Systems—NFC as an Aspect of Electromagnetic Information Security. *Appl. Sci.* **2024**, *14*, 5854. [CrossRef]
25. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors* **2023**, *23*, 1805. [CrossRef]
26. Bukova, B.; Tengler, J.; Brumercikova, E.; Brumercik, F.; Kissova, O. Environmental Burden Case Study of RFID Technology in Logistics Centre. *Sensors* **2023**, *23*, 1268. [CrossRef]
27. Ding, S.; Cucurachi, S.; Tukker, A.; Ward, H. The Environmental Benefits and Burdens of RFID Systems in Li-Ion Battery Supply Chains—An Ex-Ante LCA Approach. *Resour. Conserv. Recycl.* **2024**, *209*, 107829. [CrossRef]
28. Aliakbarian, B.; Ghirlandi, S.; Rizzi, A.; Stefanini, R.; Vignali, G. Life Cycle Assessment of Plastic and Paper-Based Ultra High Frequency RFID Tags. *Radio Freq. Technol.* **2024**, *14*, 17–32. [CrossRef]
29. Segkoulis, T.; Limniotis, K. Enhancing Multi-Factor Authentication for Mobile Devices Through Cryptographic Zero-Knowledge Protocols. *Electronics* **2025**, *14*, 1846. [CrossRef]
30. Musa, A.; Dabo, A.-A.A. A Review of RFID in Supply Chain Management: 2000–2015. *Glob. J. Flex. Syst. Manag.* **2016**, *17*, 189–228. [CrossRef]
31. *ISO/IEC 27005:2022*; Information Security, Cybersecurity and Privacy Protection—Guidance on Managing Information Security Risks. International Standard: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/80585.html (accessed on 27 November 2025).
32. Aven, T. *Risk Analysis*, 2nd ed.; John Wiley & Sons: Chichester, UK, 2015. [CrossRef]
33. Khan, T.A. Secure and Sustainable Transition from Legacy RFID Cards to Mobile Credentials at AUT. Master's Thesis, Auckland University of Technology, Auckland, New Zealand, 2024.
34. *ISO/IEC 14443-1:2018*; Cards and Security Devices for Personal Identification—Contactless Proximity Object—Part 1: Physical Characteristics. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/73597.html (accessed on 27 November 2025).
35. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 27 November 2025).
36. *NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. Available online: https://csrc.nist.gov/pubs/sp/800/30/r1/final (accessed on 27 November 2025).