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

Rashid Mustafa , Toseef Khan , Nurul I. Sarkar *

Posted Date: 22 September 2025

doi: 10.20944/preprints202509.1740.v1

Keywords: university access control; mobile credentials; risk analysis; sustainable security; cloudbased integration; bluetooth low energy; near field communication

 doi:10.20944/preprints202509.1740.v1

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
* 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. But using old Mifare Classic credentials, which use antiquated Crypto1 encryption, leaves the system vulnerable to replay and cloning attacks. For laboratories, testing facilities, and technical areas that need stringent security measures, such flaws pose serious risks. 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

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

 doi:10.20944/preprints202509.1740.v1

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.

1.1. Research Challenges

The growing use of electronic access systems on college campuses presents a number of unsolved issues.

Firstly, what weaknesses are present in the current infrastructure for card-based access, and how do they jeopardise the security of the institution? Mifare Classic cards are still used at AUT despite their widespread use, despite the fact that their Crypto1 encryption has long since been cracked. As a result, technical areas, testing facilities, and labs are vulnerable to illegal access and credential cloning attacks. Understanding how such vulnerabilities convert into operational risks for a sizable and intricate organisation is just as difficult as determining the extent of exposure.

Secondly, What mitigation techniques can be created to supplement or replace compromised credentials while maintaining compatibility with current infrastructure? That is the second question. Universities have tens of thousands of users to serve and thousands of doors to secure. Gallagher's current security platform must be seamlessly integrated with any new strategy without interfering with day-to-day operations. The difficulty lies in identifying substitutes, like mobile login credentials, that can be implemented gradually while preserving a uniform security posture across several campuses.

Thirdly, What equilibrium can be struck between enhanced security, user convenience, and environmental sustainability? That is the third question. It may be possible to reduce waste and align with AUT's sustainability roadmap by moving away from plastic-based cards, but there are also issues with system costs, smartphone dependency, and user adoption. It is difficult to determine whether mobile credentials or other cutting-edge strategies can address threats, improve user experience, and support ecological responsibility all at once.

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 [1]. 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

 doi:10.20944/preprints202509.1740.v1

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.

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.

2. Related Work

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 [2]. 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 [3]. 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 [4]. 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. [5], 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. [6] 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. [7], 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. [8] 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 [9]. 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. [10] 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 [11]. 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. [12], which also identifies flaws and suggests solutions. Their research highlights the significance of RFID security across a range of fields, from identity management to

 doi:10.20944/preprints202509.1740.v1

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 [13]. 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 [14]. 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 [15]. 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 [16]. To improve NFC communications, this study presents DC-NFC, a security framework that blends dynamic contextual evaluation and deep learning [17]. Their method constantly adjusts to changing assault patterns and improves danger detection. To improve resilience against interference and ensure universal device compatibility, [18] investigates data immunity in near-field RFID communication. Their research suggests ways to keep data interchange secure and dependable in a variety of settings. 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 [19]. Strong protection and lightweight performance are difficult to balance, as the article points out. IoT access control models are surveyed in [20], 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. The advantages and implementation difficulties of [21] blockchain in protecting IoT systems are both highlighted in their survey. Reference [22] 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. [23] 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 [24]. 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 [25]. According to [26], 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. 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 [2–4] 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 [5–7] demonstrate the operational fragility of older card-based technologies, particularly in high-risk environments such as laboratories and research facilities (See Table1).

Recent works on **lightweight authentication protocols** [9–11] illustrate that efficient cryptographic designs can enable secure, low-latency access, though trade-offs between scalability and resource overhead remain. Broader reviews of **IoT access control models** reveal opportunities for dynamic, adaptive policies, with blockchain-based approaches offering decentralisation and auditability [19–

 doi:10.20944/preprints202509.1740.v1

21]. At the same time, **sustainability-focused research** [22–24] highlights the environmental cost of PVC-based cards, with life-cycle analyses demonstrating the advantages of mobile and paper-based alternatives. 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 25-papers listed below.

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

Ref.	Domain/Focus	Main Contribution / Relevance
[2]	BLE Security Survey	Maps BLE flaws and defences; foundation for secure mobile credential design.
[3]	NFC Threat Review	Systematic review of NFC attacks/mitigations; supports secure migration to mobile.
[4]	RFID System Reliability	Quantifies throughput/permeability in access control; informs door/mobile deployments.
[5]	Contactless Chip Immunity	Tests card chip performance under EMI; justifies replacing MIFARE Classic.
[6]	BLE Security Evolution	Assesses newer BLE devices; shows progress but persistent risks.
[7]	BLE Device Weaknesses	Empirical flaws in consumer BLE devices; relevance to PACS readers.
[8]	Mobile Authentication	Survey of MFA, biometrics, cryptographic methods; informs mobile credential policy.
[9]	Lightweight RFID Protocols	Reviews RFID auth protocols; categorises by scalability, overhead, security.
[10]	Fast RFID Authentication	New lightweight protocol; efficient against cloning/relay.
[11]	Key Agreement (IoV)	PUF+ECC protocol; shows resilience transferable to PACS.
[12]	RFID Applications	Broad survey of RFID uses/security; underscores legacy risks.
[13]	RFID Reliability	Models IoT RFID availability; relevant to continuous door operation.
[14]	Bluetooth Mesh	Surveys BLE Mesh uses, challenges; scalability insights for campus-wide access.
[15]	BLE Address Privacy	Analyzes randomization weaknesses; implications for mobile credential privacy.
[16]	NFC Physical Security	Robust beamfocusing to improve NFC resilience.
[17]	NFC + Deep Learning	Proposes DL-based DC-NFC; adaptive security for mobile apps.
[18]	Near-field RFID	Studies data immunity/interference; improves secure door placement.
[19]	IoT Protocols	Reviews auth/key-agreement; trade-offs in lightweight vs secure schemes.
[20]	IoT Access Control	Surveys AC models/policies; relevance to dynamic campus contexts.
[21]	Blockchain AC	Taxonomy of blockchain-based IoT access control.
[22]	RFID Sustainability	Case study of RFID in logistics; ecological trade-offs highlight plastic card waste.
[23]	RFID LCA	Ex-ante LCA of RFID; shows sustainability benefits and burdens.
[24]	UHF Tag Lifecycle	Compares paper vs plastic RFID tags; supports greener material transition.
[25]	Mobile MFA	Reviews contextual/biometric MFA; relevant for mobile credential security.
[26]	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.

 doi:10.20944/preprints202509.1740.v1

3.1. Mathematical Risk Model

For any questions, please let me know. As lab is just for practising the assignment activities. 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

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

which lies in $[0,1]$ when each factor is normalized.

The zone-level Risk Index (RI) is then calculated as:

$$RI_z(t) = \sum_{i \in C} p_i(t) \cdot w_{i,z} \cdot a_{i,z} \cdot \ell_t,$$

which remains bounded in $[0,1]$ when all

(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.

 doi:10.20944/preprints202509.1740.v1

Case 1: Classic Credentials. With Classic credentials (ℓ_{Classic}=1), the zone-level risk index is:

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

which is Equation (4).

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

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

which is Equation (5).

Interpretation. 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.

4. System Design and Implementation Issues

The design and implementation of this study followed a structured approach that combined risk analysis of existing systems with the introduction of mobile credential technologies. The primary focus was to identify institutional exposure caused by outdated MIFARE Classic cards and then to design a sustainable, secure, and practical migration pathway.

The initial phase involved mapping the distribution of access cards across AUT's user groups. As shown in Figure 1, students accounted for 73% of issued MIFARE Classic 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.

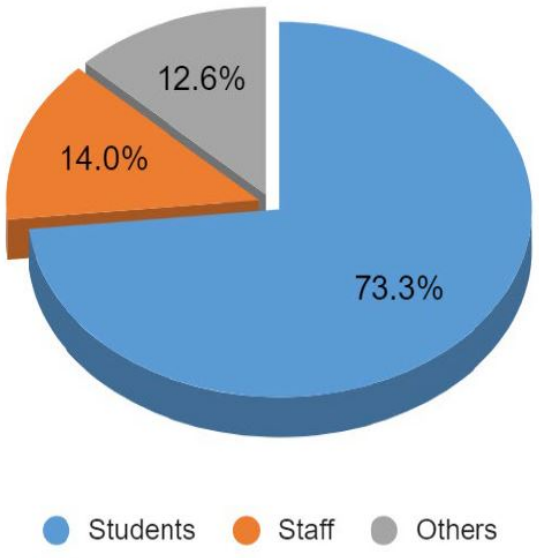

Figure 1. MIFARE Classic cards distribution at AUT.

 doi:10.20944/preprints202509.1740.v1

In the second phase, card issuance records were analysed by year. Figure 2 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.

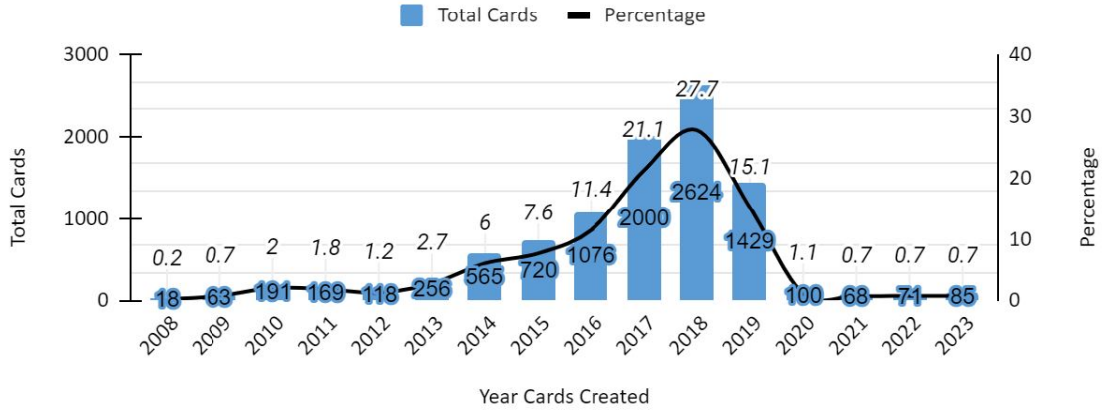

Figure 2. MIFARE cards created per year.

The implications of such continued use were further reinforced by examining restricted laboratory access. Figure 3 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.

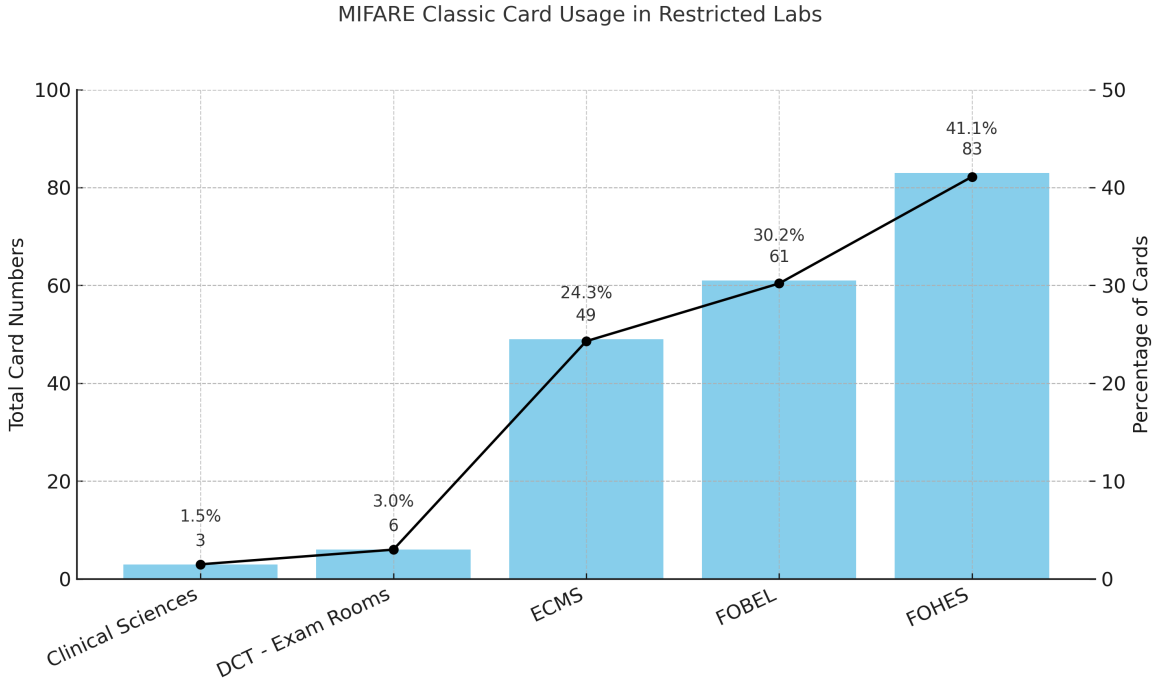

Figure 3. MIFARE Classic card usage in restricted Labs.

Two mitigation pathways were considered. The first was the adoption of mobile credentials. Figure 4 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

 doi:10.20944/preprints202509.1740.v1

with AUT's sustainability strategy, as the shift from PVC-based cards reduced material waste and reliance on plastic.

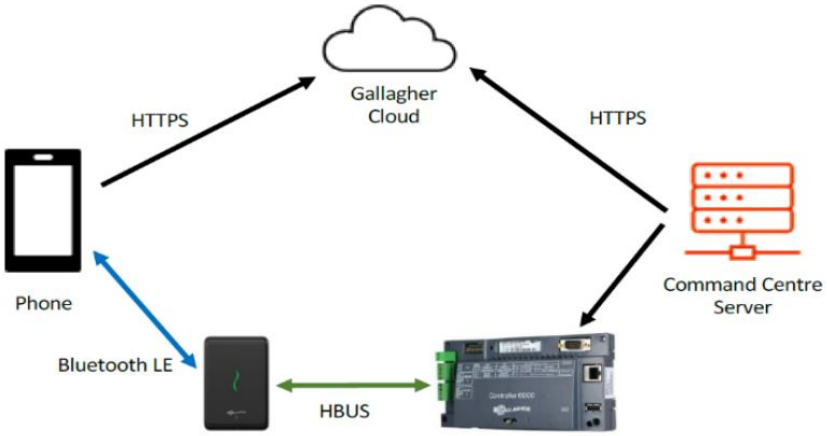

Figure 4. Mobile access overview.

The second pathway considered was biometric authentication. Figure 5 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.

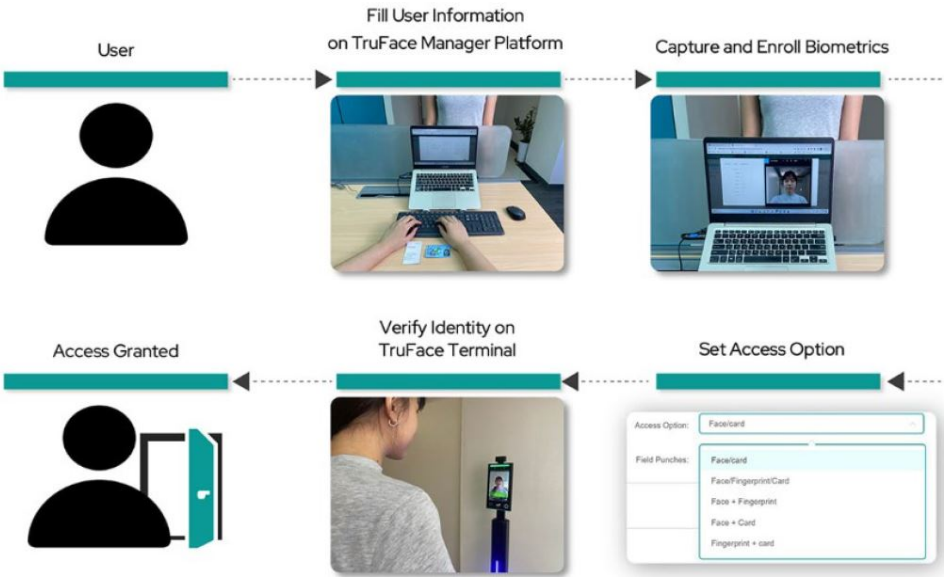

Figure 5. Biometric system workflow.

The Gallagher–Salto integration at AUT formed the backbone of system design. Figure 6 demonstrates how Gallagher Command Centre serves as the central policy engine, while Salto components extend access control to wireless environments where full cabling is not feasible. This hybrid architecture balances security with operational flexibility.

 doi:10.20944/preprints202509.1740.v1

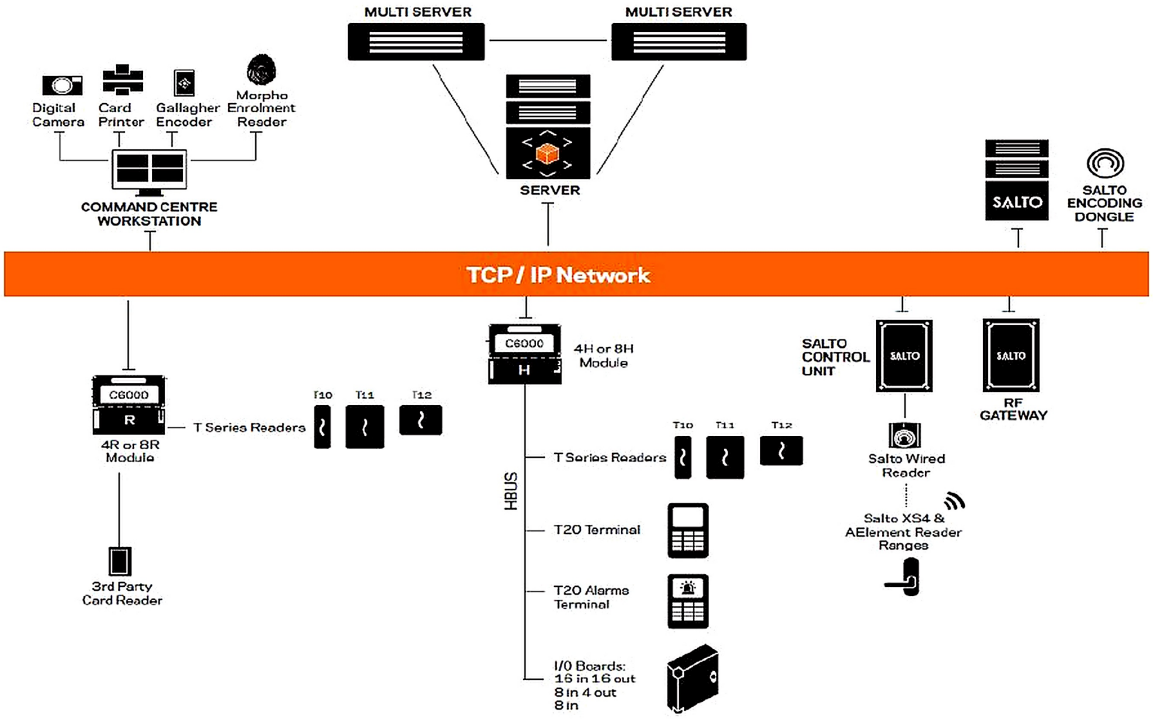

Figure 6. AUT building security design.

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.

The High-Security Controller 6000, depicted in Figure 7, provides real-time enforcement of institutional policies, while supporting multiple reader protocols. Reader configurations (Figure 8) were reviewed, with Bluetooth-capable devices identified as critical for mobile credential deployment.

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.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 September 2025 doi:10.20944/preprints202509.1740.v1

Salto wireless locks (Figure 9) were also highlighted for their sustainability benefits, consuming up to 65% less energy than fully wired systems.

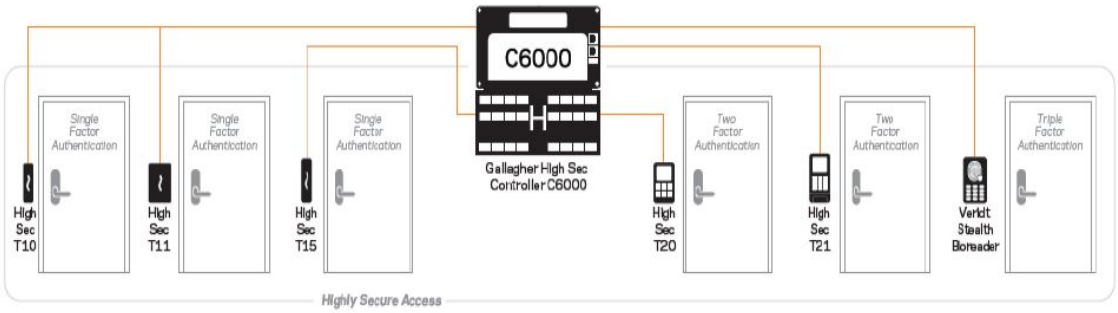

Figure 7. Doors connectivity with Controller 6000 and readers.

Figure 8. Security access card readers used at AUT.

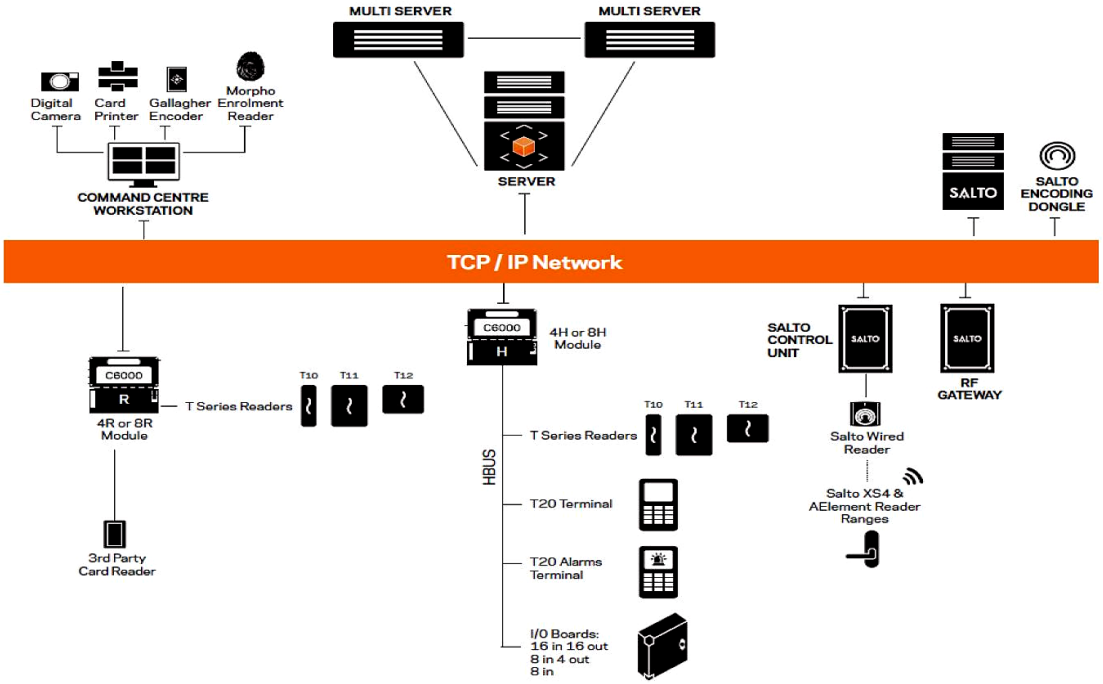

Figure 9. University Salto infrastructure.

Finally, cloud-based integration was implemented. The Gallagher Command Centre server was linked to Gallagher's cloud service via TLS-protected WebSocket protocols as shown in Figure 10.

 doi:10.20944/preprints202509.1740.v1

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. Figure 11 outlines the configurable parameters, including regional settings, credential lifecycle, and invitation expiry rules. 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 12 illustrates the mobile credential registration workflow, 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 10. Protocol between Command Centre & cloud (TLS over WebSocket).

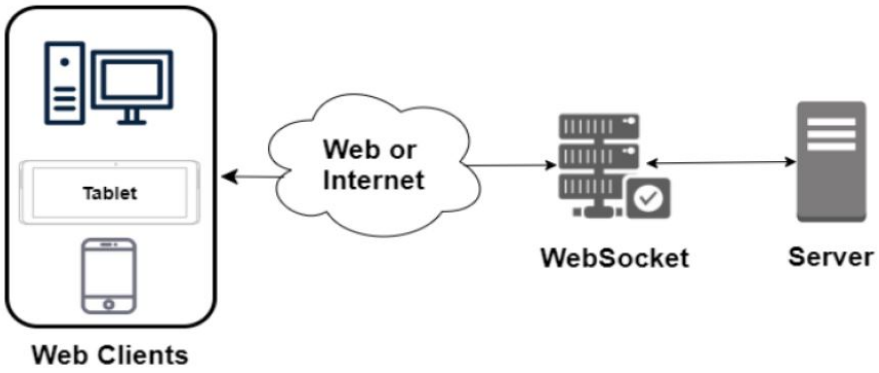

Figure 11. Gallagher mobile application parameters for deployment.

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.

 doi:10.20944/preprints202509.1740.v1

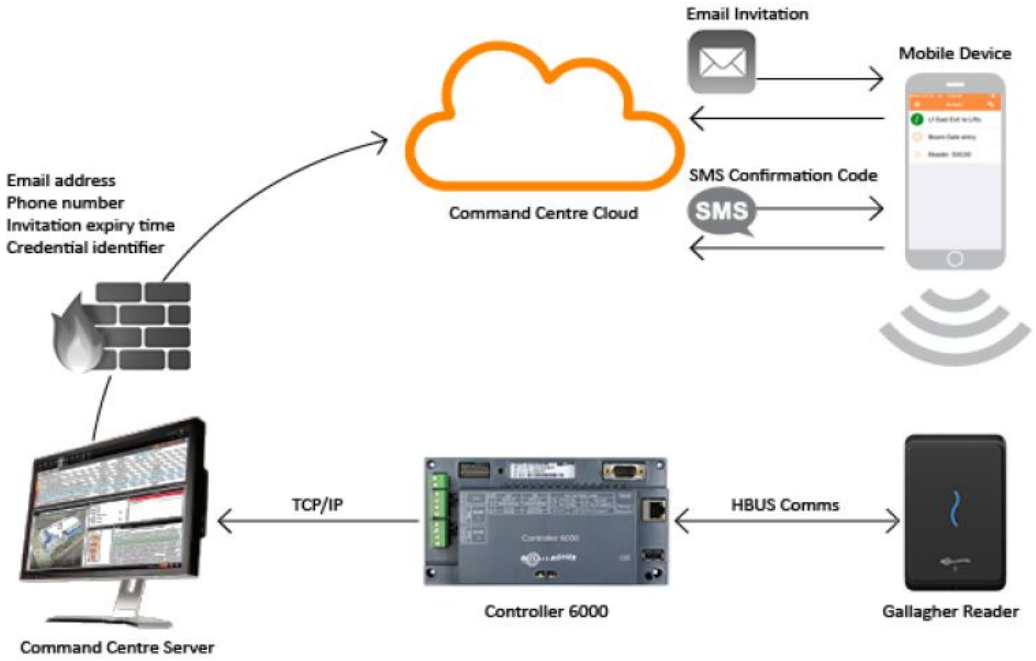

Figure 12. Gallagher mobile app registration process.

5. Results and Discussion

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 1 and the restricted lab analysis in Figure 3 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. Results confirmed high reliability in most areas, with minor failures observed in locations where legacy hardware persisted. Figure 13 illustrates the coverage of mobile credentials across the 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.

A key policy implication emerging from these results is the necessity of enforcing a mutually exclusive model of credential use. As illustrated in Figure 14, 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.

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 [22,23]. 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 [5,12]. 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 universities: one that combines (*i*) cryptographic risk reduction, (*ii*) operational continuity in live deployments, and (*iii*) measurable sustainability outcomes.

 doi:10.20944/preprints202509.1740.v1

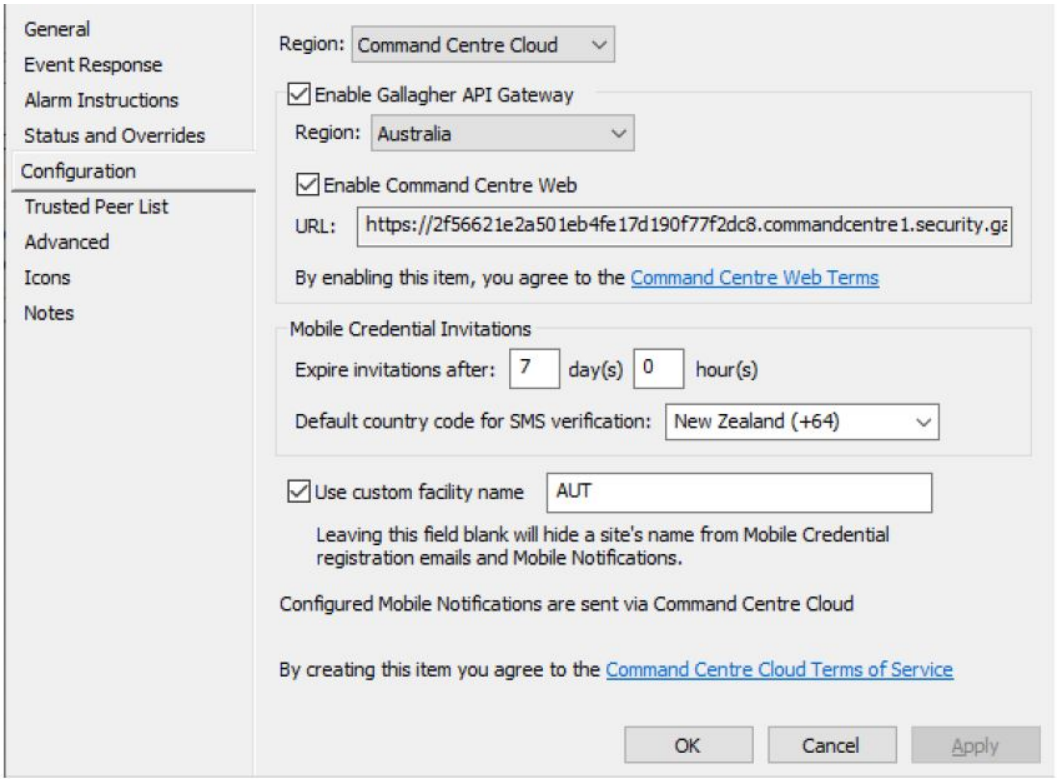

Figure 13. Mobile app test results in AUT City Campus.

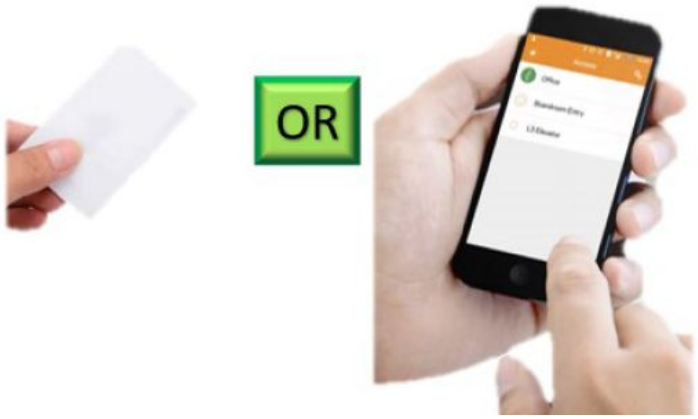

Figure 14. Access card *or* mobile app—recommended mutually exclusive policy.

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

 doi:10.20944/preprints202509.1740.v1

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 emphasized 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.

6. System Implications and Open Issues

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.

6.1. 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

 doi:10.20944/preprints202509.1740.v1

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.

Table 2. 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 (Figure 1, Figure 3)	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 (Figure 6, Figure 7)	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 13)	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 14)	Enforce mutually exclusive policy: *mobile or card* per user, not both	Reduces sharing/abuse; clearer audit and revocation

6.2. 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.

 doi:10.20944/preprints202509.1740.v1

When combined, these outstanding issues demonstrate that switching from traditional smart cards to mobile credentials is a continuous process rather than a one-time improvement; universities may expand and extend the advantages of AUT to other academic contexts by integrating the migration into a larger security and sustainability plan.

Table 3. 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 13)	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 14)	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

7. Conclusions

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.

 doi:10.20944/preprints202509.1740.v1

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. 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*. https://doi.org/10.3390/s24227209.
2. Cäsar, M.; Pawelke, T.; Steffan, J.; Terhorst, G. A survey on Bluetooth Low Energy security and privacy. *Computer Networks* **2022**, *203*, 108712. https://doi.org/10.1016/j.comnet.2021.108712.
3. Onumadu, I.; Abroshan, H. Near Field Communication (NFC): Cyber Threats and Mitigation—A Systematic Review. *Sensors* **2024**, *24*, 7423. https://doi.org/10.3390/s24237423.
4. Veľas, A.; Boroš, M.; Kuffa, R.; Lenko, F. Testing of Permeability of RFID Access Control System for Buildings. *Applied Sciences* **2024**, *14*, 4227. https://doi.org/10.3390/app14104227.
5. Vestenický, P.; Hruboš, M.; Kolla, E. Evaluation of Contactless Identification Card Chip Immunity to Electromagnetic Disturbance. *Electronics* **2023**, *12*, 4875. https://doi.org/10.3390/electronics12234875.
6. Greß, H.; Krüger, B.; Tischhauser, E. The Newer, the More Secure? Standards-Compliant BLE Devices as Exemplary Targets for Security in Early 2025. *Sensors* **2025**, *25*, 1815. https://doi.org/10.3390/s25061815.
7. Peker, Y.K.; Bello, G.; Perez, A.J. On the Security of BLE in Two Different Consumer Devices. *Sensors* **2022**, *22*, 988. https://doi.org/10.3390/s22030988.
8. 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. https://doi.org/10.3390/s25030700.
9. Mudra, G.; Cui, H.; Johnstone, M.N. Survey: An Overview of Lightweight RFID Authentication Protocols Suitable for the Maritime Internet of Things. *Electronics* **2023**, *12*, 2990. https://doi.org/10.3390/electronics12132990.
10. 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. https://doi.org/10.3390/s23115198.
11. Wang, S.; Fan, Z.; Su, Y.; Zheng, B.; Liu, Z.; Dai, Y. A Lightweight, Efficient, and Physically Secure Key Agreement Scheme for IoV. *Electronics* **2024**, *13*, 1418. https://doi.org/10.3390/electronics13081418.
12. Munoz-Ausecha, C.; Ruiz-Rosero, J.; Ramirez-Gonzalez, G. RFID Applications and Security Review. *Computation* **2021**, *9*, 69. https://doi.org/10.3390/computation9060069.
13. Corches, C.; Daraban, M.; Miclea, L. Availability of an RFID Object-Identification System in IoT. *Sensors* **2021**, *21*, 6220. https://doi.org/10.3390/s21186220.
14. 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. https://doi.org/10.3390/s23041826.

15. Sun, D.; Tian, Y. Study on Address Privacy for Bluetooth Low Energy. *Mathematics* **2022**, *10*, 4346. https://doi.org/10.3390/math10224346.
16. Chen, W.; Wei, Z.; Yang, Z. Robust Beamfocusing for Secure Near-Field Communications with Imperfect Channel State Information. *Sensors* **2025**, *25*, 1240. https://doi.org/10.3390/s25041240.
17. Rehman, A.; Alharbi, O.; Qasaymeh, Y.; Aljaedi, A. DC-NFC: Securing NFC with Deep Learning and Dynamic Contextual Evaluation. *Sensors* **2025**, *25*, 1381. https://doi.org/10.3390/s25051381.
18. Firlej, A.; Musial, S.; Kubiak, I. Data Immunity in Near Field RFID Communication for Universal Devices. *Applied Sciences* **2024**, *14*, 5854. https://doi.org/10.3390/app14135854.
19. Szymoniak, S.; Kesar, S. Key Agreement and Authentication Protocols in the Internet of Things: A Review. *Applied Sciences* **2022**, *13*, 404. https://doi.org/10.3390/app13010404.
20. Ragothaman, K.M.; Wang, Y.; Rimal, B.P.; researchgate.net, M.L. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors* **2023**, *23*, 1487. https://doi.org/https://doi.org/10.3390/s23041805.
21. Namane, S.; Dhaou, I.B. Blockchain-Based Access Control Techniques for IoT Systems: A Taxonomy. *Electronics* **2022**, *11*, 2225. https://doi.org/10.3390/electronics11142225.
22. Bukova, B.; Tengler, J.; Brumercikova, E.; Brumercik, F.; Kissova, O. Environmental Burden Case Study of RFID Technology in Logistics Centre. *Sensors* **2023**, *23*, 1268. https://doi.org/10.3390/s23031268.
23. 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. *Resources, Conservation & Recycling* **2024**. https://doi.org/10.1016/j.resconrec.2024.107527.
24. Aliakbarian, B.; Ghirlandi, S.; Rizzi, A.; Stefanini, R.; Vignali, G. Life Cycle Assessment of Plastic and Paper-Based Ultra High Frequency RFID Tags. *Radio Frequency Technology* **2023**. https://doi.org/10.3233/RFT-230044.
25. Segkoulis, T.; Limniotis, K. Enhancing Multi-Factor Authentication for Mobile Devices: A Survey. *Electronics* **2025**, *14*, 1914. https://doi.org/10.3390/electronics14091914.
26. Zhang, W.; Wu, J.; Chen, L. A Review of RFID Applications and Security Challenges in Supply Chain Management. *Computers & Security* **2022**, *117*, 102683. https://doi.org/10.1016/j.cose.2022.102683.