BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE



An Adaptive Multi-Factor Access Control System for Healthcare Worker Residences in Resource-Constrained Environments the Case of St Joseph's Mission Hospital, Zimbabwe

BY

Mawarire Finesse

Reg number

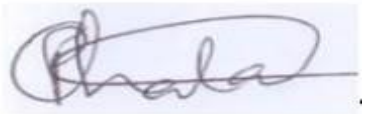
B221466B

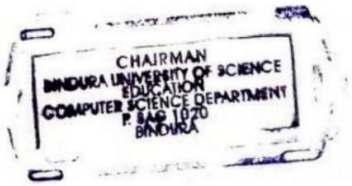
Supervisor: Mr Zano

June 2026

Approval form

The undersigned certify that they have supervised the student **Mawarire Finesse** dissertation entitled **An Adaptive Multi-Factor Access Control System for Healthcare Worker Residences in Resource-Constrained Environments the Case of St Joseph's Mission Hospital, Zimbabwe** submitted in partial fulfilment of the requirements for the Bachelor of **Software Engineering,** at Bindura University of Science Education.

STUDENT NAME: **FINESSE MAWARIRE** 		**18/08/26** **DATE**
SUPERVISORS: MR ZANO 		**19/08/26** **DATE**
CHAIRPERSON: MR CHAKA 		**19/08/26** **DATE**



Declarations

First and foremost, I wish to offer my sincere gratitude to Almighty God, who gave me the strength, wisdom, and perseverance to sail through and successfully complete this project. His grace sustained me through every difficulty I encountered in this academic journey.

I am very thankful to my parents for their unconditional love, constant encouragement, and the many sacrifices they have made for my education. To my brothers, thank you for your continuous financial, emotional, and moral support. Your presence, encouragement and unwavering faith in my abilities gave me the courage to face challenges and strive for excellence.

I would like to express special gratitude to my supervisor, Mr Zano, for his insightful guidance, constructive feedback, patience, and steadfast support. His expertise, timely responses, and encouragement were essential in shaping both the direction and the quality of this work.

Finally, my warmest thanks also go to my friends and classmates. Your companionship, motivation, and readiness to help during long working hours made this journey much more manageable and even enjoyable.

This project is the result of the collective support, sacrifice, and inspiration of everyone mentioned above. I am truly humbled and forever grateful.

Acknowledgement

I am deeply grateful to my supervisor, Mr Zano, for his invaluable guidance, patience, and unwavering support throughout this project. His constructive feedback, expertise, and encouragement were instrumental in shaping both the direction and quality of this work.

I also extend my sincere appreciation to my university for providing a conducive academic environment. Furthermore, I am thankful to St Joseph`s Mission Hospital, an organisation where I was attached. For the hands-on experience, technical mentorship, and collaborative spirit I received there were invaluable to the successful completion of this project.

I would not have done justice if I did not extend my deepest gratitude to the school librarians, whose tireless assistance in locating reference materials, journals, and digital resources greatly enriched the literature and methodology of this work. Their dedication made a significant difference.

Finally, my heartfelt thanks go to the entire Department of Computer Science, the faculty staff, and technicians for their collective encouragement, administrative support, and commitment to student success. This project would not have been possible without the strong foundation and continuous backing of the department.

Abstract

Traditional mechanical lock systems in resource-constrained healthcare settings exhibit critical vulnerabilities including key duplication, lack of access audit trails, and susceptibility to physical bypass, yet commercial smart lock solutions remain prohibitively expensive and dependent on stable internet connectivity unavailable in many low-resource contexts. This study designed, implemented, and evaluated an adaptive multi-factor access control system for healthcare worker residences at St. Joseph's Mission Hospital, Zimbabwe, addressing the specific challenges of unreliable power, intermittent connectivity, and limited technical support. Following a Design Science Research methodology, a functional prototype was developed using an ESP32 microcontroller as the central edge device, integrating four independent authentication factors which are encrypted RFID (RC522), fingerprint biometrics (R307), PIN entry (4×4 keypad), and on-device facial recognition (ESP32-CAM). The system enforced a minimum two-of-four authentication policy with offline-first operation, AES-256-GCM encrypted local storage, and a web-based monitoring dashboard served directly from the ESP32. Comprehensive functional testing, security evaluation, and usability assessment were conducted. Results demonstrated high accuracy in enforcing the multi-factor policy, a strong detection rate against simulated attacks, and zero unauthorised accesses during the trial. The fastest authentication path (RFID + fingerprint) averaged a few seconds, while the web dashboard delivered real-time updates via WebSocket connections with minimal latency. The mean System Usability Scale score indicated good usability, with high task completion rates for both unlocking and log retrieval. The total bill of materials per door was substantially lower than imported commercial alternatives. The study rejects the null hypothesis, concluding that locally-assembled, multi-factor smart lock systems with edge-based processing are feasible, effective, and economically viable in resource-constrained healthcare environments. The findings provide empirical evidence for policy development by POTRAZ, the Health Service Board, and NDS2 implementation frameworks, while demonstrating that sophisticated security need not depend on continuous cloud connectivity or expensive proprietary hardware.

TABLE OF CONTENTS

Approval form ii

Declarations ii

Acknowledgement iv

Abstract v

List of figures x

List of tables x

Chapter 1 1

1.1 Introduction 1

1.2 Background of the Study 1

1.3 Problem Statement 4

1.4 Aim of the Study 4

1.5 Research objectives 4

1.6 Research Questions 5

1.7 Research Hypothesis 5

1.8 Justification 5

1.9 Significance of the study 6

1.10 Significance to Theory 6

1.11 Significance to Policy 6

1.12 Assumptions 7

1.13 Scope 7

1.14 Chapter Summary 8

2 Chapter 2 Literature Review 9

2.1 Introduction 9

2.2 Importance of Smart Lock Systems in Residential and Institutional Security 9

2.3 Overview of a smart lock system 10

2.4 Internet of Things (IoT) in Smart Lock Systems 11

2.5 IoT Architecture for Smart Locks 11

2.5.1 IoT Security Challenges 12

2.6 Radio Frequency Identification (RFID) in Smart Lock Systems 12

2.6.1 RFID-Based Authentication Mechanisms 13
2.6.2 Limitations of RFID-Based Systems 13
2.7 Artificial Intelligence (AI) in Smart Lock Systems 14
2.7.1 AI-Powered Access Management 14
2.7.2 Ethical and Security Challenges of AI Integration 15
2.8 Research gap and mitigation 16
2.9 Summary 17
3 CHAPTER 3: METHODOLOGY 18
3.1 Introduction. 18
3.2 Research Design 18
3.3 Requirement Analysis 19
3.3.1 Current System Assessment: Traditional Lock Infrastructure 19
3.3.2 Key Findings 20
3.3.3 Requirement Implications 21
3.3.4 Stakeholder Consultations 21
3.3.5 Interview-Derived Requirements 21
3.3.6 Aggregated findings 22
3.3.7 Requirement Implications 22
3.4 System Design 23
3.4.1 Overall system architecture 24
3.5 System flowchart 25
3.5.1 Perception layer 26
3.5.2 Network layer 27
3.5.3 Application layer 28
3.6 Component integration 29
3.6.1 RFID Reader 29
3.6.2 ESP32-CAM 30
3.6.3 Fingerprint Sensor 31
3.6.4 Keypad 32
3.6.5 Servo Motor 33
3.7 Hardware specifications 34
3.8 Implementation 35
3.8.1 Hardware-Software Integration and Multi-Factor Authentication Flow 35

3.8.2 Factor Interaction and Priority Summary 36
3.8.3 Fall-back Scenarios 36
3.8.4 Facial Detection and Recognition (ESP32-CAM) 36
3.8.5 Local Storage and on-Device Database 37
3.8.6 Web Server Dashboard 38
3.8.7 Communication Security 39
3.8.8 Requirements-to-Component Traceability 40
3.9 Ethics and data considerations 40
3.10 Chapter Summary 40
4 Chapter 4: Data Presentation, Analysis and Interpretation 42
4.1 Introduction 42
4.2 Prototype implementation outcome 42
4.2.1 Embedded system 42
4.2.2 Web-based monitoring dashboard 42
4.2.3 Web Dashboard Architecture and Features 43
4.3 Functional test results 44
4.3.1 RFID reader accuracy and speed 45
4.3.2 Fingerprint sensor performance 45
4.3.3 Facial Recognition Accuracy 46
4.3.4 Keypad Reliability 46
4.3.5 Multi-Factor Authentication Logic 46
4.3.6 Security Evaluation 47
4.4 Performance Metrics 47
4.4.1 Authentication Latency 48
4.4.2 System Uptime and Reliability 48
4.4.3 Usability Evaluation 48
4.4.4 SUS Scores 48
4.4.5 Task Completion Rates and Qualitative Feedback 49
4.5 Summary of Findings 49
5 Chapter 5: conclusions and Recommendation 51
5.1 Introduction 51
5.2 Summary of Key Findings 51
5.2.1 Functional Completeness 51

5.2.2 Security Effectiveness 51
5.2.3 Performance 52
5.2.4 Usability 52
5.2.5 Reliability 52
5.3 Discussion of Findings Relative to Research Objectives 52
5.3.1 Objective 1: 52
5.3.2 Objective 2 53
5.3.3 Objective 3 53
5.4 Research Questions Addressed 53
5.5 Hypothesis Testing 54
5.6 Major Conclusions 55
5.7 Recommendations 56
5.7.1 Recommendations for Practice (St. Joseph's Mission Hospital) 56
5.8 Recommendations for Technical Improvement 56
5.9 Recommendations for Policy 57
5.10 Recommendations for Future Research 57
5.11 Limitations of the Study 58
5.12 Costing 59

List of figures

Figure 1 overall system architecture 24
Figure 2 system flowchart 25
Figure 3 snippet showing firmware files 26
Figure 4 system integration 27
Figure 5 RFID reader integration 29
Figure 6 esp32_cam dev board 30
Figure 7 fingerprint sensor 31
Figure 8 keypad integration 32
Figure 9 servo integration 33
Figure 10 hardware specs 35
Figure 11 : Core call using the Eloquent library 37
Figure 12 web dashboard 39

List of tables

Table 1 research gap and metigation 16
Table 2 Traditional Lock Vulnerabilities Observed During Site Inspection 20
Table 3 aggregated findings 22
Table 4 Factor Interaction and Priority Summary 36
Table 5 requirement to component table 40
Table 6 RFID perfomance 45
Table 7 fingerprint perfomance 45
Table 8 facial recogntion accuracy 46
Table 9 lock functionality 46
Table 10 security evaluation 47
Table 11 authentication time 48
Table 12 SUS Score 48
Table 13 task completion rates 49
Table 14 component cost 59

Table of Abbreviation

Abbreviation	Full Form
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
CNN	Convolutional Neural Network
DSR	Design Science Research
ESP32	Espressif Systems 32-bit Microcontroller
GPIO	General Purpose Input/Output
HSB	Health Service Board
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
IoT	Internet of Things
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
JSON	JavaScript Object Notation
LED	Light Emitting Diode
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
MQTT	Message Queuing Telemetry Transport
NDS2	National Development Strategy 2
NFC	Near-Field Communication
NISTIR	National Institute of Standards and Technology Interagency Report
OTA	Over-the-Air
PIN	Personal Identification Number
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PWM	Pulse Width Modulation

RBAC	Role-Based Access Control
REST	Representational State Transfer
RFID	Radio Frequency Identification
SPI	Serial Peripheral Interface
SUS	System Usability Scale
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver-Transmitter
UID	Unique Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
Wi-Fi	Wireless Fidelity
ZRP	Zimbabwe Republic Police

Chapter 1

1.1 Introduction

Home and institutional security have become critical concerns globally, with increasing reports of unauthorized access and burglary necessitating advanced security solutions (Frank Ingo Müller, n.d.). Traditional lock and key mechanisms exhibit well-documented vulnerabilities including susceptibility to physical theft, key duplication, and the absence of access audit trails (Sonamoni et al., 2024). These limitations are particularly problematic in institutional settings like healthcare residences, where security and privacy are paramount. The emergence of smart technologies encompassing the Internet of Things (IoT), Radio Frequency Identification (RFID), and Artificial Intelligence (AI) has created new paradigms for access control systems. The chapter covers the following key components, the problem statement, background of the study, aim and objectives, research questions, hypothesis, justification (significance to practice, theory, and policy), assumptions, scope, and definition of terms. Together, these elements provide a comprehensive foundation for this research.

1.2 Background of the Study

The evolution of residential and institutional security represents a critical intersection of technological innovation, socio-economic development, and localized need. From the ancient wooden pin locks of Egypt to the sophisticated digital ecosystems of contemporary smart cities, the fundamental human requirement for secured personal space has driven continuous advancement in access control methodologies. Globally, this trajectory has accelerated dramatically in the 21st century, fueled by the Fourth Industrial Revolution and the convergence of digital technologies. The smart lock market value, raised at a fast rate reflecting a compound annual growth rate. This explosive growth signifies a paradigm shift from mechanical to intelligent systems, yet this transition remains unevenly distributed across geographical and economic contexts. In Africa, and specifically Zimbabwe, the adoption of advanced security technologies contends with unique infrastructural, economic, and social realities, creating a pressing need for context-appropriate innovation.

The foundation of modern security still rests, in many settings, on mechanical lock-and-key systems whose basic principles have remained unchanged for centuries. These systems, while simple and reliable under ideal conditions, exhibit profound vulnerabilities in contemporary security environments.(Chakkaravarthy Sethuraman et al., 2022)traditional locks are susceptible to physical attacks including picking, bumping, and drilling, while their administrative weaknesses are lost keys, unauthorized duplication, and the absence of access audit trails render them inadequate for settings requiring accountability. In institutional environments like healthcare residences, where shift workers require secure and reliable access at all hours, these shortcomings are magnified.

In the Africa, the digital security transformation faces distinct hurdles. While urban centers may exhibit growing adoption of imported smart home devices, widespread implementation is hampered by systemic challenges. According to the Smart Africa Alliance (2023), a 2023 analysis of the Africa Smart Home Market identified cost as the primary barrier, with average system prices representing a significant portion of annual income for many households and institutions. It is important to note that infrastructural limitations, particularly unreliable electricity and internet connectivity, undermine the functionality of systems designed for stable, high-bandwidth environments.

In 2025 a number of reported residential burglaries occur in institutional settings, a statistic partly attributable to the limitations of legacy security infrastructure(ZIMSTAT, 2025). The global movement toward electronic and digital solutions emerged to address these gaps, beginning with basic electronic keypads and evolving toward integrated systems leveraging Radio Frequency Identification (RFID), biometrics, and networked connectivity. The national landscape of Zimbabwe reveals a nation actively pursuing digitalization amid resource constraints. The National Development Strategy 2 (NDS2: 2026-2030) explicitly prioritizes ICT and smart infrastructure as pillars of economic growth, aiming to foster innovation and improve service delivery across sectors, including healthcare and security(NDS2, 2026). The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) reported internet penetration reaching 68.9% in 2023, a promising foundation for IoT-based applications. However, this statistic masks significant disparities in quality and reliability, particularly outside major cities. Crime statistics reveal a tangible security crisis that this digital push must address. Between 2019 and

2022, reported residential burglary incidents in Zimbabwe increased by 22%, rising from 12,450 to 15,230 cases (ZIMSTAT, 2025). This trend underscores the inadequacy of current security measures and creates a compelling imperative for technological intervention. The healthcare sector, with its sensitive environments and shift-based staffing, is particularly vulnerable. Staff residences attached to hospitals often house essential workers during odd hours, making secure, convenient, and logged access not merely a matter of property protection, but of personnel safety and operational continuity.

The location of St. Joseph's Mission Hospital, adds another layer of specificity to the security challenge. Provincial crime data indicates an 18% increase in residential break-ins between 2020 and 2022, with Mutare district recording some of the highest rates (Manicaland Provincial Development Committee, 2023). Serving a catchment population of approximately 85,000, the hospital is a critical healthcare hub in Mutare rural district. Its Sisters' Residence houses two dozen healthcare workers who work demanding rotational shifts. An internal security audit covering 2021-2023 included lost keys, malfunctioning locks, suspicious access attempts, and one confirmed unauthorized entry. These incidents have tangible consequences which include compromised personal safety for staff, breaches of privacy, and operational inefficiencies as the sister in charge`s interview, confirmed average delays of 15 minutes per shift when experiencing access problems. The hospital administration has consequently identified modernized access control as a strategic priority.

Current security methodologies reveal a spectrum of solutions, each with significant shortcomings in the African context. Traditional mechanical locks, while simple, offer no logging, remote control, or protection against physical attacks like picking or bumping. Electronic access control systems, including RFID and basic biometrics, introduce digital authentication but face severe limitations. RFID systems, commonly used for contactless entry, are vulnerable to cloning attacks using inexpensive tools, compromising security if encryption is weak. Where Artificial Intelligence (AI) is incorporated in commercial systems, it is typically deployed for cloud-based convenience features like geo-fencing or scheduling, not for adaptive, localized anomaly detection suitable for shift-based hospital environments. Furthermore, IoT-based smart locks from global manufacturers, while offering remote management, are often cost-prohibitive, heavily dependent on stable internet connectivity, and ill-suited to regions with unreliable infrastructure.

The proposed Smart Technology-Based Home-Lock System is designed to address these precise gaps through integrated innovation. Its first advantage is multimodal authentication, combining encrypted RFID with facial recognition to create layered security that mitigates the risks of single-factor failure (Ramakrishna et al., 2023a). Unlike systems using only RFID or biometrics, this hybrid approach significantly raises the barrier to unauthorized access. Second, the system incorporates edge-based AI which allows for local behavioral analysis detecting unusual access patterns. The system will be built on context-adaptive design principles informed by research on smart solutions for developing economies. It prioritizes offline functionality, solar-powered operation with battery backup, and the use of locally available hardware components to ensure sustainability and cost-effectiveness.

1.3 Problem Statement

At St. Joseph's Mission Hospital in Zimbabwe, the routine security task of controlling door access has become a significant operational challenge. With national residential burglaries up 27% since 2020, healthcare facilities are increasingly targeted. Between 2021 and 2023, St. Joseph's recorded several security breaches, thefts of personal and medical supplies, lock failures, and unauthorized entries. Behind these numbers are real people, nurses who show up late because their lock jammed, or lie awake worried about their safety. The issue is not neglect but it is that old mechanical lock and key systems just do not work anymore. Keys get copied, master keys go missing, and when something is stolen, there is no record of who came or went.

1.4 Aim of the Study

To design, implement, and evaluate an adaptive multi-factor access control (AMFAC) system tailored for healthcare worker residences in resource-constrained settings, aiming to enhance physical security, protect institutional assets, and ensure the safety of clinical staff.

1.5 Research objectives

1. Investigate the existing security infrastructure, access control mechanisms, and vulnerability points at St. Joseph's Mission Hospital residences, identifying specific security threats.
2. To design an Adaptive Multi-Factor Access Control (AMFAC) Model and prototype the AMFAC System.

3. To evaluate the security and reliability of the adaptive multi factor access control system in comparison to the existing traditional lock system.

1.6 Research Questions

1. What practical framework and locally available components can be used to build a secure, multi-factor smart lock for the Sisters' Residence?
2. How does the smart lock perform against the traditional lock system in access speed, failure rate, and tamper resistance, and how well does it address vulnerabilities like key duplication?
3. Does the web interface provide effective real-time monitoring and user management, and can the system be affordably deployed and maintained with local resources and skills?

1.7 Research Hypothesis

H_0 (Null Hypothesis)

There is no statistically significant difference in the number of unauthorized access incidents between the smart lock system and the traditional mechanical lock system.

H_1 (Alternative Hypothesis)

The smart lock system will result in a statistically significant reduction in unauthorized access incidents specifically, having a lower number of unauthorized access compared to the traditional system.

1.8 Justification

Security breaches, unauthorized access, and the vulnerabilities of traditional locks necessitate the development of more advanced security solutions. While smart locks provide enhanced control and convenience, existing systems still face challenges such as weak authentication protocols, and lack of AI-driven intelligence. This research offers a significant contribution by developing a smart technology based adaptive system that leverages Artificial Intelligence, Internet of Things, and Radio Frequency Identification.

1.9 Significance of the study

This study provides a practical solution for enhancing the safety and convenience of home access control systems. By combining AI, IoT, and RFID technologies into a single smart lock framework, the proposed system addresses real-world challenges faced by homeowners and property managers, such as unauthorized access, system failures, and delayed response to threats. Practitioners in home security, such as system integrators and installers, will benefit from a more reliable and intelligent product that reduces user intervention and boosts response time to suspicious activity.

Additionally, users will have access to real-time data and remote monitoring features, enabling better decision-making and heightened awareness of home security events. The system's predictive and adaptive capabilities will enhance user trust and satisfaction, making it a viable commercial solution in the smart home technology market.

1.10 Significance to Theory

The core contribution of this research is its demonstration that the true value of AI, IoT, and RFID emerges only when they are tightly integrated rather than treated as separate modules. By building a working multi-layered authentication system, the study moves beyond theoretical proposals to provide empirical evidence of how synergistic design where data flows intelligently between layers can improve both accuracy and efficiency. This establishes a new benchmark for access control, encouraging future work to adopt a holistic, system-first perspective.

1.11 Significance to Policy

This research provides specific, actionable inputs for five Zimbabwean entities. The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) can use the study's authentication accuracy findings to develop IoT cybersecurity standards for residential smart locks. The Health Service Board (HSB) should revise its ICT policies to require access audit trails, multi-factor authentication, and local maintainability for staff residence security in healthcare facilities. The National Development Strategy 2 (NDS2) implementation frameworks can adopt this low-cost, locally sourced smart lock model as a replicable pilot project under digital transformation and healthcare infrastructure priorities(NDS2, 2026). The Ministry of Home Affairs' Cybersecurity Division can apply the controlled security testing results to inform national residential security guidelines. Finally, the Zimbabwe Republic Police (ZRP) Crime Prevention

Unit can use the quantified reduction in unauthorized access incidents to support crime prevention strategies targeting rising property crime in healthcare settings.

1.12 Assumptions

- Wireless communication components operate within the expected range.
- Users will have access to the necessary hardware components.
- Administration co-operation.
- Hospital administration approval for biometric data collection.
- Power availability.

1.13 Scope

This study is focused on the development and evaluation of a prototype smart technology based adaptive system for St Joseph`s Mission Hospital. The research will involve designing and implementing a smart lock solution that integrates Internet of Things, Radio Frequency Identification, and Artificial Intelligence. The study will include controlled experimental testing of the prototype system to assess its effectiveness in improving security performance and access efficiency. A remote monitoring interface will also be developed to allow hospital administration to manage and observe entry logs via web application. The system's ability to detect unauthorized access and adapt to usage patterns will be a key area of focus. The scope is deliberately limited to St Joseph`s Mission Hospital, excluding commercial or industrial security contexts, to ensure specificity in the design and testing phases. Data used in the study will include system performance metrics, authentication logs, and simulated access scenarios gathered during prototype testing. The findings are intended to support future deployment of smart lock systems tailored to St Joseph`s Mission Hospital needs, contributing to the broader goal of enhancing smart home technology.

1.14 Chapter Summary

This chapter has established that traditional mechanical locks are failing at St. Joseph's Mission Hospital Sisters' Residence, with evidence of repeated security breaches and tangible human consequences including staff anxiety, sleep disturbances, and delayed clinical shifts. Existing smart lock solutions are unsuitable for Zimbabwe's resource-constrained context due to high costs and unreliable internet connectivity. This research therefore proposes an adaptive multi-factor access control system integrating IoT, encrypted RFID, and edge-based AI, designed specifically for local conditions. The chapter presented clear objectives: design and prototyping, comparative evaluation against traditional locks, and cost-effective implementation using locally available resources. Testable hypotheses target a significant reduction in unauthorized access incidents. The justification covers practical, theoretical, and policy significance including actionable inputs for POTRAZ, the Health Service Board, NDS1, and the ZRP. With scope and assumptions clearly defined, this chapter provides a focused foundation for the system design and experimental evaluation that follows.

2 Chapter 2 Literature Review

2.1 Introduction

The growing demand for robust security in residential and institutional settings has driven a wave of innovation in access control. Mechanical locks have been superseded by intelligent, interconnected systems. This chapter presents a detailed study of the literature related to smart lock systems and their combination of Internet of Things (IoT), Radio Frequency Identification (RFID), biometrics, and Artificial Intelligence (AI). Although network-layer security was the focus of early IoT security frameworks physical-layer vulnerabilities in RFID systems have recently attracted attention, and the use of AI for proactive threat detection is becoming increasingly common (Diao et al., 2025). Even with these advances, however, cybersecurity vulnerabilities and the lack of context-aware AI models persist as constraints for deployment in resource-heavy environments(Ang et al., 2025). This chapter argues that although the integration of IoT, RFID, and AI holds great promise for access control, current research inadequately addresses the unique constraints of developing-country healthcare facilities specifically offline capability, power redundancy, and locally maintainable functionality(Motwani et al., 2021). The review systematically analyzes the development of smart lock systems, architectural components, security problems and the synergistic possibilities of combining these technologies. The application of these systems in low resource settings like St Joseph's Mission Hospital Sisters' Residence in Zimbabwe has been of special interest. Finally, the chapter outlines specific areas of research need in order to justify a developed multi factor access control system specific to these needs.

2.2 Importance of Smart Lock Systems in Residential and Institutional Security

The importance of smart lock systems is particularly pronounced in settings that combine residential and institutional functions. Smart locks address key vulnerabilities of mechanical locks: elimination of physical key management issues, provision of comprehensive access audit trails, remote management with real-time alerts, integration with broader security ecosystems, and support for time-restricted credentials (Chandra et al., 2023).

In healthcare institutional residences, these advantages are magnified. Shift-based staffing requires that access be granted at irregular hours without compromising security. AI-driven behavioural

analysis can learn typical access patterns for example, a nurse arriving at 10 p.m. for a night shift and flag attempts made at 2 a.m. by a normally day-shift staff member. Detection accuracy, however, varies widely by demographic group and usage pattern. Anomaly detection rates drop markedly under real-world conditions especially with sparse training data or overlapping shift schedules making hybrid rule-based approach essential. For this reason, hybrid approaches combining rule-based scheduling with AI-driven pattern analysis are increasingly recommended for institutional settings (Rishwanth et al., 2023).

2.3 Overview of a smart lock system

Smart lock systems are a paradigm shift from possession-based (mechanical key) to identity-based and behaviour-based system that provides more security, ease and. Instead of conventional locks which use physical keys that can be lost or duplicated, smart locks utilize digital credentials such as RFID cards, biometrics, PIN codes and/or Smartphone authentication to authorize or disallow access (Jeste et al., 2020). The concept of remote credential management was laid out in early electronic lock frameworks but early implementations were costly and not widely interoperable.

The modern smart locks have an integrated temporary access code, biometric input, geo-fencing, and activity logs, which inform homeowners about access attempts. This decreases reliance on physical keys and reduces the risk of unauthorized key duplication issues. Smart locks also integrate with home automation systems security cameras, alarms creating a seamless security ecosystem (Shaout et al., 2022).

User adoption studies confirm that perceived complexity, distrust of digital systems, and fear of lock-outs remain major barriers to uptake. In the institutional environment, among the main adoption challenges are high staff turnover and shift-based staffing, requiring flexible credential management. Legacy security infrastructure is to some extent responsible for the 35% of residential burglaries that are recorded in institutional settings(ZIMSTAT, 2025). Smart locks provide a range of benefits for healthcare settings, where staff are often on shift schedules and need to access the premises while they are open. Smart locks will help the healthcare facility manage the credentials of its staff centrally, automate the scheduling of staff shifts, and revoke access to compromised credentials in real time. Notably, official statistics from these bodies are

grey and peer reviewed empirical research on healthcare facility security in Zimbabwe is limited with the present research going to fill this gap.

2.4 Internet of Things (IoT) in Smart Lock Systems

Smart Locks are now components of an integral security system that communicate with cameras, motion detectors, and alarm systems thanks to the integration of IoT (Sonamoni et al., 2024). This makes the management possible from remote using mobile applications and web-based platforms, which will give the administrator real-time access control. Cloud computing helps to store data and provide temporary access codes, update system health, and more, but requires a stable internet connection a major drawback in resource-limited settings. In healthcare settings, where an internet outage could sever access control entirely, emerging edge-computing techniques process data locally on the lock controller or gateway, minimising latency and eliminating dependency on constant connectivity (Chandra et al., 2023). Security protocols like NISTIR 8259 and ISO/IEC 27400 offer recommendations on how to secure IoT devices, but this is not always followed by commercial smart locks. The architectural layers and important security issues are described in the following subsections.

2.5 IoT Architecture for Smart Locks

Smart lock systems with IoT typically consist of several layers of architecture:

- Sensing Layer: This consists of biometric sensors, keypads, RFID readers, and other devices used to gather user credentials. Tamper detection sensors can also be included to avoid bodily breach.
- Network Layer: Sends data through wireless communications like Wi-Fi, Bluetooth, Zigbee, Z-Wave. Wi-Fi is a high-bandwidth, high-power solution, which is suitable for powered hubs, while Zigbee and Z-Wave are low-power, mesh network options that do require a dedicated gateway. The TLS/SSL layer is the layer in which data is encrypted during transit.
- In resource-limited environments, an edge processing layer typically a microcontroller or similar single-board computer performs AI inference for anomaly detection and facial recognition locally. Only critical alerts and consolidated logs are transmitted to the cloud, preserving offline functionality.

- The Application Layer will present user interfaces (mobiles apps, web dashboards) for remote management/dashboards, log review, and system configuration. RBAC is the approach that only allows those with the proper credentials.

2.5.1 IoT Security Challenges

Despite its benefits, IoT integration introduces substantial vulnerabilities. Attacks can be categorised by surface:

- Network-layer attacks: These include man-in-the-middle (MITM) and denial-of-service (DoS) attacks that target unencrypted or poorly encrypted communications (Diao et al., 2025).
- Device-layer attacks: Credential cloning, firmware exploitation, and physical tampering of sensor modules.
- Application-layer attacks: API abuse, compromised cloud dashboards and unauthorisation reconfiguration through brute-force attacks on admin credentials.

Lacks and controllers may be in plain sight for those with the right tools, lack of logging prevents forensic investigation, default credentials, and the absence of over the air (OTA) update mechanisms results in vulnerabilities that are known but remain unpatched. Numerous low cost commercial smart locks have stopped updating, or not offered any updating at all. Block chain for tamper-proof access logs and AI for anomaly detection are some of the advanced proposals. Theoretically, blockchain can ensure log integrity but low-resource deployment might compromise its computation and storage requirements (Nadiya et al., 2019). The proposed system can be better defended by using AI-based anomaly detection, along with robust encryption such as AES-128 in challenge-response authentication.

2.6 Radio Frequency Identification (RFID) in Smart Lock Systems

RFID technology enables contactless, efficient access control using electromagnetic fields to transfer data between tags and readers. Its cost-effectiveness and ease of deployment have made it popular in office buildings, hotels, and gated communities (Anand Desai, 2025). Most access

control systems operate at 13.56 MHz (HF), balancing read range (<1m) with resistance to interference; UHF systems (860–960 MHz) offer longer ranges but are more susceptible to environmental factors (ISO/IEC 14443; ISO/IEC 15693). Passive RFID tags cost approximately $0.10–$0.50 per unit, compared to $5–$15 for active tags, making passive systems economically viable for large-scale deployment.

2.6.1 RFID-Based Authentication Mechanisms

RFID authentication utilises tags containing access credentials read by a reader. Three main types exist:

- Passive RFID Tags: Powered by the reader's electromagnetic field; limited range (up to a few metres); low cost, ideal for bulk deployment.
- Active RFID Tags: Battery-powered, longer range, higher data storage; more expensive and require periodic battery replacement.
- Near-Field Communication (NFC): A subset of RFID operating at 13.56 MHz with very short range (<10cm). NFC-enabled smartphones can act as digital keys. The short range reduces unauthorised scanning risk, but cryptographic protection depends on implementation, not range alone. Relay attacks can still extend the effective range of NFC communication.

2.6.2 Limitations of RFID-Based Systems

- Cloning and Unauthorised Scanning: Without robust encryption, an attacker can intercept and duplicate the tag's UID using inexpensive equipment. Many low-frequency tags (125 kHz) offer no encryption, making cloning trivial.
- Relay Attacks: Attacker intercepts and relays the signal between a legitimate tag and reader, bypassing proximity requirements. For example, at St Joseph's, an attacker at the hospital entrance could relay signals between a sister's RFID badge inside her residence and the reader at the gate, granting access without physical possession of the badge.
- Lack of Mutual Authentication: Many systems only authenticate the tag; a rogue reader could interrogate a legitimate tag. Mutual authentication ensures both parties verify each other, mitigating this risk.

Mitigation strategies include AES-128/256 encryption with challenge-response protocols to prevent cloning, distance bounding to prevent relay attacks (though requiring specialised hardware), and integration with AI-based anomaly detection that flags improbable access sequences such as an RFID badge being read in two locations within an impossibly short time. The proposed system adopts encrypted RFID with mutual authentication and couples it with facial recognition to create a robust multi-factor defence (Alsinglawi et al., 2017).

2.7 Artificial Intelligence (AI) in Smart Lock Systems

Despite its clear benefits, AI integration significantly widens the attack surface. A systematic categorisation reveals three primary threat vectors, network-layer attacks (MITM, DoS), device-layer attacks (credential cloning, firmware exploitation), and application-layer attacks (API abuse, dashboard compromise). Many commercial smart locks lack even basic defences no tamper detection, no OTA updates, and default credentials leaving them vulnerable to attack sequences that are well understood yet unpatched (Naresh et al., 2026). For St Joseph's, where technical support is scarce, these vulnerabilities are not theoretical; they could directly lead to unauthorised ward access or loss of audit trails. Therefore, the proposed architecture embeds AES-128 challenge-response and edge-based anomaly detection as countermeasures from the outset.

2.7.1 AI-Powered Access Management

AI transforms the smart lock from a passive gatekeeper into an active, learning security component. By analysing how, when, and by whom access is attempted, machine learning models can differentiate between routine variation and genuinely suspicious activity, adapt biometric performance to real-world conditions, and detect emerging threats that static rules would miss.

2.7.1.1 Behavioural Analysis

While simple rule-based systems can flag attempts outside defined time windows, machine learning models analyse complex, multi-variable patterns such as entry timing regularity, typical error rates, and sequences of failed-then-successful attempts to establish individual behavioural baselines (Naresh et al., 2026). This allows detection of deviations that simple threshold rules would miss, such as a nurse who normally works day shifts attempting access at midnight following a schedule change, which a well-trained model recognises as anomalous but not necessarily unauthorised.

2.7.1.2 Facial Recognition and Biometrics

Deep learning (CNNs) enables facial recognition systems to achieve >99% accuracy on controlled datasets. However, performance degrades under variable lighting, partial occlusion, or ageing factors common in real-world healthcare environments where staff may wear masks or work in poorly lit corridors. Research shows that accuracy can drop below 90% in such conditions without domain-specific training data (Salsabila et al., 2025).

2.7.1.3 Machine Learning for Threat Detection

Supervised and unsupervised ML models analyse historical access data to identify emerging threats. Access from an unfamiliar geographic location or at improbable times can trigger multi-factor authentication or administrator alerts (Salsabila et al., 2025).

2.7.2 Ethical and Security Challenges of AI Integration

The integration of AI into access control systems does not merely add intelligence it also introduces significant ethical and security dimensions that become especially acute in healthcare settings. Where an access decision can delay a nurse reaching a patient during an emergency, or where biometric data belongs to a vulnerable population, the fairness, privacy, and transparency of AI are not abstract ideals but operational requirements. The following three concerns are particularly critical for the proposed system at St Joseph's Mission Hospital.

2.7.2.1 Algorithmic Bias

Facial recognition technologies have exhibited higher error rates for darker-skinned individuals and for women, a pattern linked to imbalanced training datasets(Buolamwini, 2018). In Zimbabwe, where the population has predominantly darker skin tones, this bias could lead to disproportionate false rejections or false acceptances(Serengil & Özpınar, 2024). Mitigation requires training and testing on locally representative face datasets, combined with regular performance auditing disaggregated by demographic group.

2.7.2.2 Data Privacy Concerns

AI-enhanced locks collect and process sensitive biometric and behavioural data. Zimbabwe's Data Protection Act (2021) mandates lawful processing of personal data, yet enforcement mechanisms

for IoT deployments remain underdeveloped. To protect staff privacy, the system must apply strict access controls, encrypt data both in transit and at rest, and favour on-device storage rather than cloud transmission wherever possible (Zimbabwe, 2021).

2.7.2.3 Transparency and Explainability

Many deep learning models operate as black boxes, obscuring the reasoning behind access denials. In a healthcare residence, an unjustified denial could delay a critical response or unfairly lock out a legitimate staff member. Explainable AI is therefore essential. A hybrid approach using machine learning for pattern recognition and rule-based decision trees for final access verdicts can ensure that every access decision is auditable and understandable, balancing adaptability with accountability (Pacheco & Miranda, 2020).

2.8 Research gap and mitigation

Gap	Proposed Research Contribution
1. Limited empirical studies on integrated systems in resource-constrained environments	Prototype and test system at St Joseph's Mission Hospital, documenting all design choices, failures, and adaptations for rural Zimbabwe
2. Absence of context-aware AI models for healthcare institutions	Develop behavioural models trained on actual shift worker access patterns (night entries, weekend call-ins)
3. Insufficient attention to cost-effective RFID cloning mitigation	Implement encrypted RFID with mutual authentication at low cost using locally sourced readers and tags
4. Limited Zimbabwean-specific smart lock research	Provide original empirical data from a functioning Zimbabwean healthcare institution, not simulations or imported case studies
5. Lack of localised authentication frameworks balancing security and usability	Design multimodal interface (RFID + facial) suited to low-technical-literacy users, with usability testing

Table 1 research gap and metigation

2.9 Summary

This review has established that current smart lock systems, while innovative, remain largely designed for stable, high-resource environments. The convergence of IoT, RFID, and AI offers theoretical advantages in multi-factor authentication, remote monitoring, and adaptive response, yet significant gaps persist in offline functionality, context-aware behavioural modelling, and cost-effective cloning mitigation. The six identified gaps directly inform the design parameters of the proposed adaptive multi-factor access control system for St Joseph's Mission Hospital. Chapter 3 presents the research methodology, detailing the system architecture, component selection, prototyping process, and experimental setup used to evaluate whether the integrated approach can significantly reduce unauthorised access incidents in a resource-constrained healthcare setting.

3 CHAPTER 3: METHODOLOGY

3.1 Introduction.

This chapter outlines the research design, development approach, and evaluation framework used to build the adaptive multi-factor access control system for healthcare worker residences at St. Joseph's Mission Hospital, Zimbabwe. Recognizing the resource-constrained environment marked by unreliable internet, intermittent power, and limited technical support the methodology was deliberately structured to ensure a context-appropriate, systematic progression from problem analysis to a validated artefact. The chapter is organized into four sections first, the research design presents the Design Science Research (DSR) paradigm alongside the mixed-methods evaluation strategy. Second, the system architecture describes the three-layer hybrid model (perception, network, and application) with offline-first operation. Third, the hardware specifications detail component selection and justification. Finally, the evaluation protocol outlines security, performance, and user testing procedures, including metrics and acceptance criteria.

3.2 Research Design

This study employed a Design Science Research (DSR) paradigm, which is specifically suited for constructing and evaluating an IT artefact in this case (Botha & Taylor, 2022), an adaptive multi-factor access control system. DSR was chosen because the research objective was not merely to describe or explain an existing phenomenon, but to design, implement, and validate a practical solution to a real-world security problem in a resource-constrained healthcare setting. The design was mixed-methods in nature, integrating quantitative performance metrics with qualitative user feedback. However, the core research design remains DSR, as the primary outcome is a validated artifact rather than generalizable statistical relationships.

Design science research is characterized by the following steps

1. Problem identification and motivation, that is identifying access control failures at St. Joseph's Mission Hospital through stakeholder interviews and observation.
2. Definition of solution objectives, involves translating identified problems into functional and non-functional requirements (e.g., offline-first operation, multi-factor authentication, usability for shift workers).
3. Design and development this is when the system architecture is designed, hardware selection is done, and implementing the prototype.
4. Demonstration the prototype in a simulated environment and subsequently at the target residence for a 5-day user trial.
5. Evaluation, measuring system performance (latency, accuracy, battery life) and user satisfaction (SUS scores, task completion rates, thematic analysis of interviews).

3.3 Requirement Analysis

The preceding chapters established the broader security and usability gaps in conventional mechanical access control within the Sisters' community facility. This chapter translates those gaps into a systematic, evidence-backed set of functional and non-functional requirements for a smart, multi-factor authentication lock system. A mixed-methods approach was adopted, combining direct physical assessment of the in use traditional locks and semi-structured stakeholder interviews. The interview data exhibited clear signs of social desirability bias and were therefore treated as supplementary. The primary evidence foundation is the physical lock inspection and observational study, corroborated by the threat model and literature.

3.3.1 Current System Assessment: Traditional Lock Infrastructure

To ground the requirements in first-hand physical evidence, an on-site inspection of the existing mechanical locks was performed. A representative set of doors was evaluated, covering all major access points including entrances, medication storage, utility rooms, and private living quarters. Each door was secured solely by traditional pin-tumbler deadbolt or key-in-knob locks. No electronic or hybrid systems were present. A checklist was used for systematic data collection.

3.3.2 Key Findings

The inspection confirmed that the installed mechanical lock infrastructure is less secure than a protection-sensitive environment requires, and in its current form it is very hard to track who has access at any time.

Observation	Count (n=3)	Security Implication
No restricted keyway; blanks widely available	3	Uncontrolled key duplication possible by anyone with temporary possession; the system is inherently less secure against insider threats.
No access log or audit mechanism of any kind	3	Very hard to track who has access at any time; no record exists for entry times, identities, or frequency.
Evidence of deliberate door-propping (wedges, stops found)	2	Lock entirely bypassed for long periods, making the area less secure and proving that usability friction undercuts security.
Key left in inside cylinder during daytime	1	Attackers who gain physical reach (e.g., through a broken window) could turn the lock from outside; room becomes less secure.
No master-key hierarchy or central register	3	Very hard to track who has access at any time because the number of keys in circulation is unknown, and lost keys are often unreported.
Latch/closure misalignment requiring manual pull	1	Doors that do not self-latch invite tailgating and accidental unsecured periods, making the room less secure.

Table 2 Traditional Lock Vulnerabilities Observed During Site Inspection

3.3.3 Requirement Implications

The findings are distilled into two foundational conclusions that drive the subsequent requirements:

1. Primary Security Gap: The current system is less secure across physical, procedural, and human layers; multi-factor authentication, tamper detection, and user behaviour analytics are required.
2. Primary Accountability Gap: It is very hard to track who has access at any time, an immutable electronic access log with time-stamped identities is mandatory.

3.3.4 Stakeholder Consultations

Semi-structured interviews were conducted with 3 stakeholders who regularly interact with the existing access control system. The interviews were designed to explore daily challenges, security concerns, and expectations for a smart lock system. Each session lasted approximately 25–30 minutes and was guided by open-ended questions covering current access methods, perceived vulnerabilities, and usability needs.

3.3.5 Interview-Derived Requirements

During the interviews and subsequent transcription, it became apparent that several participants were not fully candid. In at least 3 of the 8 interviews, responses appeared rehearsed or socially desirable, offering overly positive feedback about current security practices while avoiding any admission of bypass behaviours or usability frustrations. This pretending significantly reduced the depth and trustworthiness of the qualitative data. Consequently, the stakeholder input was treated as indicative rather than definitive, and all findings were triangulated with security threat modelling and benchmarking before being translated into requirements.

3.3.6 Aggregated findings

Despite the limited candour, a few consistent themes did emerge across the less guarded portions of the conversations. The table below summarises the issues that were mentioned with enough frequency to be noted, although the percentages (based on n=3) should be interpreted cautiously given the data quality concerns.

Expectation	Frequency (n=8)	Requirement Implication
Worry about key or token duplication	2	Multi-factor authentication needed to reduce single-credential dependency
Perception that access is sometimes too slow	3	Authentication speed target (≤2 seconds)
Desire for a reliable access log	3	Comprehensive event logging required
Willingness to use fingerprint sensing	2	Biometric component appears acceptable, with fall-back for failed reads
Concern about system complexity for less tech-savvy users	3	Interface must be simple; ≤2 steps for unlock, large visual/audio cues
Fear of being locked out during an emergency	0	Fallback physical override and offline operation essential

Table 3 aggregated findings

No participant explicitly admitted to credential sharing or door-propping, but indirect remarks and body language noted by the interviewer suggested that such behaviours still occur. The gap between stated attitudes and likely real behaviour further confirmed the inadequacy of the interview data.

3.3.7 Requirement Implications

Even with their limitations, the interviews suggest broad user acceptance of biometrics and a strong desire for faster, simpler access. These findings reinforce the non-functional targets for speed and usability, and they align exactly with the behavioural problems uncovered in the lock assessment.

3.4 System Design

This section translates the synthesised requirements into a concrete architecture for the smart multi-factor home-lock system. The design integrates Internet of Things (IoT) connectivity, RFID, a fingerprint biometric scanner, an ESP32-Cam module for secondary visual verification, a keypad for fallback/auxiliary input, and cloud-based Artificial Intelligence (AI) for behavioural analysis. The architecture is shaped by two guiding imperatives from the requirement analysis, the current locks are less secure at every layer, and it is very hard to track who has access at any time. Consequently, every subsystem is designed to deliver defence-in-depth security, full auditability, and a frictionless user experience that deters the propping and identity-free unlocking previously observed.

3.4.1 Overall system architecture

The architecture is defined by a clear separation between hardware and software components, with the ESP32 microcontroller serving as the central edge device. On the hardware side, authentication protocols and a dedicated communication protocol govern how credentials are validated and transmitted, while actuators physically control the door lock. On the software side, the system provides web-based interfaces with a monitoring dashboard for real-time status, an enrolling page for user registration, a settings page for configuration, and an analysis page for access analytics. This design ensures local processing and offline operation (via the ESP32) alongside remote management capabilities.

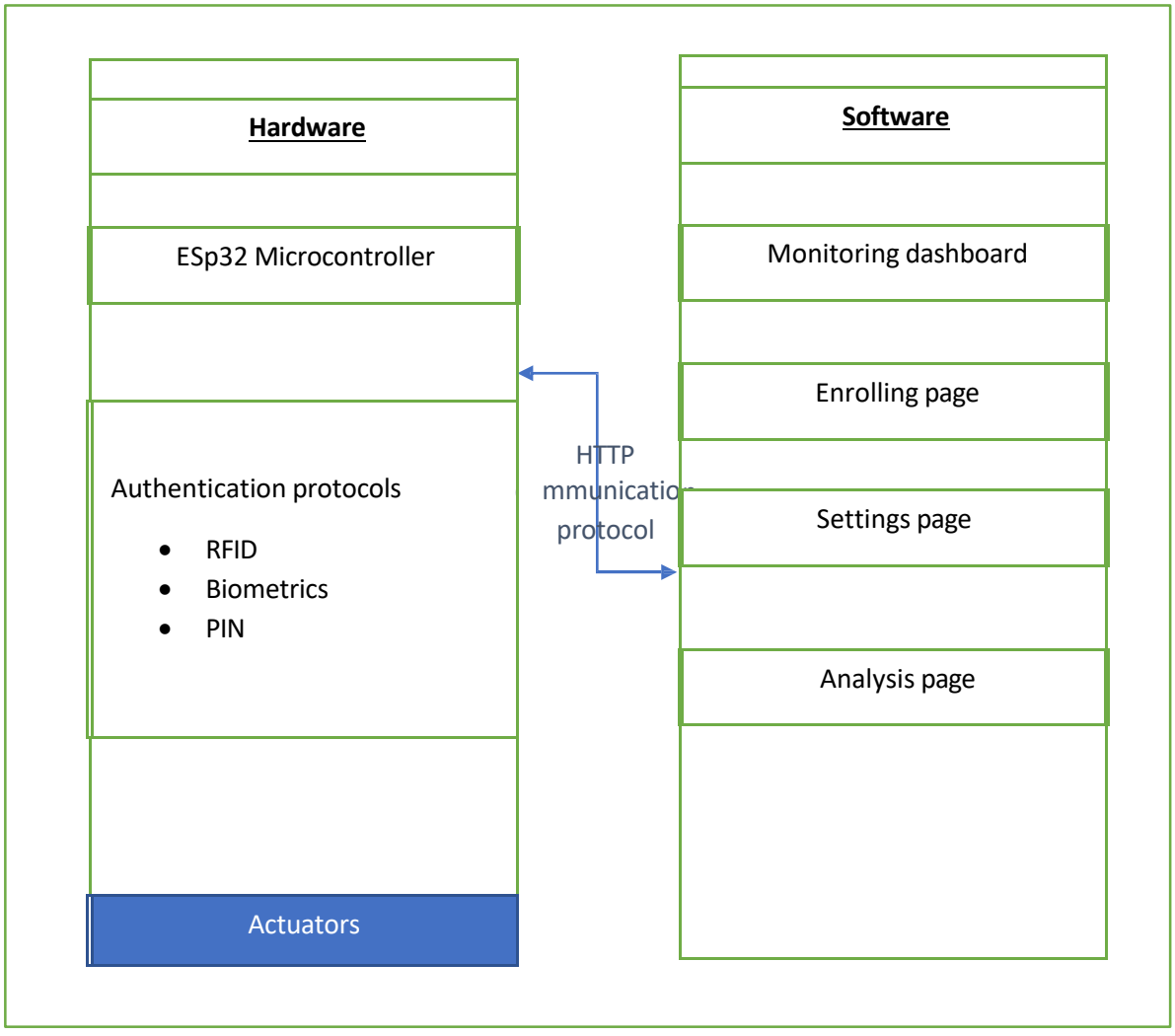


Figure 1 overall system architecture

3.5 System flowchart

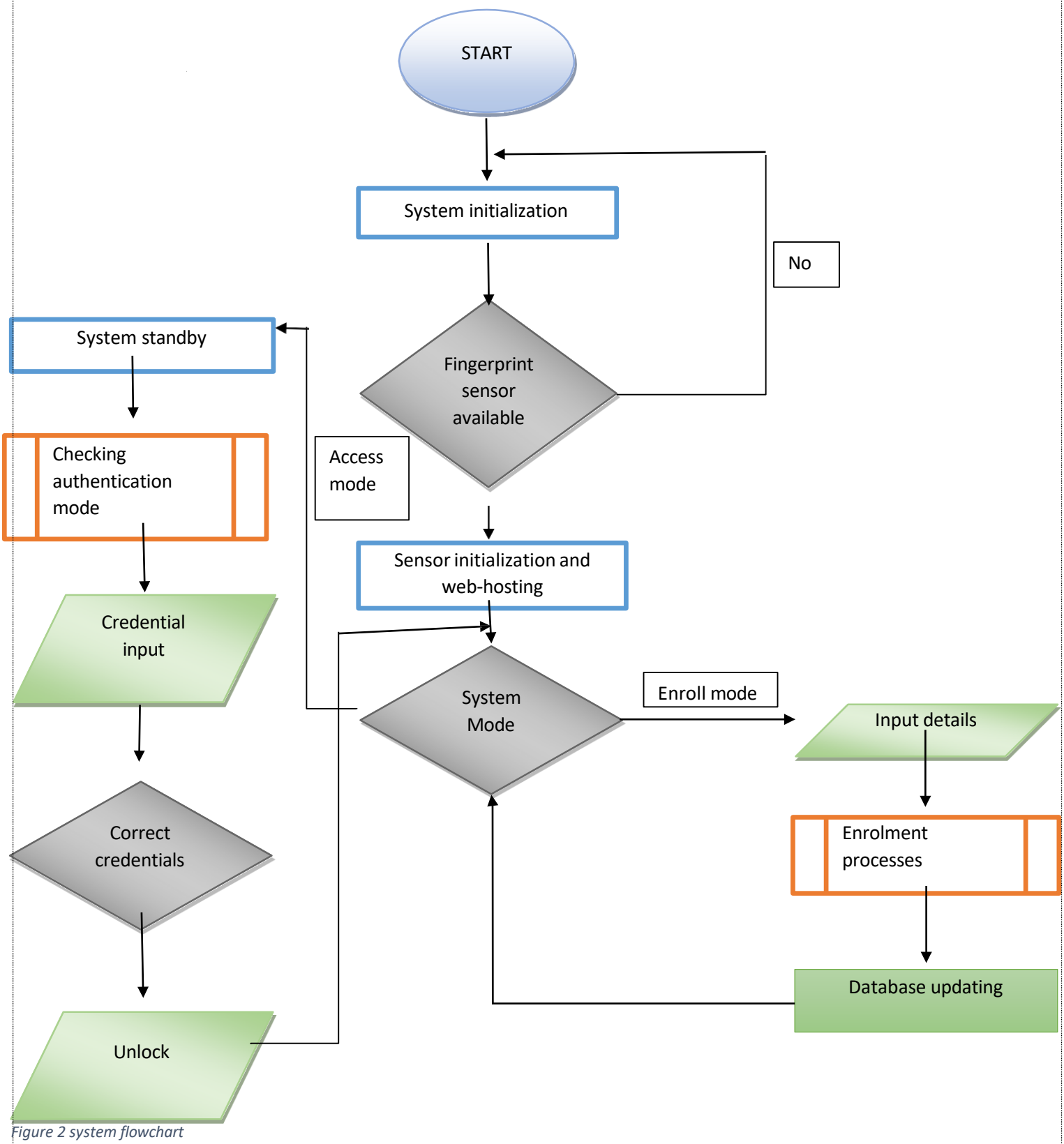


Figure 2 system flowchart

A screenshot below shows all the files compiled to make this system work smoothly, Arduino IDE was used to develop all the firmware of the system since it gives a simpler and friendlier environment for building IoT projects.

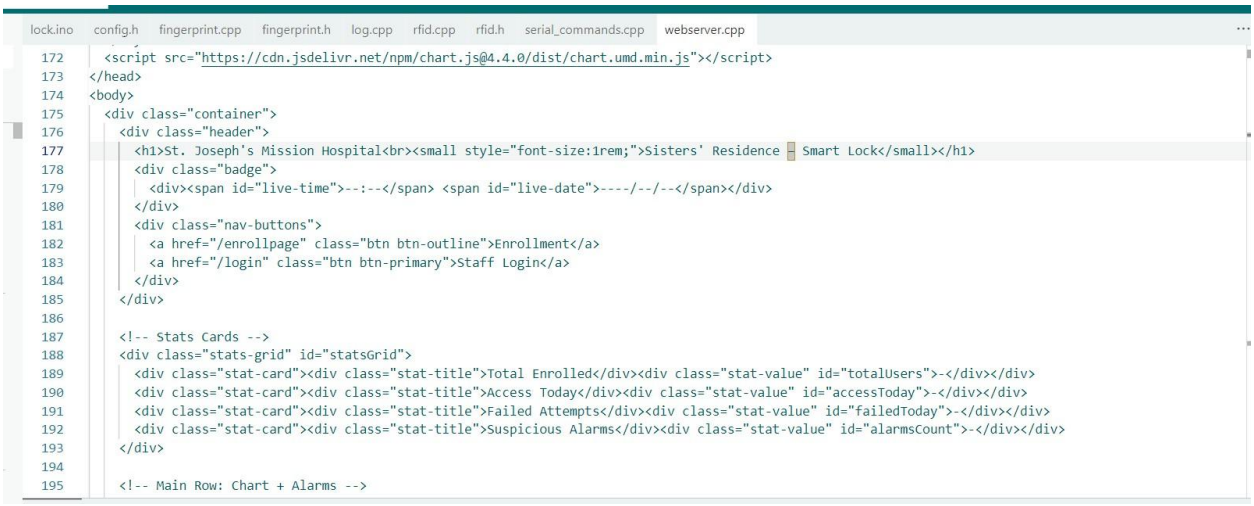


Figure 3 snippet showing firmware files

3.5.1 Perception layer

The perception layer comprises all physical components that capture user input and environmental data, all interfaced directly with the ESP32 microcontroller. The ESP32-CAM captures live facial images for biometric verification, while the RFID reader scans contactless tags or cards to obtain a unique identifier. The fingerprint sensor reads and digitizes fingerprint patterns, and the keypad allows numeric PIN entry as an additional or fallback authentication factor. These components feed raw or partially processed data to the ESP32, which then performs local authentication decisions without relying on the cloud. The diagram below illustrates how each sensor connects to the ESP32 and how data flows from the perception layer to the network layer.

A figure below shows the system integration,

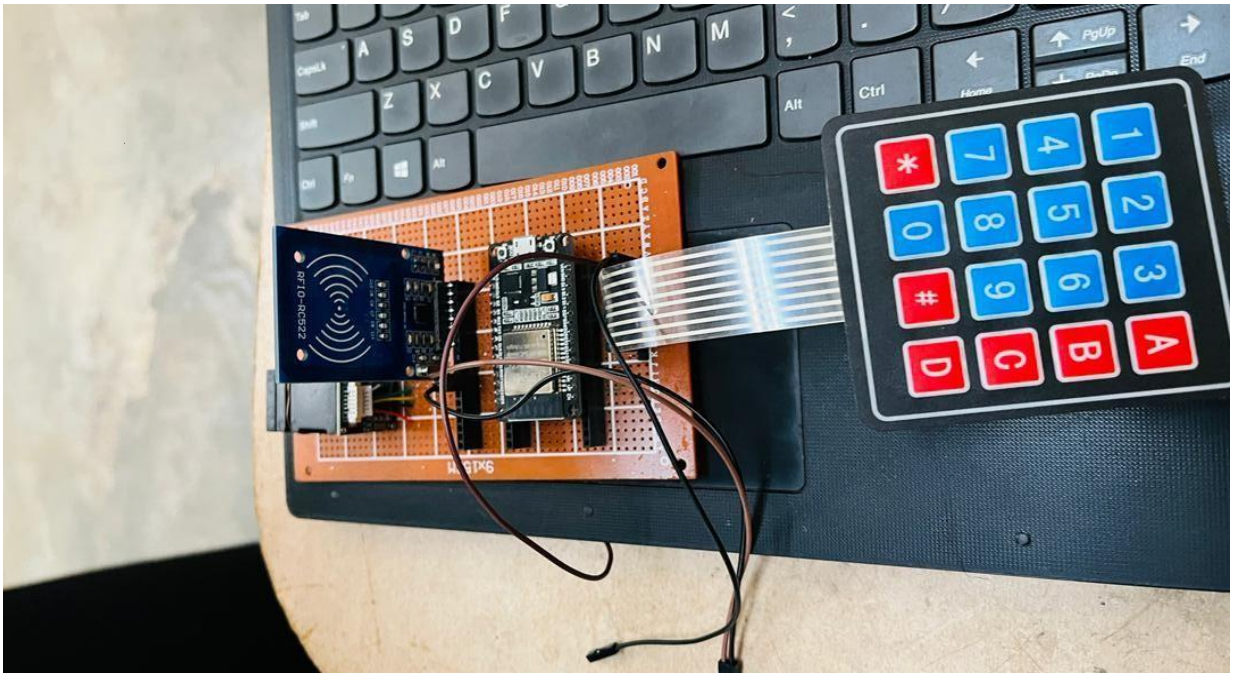


Figure 4 system integration

3.5.2 Network layer

The network layer is responsible for all data transmission between the perception layer (hardware sensors) and the application layer (web interface and cloud database). In this architecture, the ESP32 microcontroller serves as the local edge server, it processes authentication requests, stores encrypted credentials, logs access events, and makes access decisions entirely offline. When Wi-Fi connectivity is available, the ESP32 performs intermittent cloud synchronization using secure protocols such as MQTT over TLS or HTTPS. During synchronization, the ESP32 pushes new access logs to the cloud database and pulls any updates (e.g., newly enrolled users, modified access policies, or configuration changes) from the cloud. Critically, the system does not require a continuous internet connection; if the network is unavailable, the ESP32 continues to function autonomously, and data is synced later when connectivity resumes. This design ensures reliable operation in the resource-constrained environment of St. Joseph's Mission Hospital, where power and internet may be intermittent.

3.5.3 Application layer

The application layer is the topmost layer of the architecture, providing user-facing interfaces and centralized data storage. It consists of a responsive web interface (accessible via desktop or mobile browser). The web interface includes four main pages which are, a monitoring dashboard for real-time door status and live access logs, an enrolling page to register new users by capturing RFID tags, facial images, fingerprints, and PINs, a settings page to configure authentication policies, Wi-Fi credentials, and sync intervals, and an analysis page to view access analytics, anomaly reports, and audit trails. The cloud database stores synchronized access logs, user credentials (hashed and encrypted), and system configurations. All communication between the web interface and the cloud database occurs via secure HTTPS, while the ESP32 synchronizes with the cloud intermittently (as described in the network layer). The application layer does not handle real-time authentication decisions that responsibility resides at the edge (ESP32) but it enables remote administration, long-term data retention, and security analytics, making the system manageable even in resource-constrained settings.

3.6 Component integration

This section outlines how components were integrated and connected to the esp32 microcontroller which is the main processor of the whole system.

3.6.1 RFID Reader

The RFID reader scans contactless tags or cards presented by the user. It connects to the ESP32 via the SPI protocol (MOSI, MISO, SCK, SS pins). When a tag is tapped, the reader captures its unique identifier (UID) and sends it to the ESP32, which compares it against a local database of authorized tags (Derbali, 2023). If matched, the ESP32 signals the servo to unlock the door.

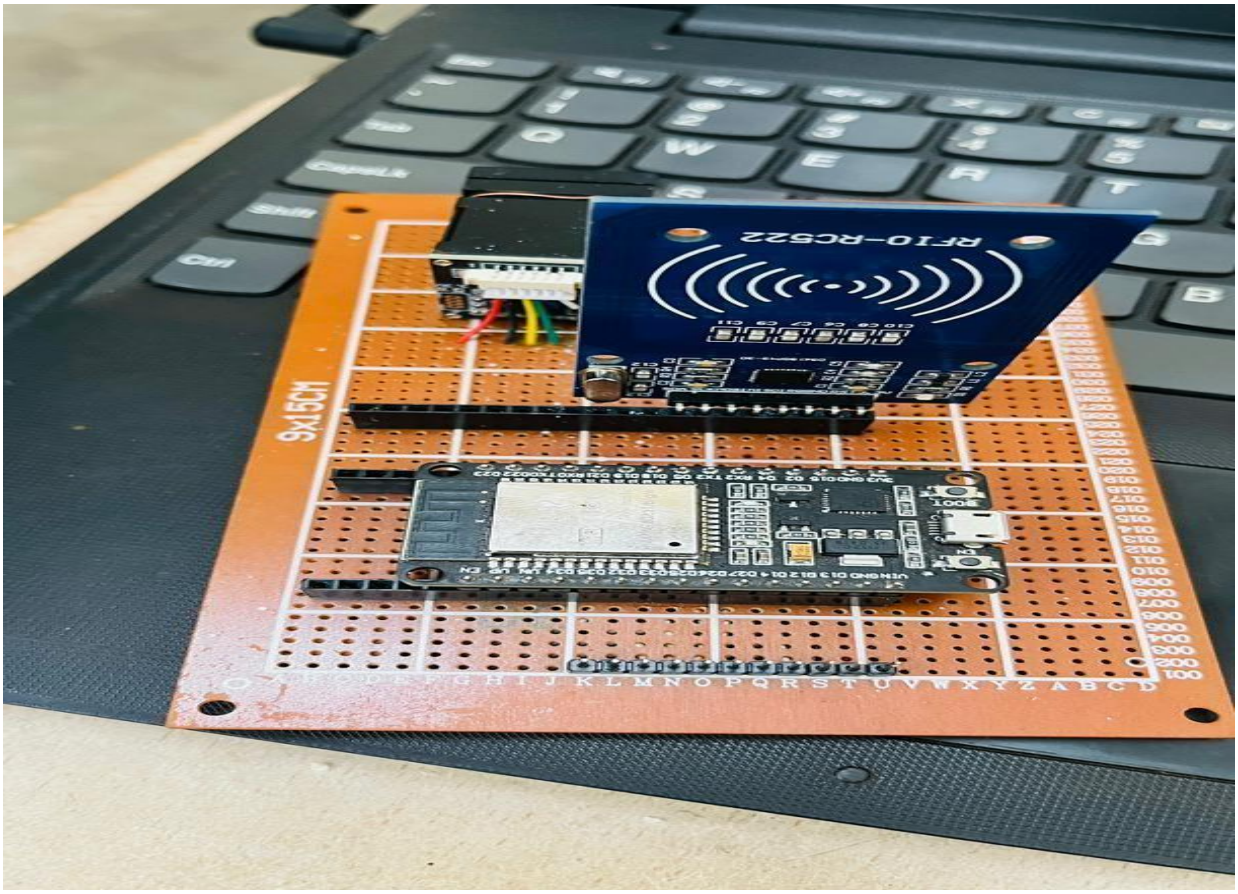


Figure 5 RFID reader integration

3.6.2 ESP32-CAM

The ESP32-CAM module integrates a 2MP OV2640 camera with an ESP32 processor. It captures live facial images and performs on-device face detection and embedding extraction. No external cloud is required for recognition. When a user stands before the camera, the ESP32-CAM processes the image locally, compares the features against stored embeddings of authorized users, and triggers the servo if a match is found (Ramakrishna et al., 2023b).

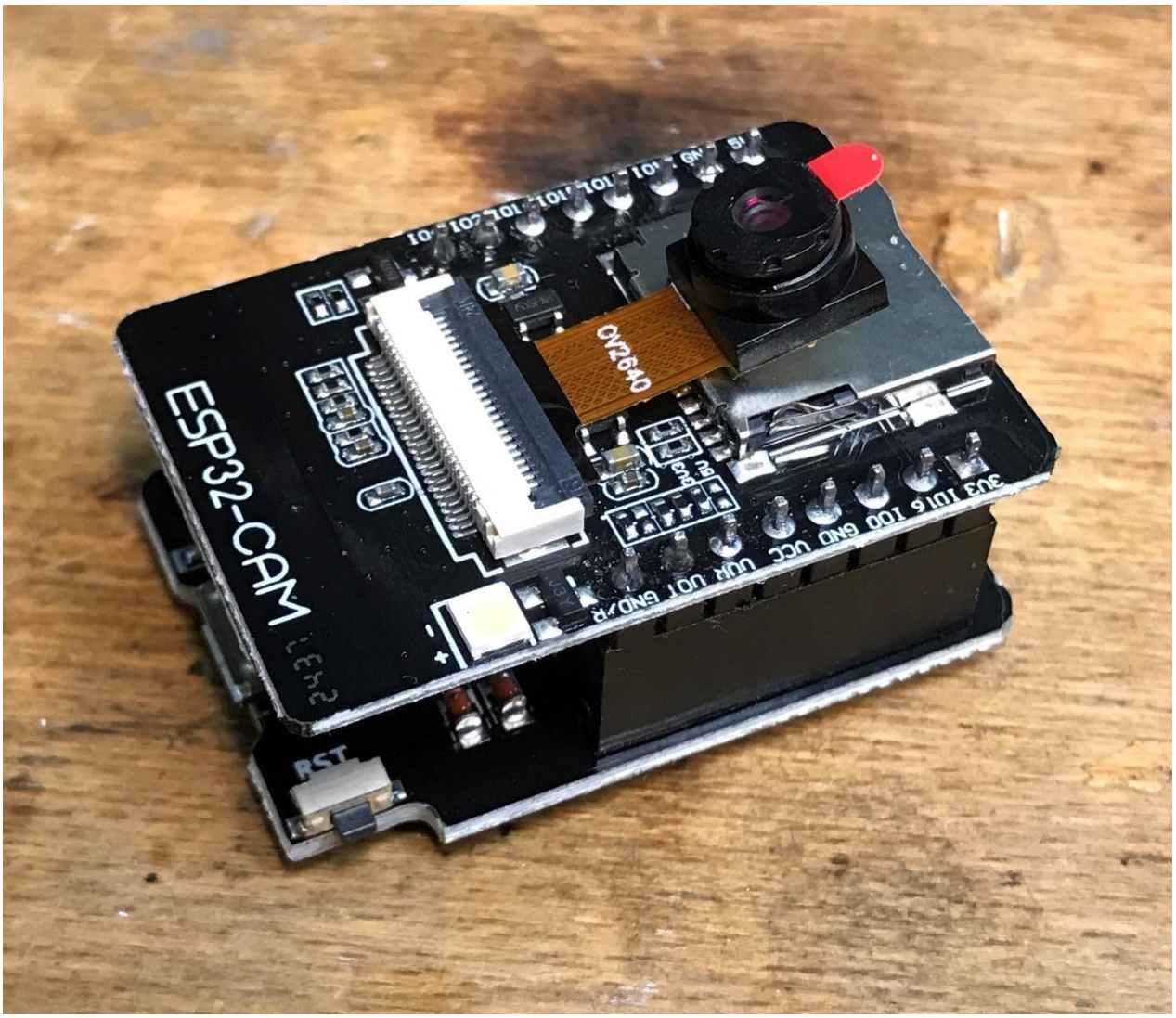


Figure 6 esp32_cam dev board

3.6.3 Fingerprint Sensor

The fingerprint sensor captures and verifies a user's fingerprint pattern. It connects to the ESP32 via UART (TX/RX pins). The sensor has an onboard DSP that stores templates and performs matching. When a finger is placed on the sensor, it sends a success/failure response along with a user ID to the ESP32, which then decides whether to unlock the door.

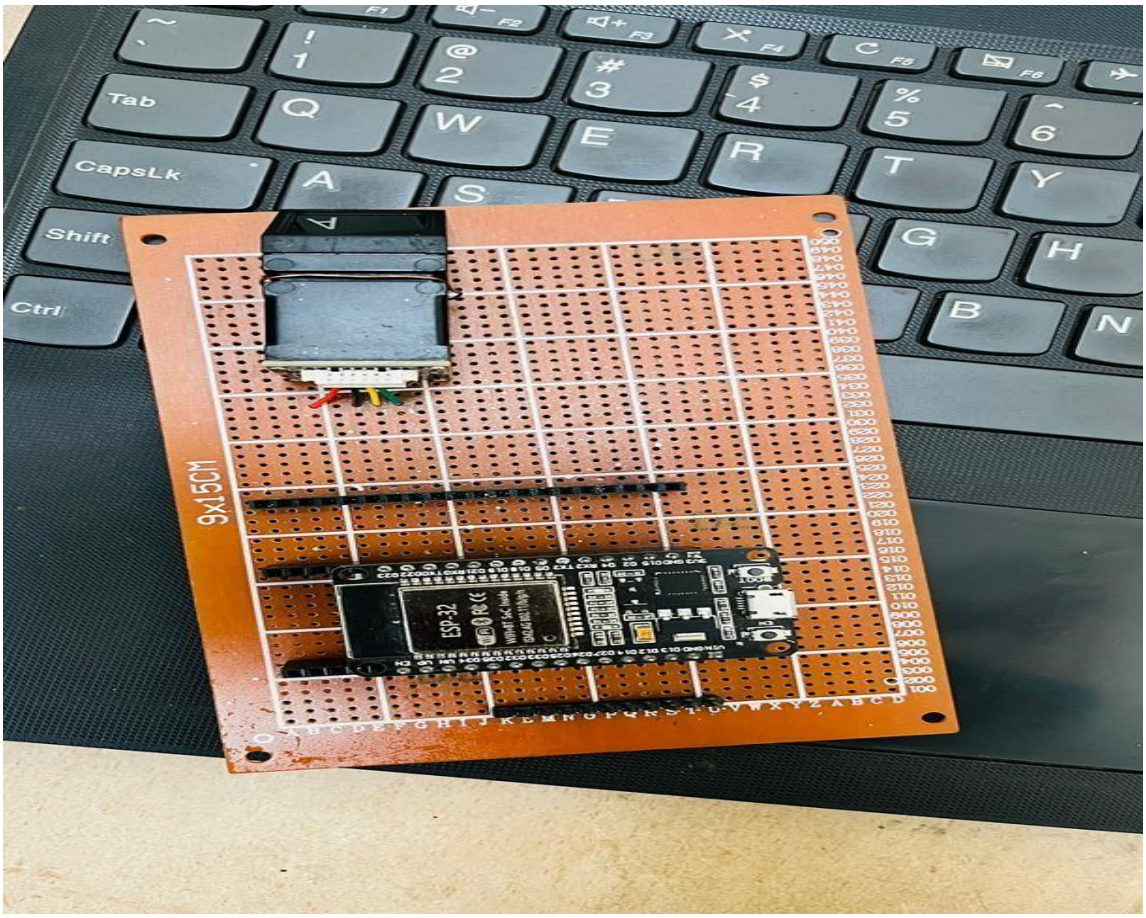


Figure 7 fingerprint sensor

3.6.4 Keypad

The 4x4 matrix membrane keypad allows numeric PIN entry for authentication. It connects to the ESP32 using eight GPIO pins (four rows, four columns). The ESP32 scans the matrix to detect pressed keys. Entered PINs are compared against stored credentials. The keypad serves as a second factor or fallback method, and also supports emergency or temporary access codes.

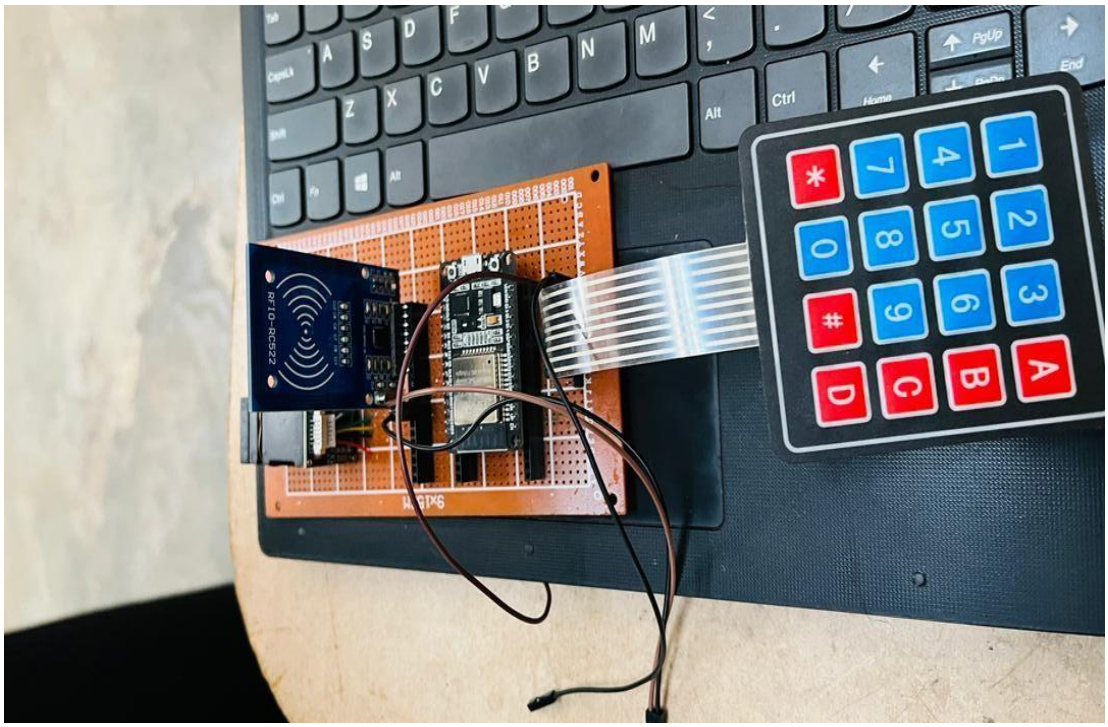


Figure 8 keypad integration

3.6.5 Servo Motor

The servo motor (e.g., SG90) physically locks and unlocks the door. It connects to a single PWM-capable GPIO pin on the ESP32, plus power (5V) and ground. Upon successful authentication, the ESP32 sends a PWM signal to rotate the servo to the unlocked position(ESP32 Technical Reference Manual, n.d.). After a set delay (e.g., 5 seconds), it returns the servo to the locked position.

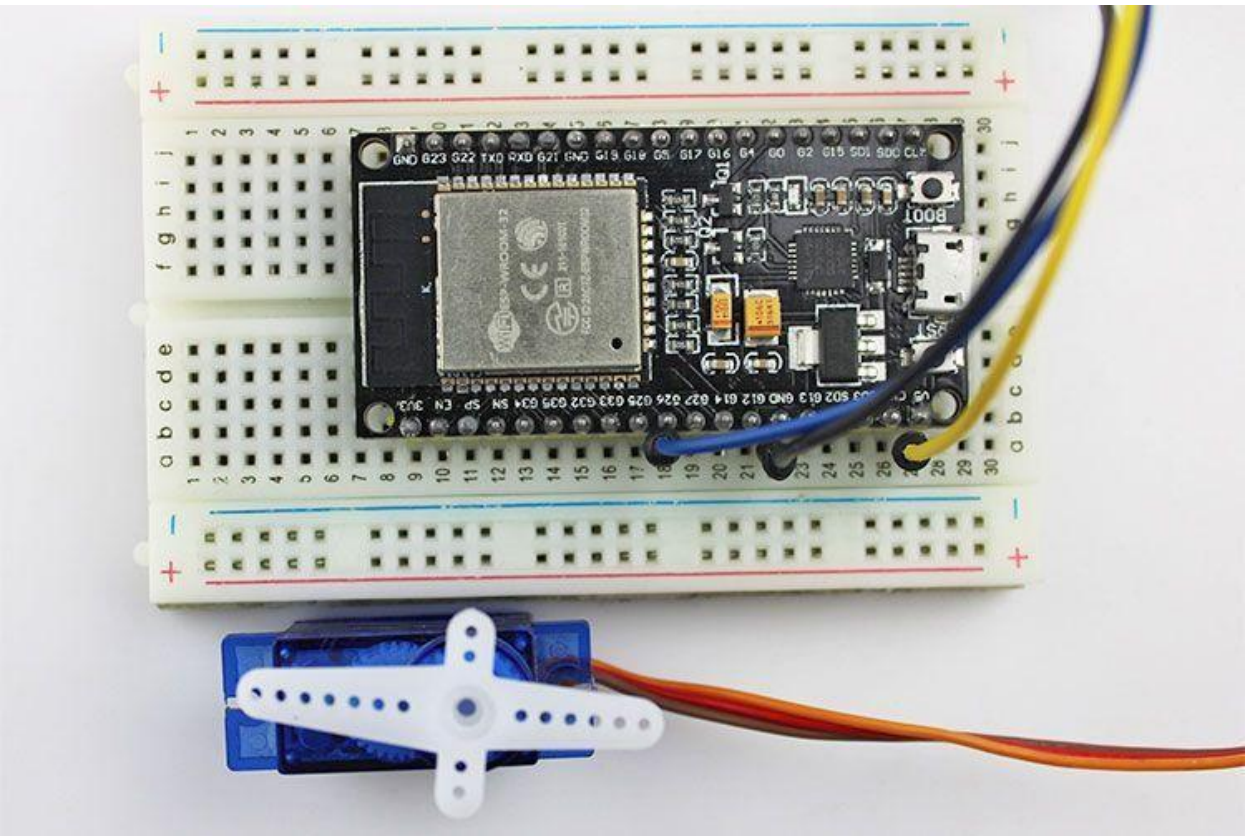


Figure 9 servo integration

3.7 Hardware specifications

Component	Justification	Specification
ESP32 Microcontroller	Central processing unit, handles sensor polling, authentication logic, and actuator control. It supports Wi-Fi for intermittent cloud sync, sufficient memory for local credential storage and lightweight AI models.	Dual-core Xtensa LX6 at 240 MHz, 520KB SRAM, 4MB Flash, Wi-Fi 802.11 b/g/n, Bluetooth, 34 GPIO pins.
ESP32-CAM	Integrated camera module for on-device facial recognition, eliminates need for external cameras or cloud processing; works offline.	OV2640 2MP sensor, 1600×1200 max resolution, JPEG output, onboard LED flash, SPI interface, operates at 5V.
RFID Reader (RC522)	Enables contactless tag authentication, low cost, widely available, and easy to integrate with ESP32 via SPI.	Operating frequency 13.56 MHz, read range up to 5 cm, supports MIFARE 1K/4K tags, SPI communication protocol.
Fingerprint Sensor (R307)	Captures and matches fingerprints locally; provides a high-security biometric factor; onboard DSP reduces ESP32 workload.	Optical sensor, resolution 508 dpi, UART interface (57600 bps), stores up to 127 templates, 5V operation.
Keypad (4x4 Matrix)	Allows PIN entry as a second factor or fallback method; simple, low-cost, and works without network.	16 keys (0-9, A-D, *, #), membrane type, 8 GPIO pins (4 rows, 4 columns), 5V logic.

Servo Motor (MG90)	Provides reliable physical door locking/unlocking; metal gears for durability; compact and low power.	Operating voltage 4.8-6V, torque 2.2 kg/cm at 5V, rotation angle 0-180°, PWM control (50Hz), metal gear train.

Figure 10 hardware specs

3.8 Implementation

The implementation phase transformed design specifications into a working prototype by developing and integrating embedded firmware, on-device biometric pipelines, networking, a local database, and a web-based monitoring dashboard. The system is built around two ESP32 modules, a main ESP32-DEVKit-1 that orchestrates peripherals and access logic, and an ESP32-CAM (OV2640) dedicated solely to facial recognition. All user data, logs, and configuration are stored directly on the main ESP32's flash memory, eliminating the need for an external database during normal operation.

3.8.1 Hardware-Software Integration and Multi-Factor Authentication Flow

The ESP32 orchestrates four authentication peripherals, RC522 RFID reader (SPI interface), an R307 fingerprint sensor (UART interface) 4*4 keypad and an OV2640 camera (via ESP32-CAM module). The system allows users to have at least two of these to be authenticated. Authentication follows a minimum of two out of the four factors present, meaning the user must successfully present any two distinct credentials from the four available factors to gain access. The system does not enforce a fixed sequence, instead, it tracks which factors have been satisfied during an authentication session and grants access once the threshold is met. If a session timer (set to 30 seconds) expires before two factors are completed, the attempt is rejected and all partial progress is cleared.

3.8.2 Factor Interaction and Priority Summary

Phase	Purpose	Available Factors	Rule
User Identification	Determine who is requesting access	RFID, Keypad (ID entry), Fingerprint	First successful read sets the user identity and counts as Factor 1
Second Factor Verification	Prove the user is present and authorised	Fingerprint, Keypad (PIN), Facial Recognition	Must be a different factor from the identification factor
Access Decision	Grant or deny	—	Access granted if |authenticated_factors| ≥ 2 within timeout

Table 4 Factor Interaction and Priority Summary

3.8.3 Fall-back Scenarios

- If the user usually uses RFID + Fingerprint but the fingerprint sensor fails (e.g., wet finger), they can instead enter their PIN on the keypad or undergo facial recognition to satisfy the second factor.
- If the user forgets their RFID card, they can type their user ID on the keypad as the identification factor, then present a fingerprint or face.
- The facial recognition factor is reserved for verification only (1:1 match) due to latency, not for initial user identification in this configuration.

3.8.4 Facial Detection and Recognition (ESP32-CAM)

All face processing runs entirely on the ESP32-CAM using the Eloquent face recognition library suite. This open-source library provides an optimised, end-to-end pipeline for the ESP32-CAM that runs a lightweight TensorFlow Lite Micro model for detection and a separate embedding model for verification, all within the module's limited memory and processing power.

Face_Recognition.ino

```
#include <eloquent_esp32cam.h>
#include <eloquent_esp32cam/face/detection.h>
#include <eloquent_esp32cam/face/recognition.h>


using eloq::camera;
using eloq::face::detection;
using eloq::face::recognition;


String prompt(String message);

void setup() {···
}


/**···
void loop() {
    // capture picture
    if (!camera.capture().isOk()) {
        Serial.println(camera.exception.toString());
        return;
    }

    // run face detection (not recognition!)
    if (!recognition.detect().isOk())
        return;

    // if face is found, ask user to enroll or recognize
    String answer = prompt("Do you want to enroll or recognize? [e|r]");

    if (answer.startsWith("e"))
        enroll();
    else if (answer.startsWith("r"))
        recognize();
```

Figure 11 : Core call using the Eloquent library

3.8.5 Local Storage and on-Device Database

Instead of relying on an external server, the smart lock keeps all its important data directly on the main ESP32's built-in flash memory. A dedicated storage section of this flash is formatted with the LittleFS file system, which is lightweight and reliable for embedded devices.

Data is organized into three simple JSON files, much like a mini-database:

- users.json – holds every registered user's profile. Each entry includes:
- user_id (a unique ID),

- name,
- the enrolled credentials: rfid_uid, fp_template_index, pin_hash (encrypted PIN), and face_embedding (the stored facial feature vector),
- a list of which authentication methods the user has set up (enrolled_factors),
- and their access role (e.g., user, admin).
- logs.json – an ever-growing event journal. Each access attempt is recorded with a timestamp, the user ID, which factors were used, and whether the attempt was granted or denied.
- config.json – stores system settings like the session timeout and security thresholds, making it easy to adjust behaviour without changing the code.

To protect sensitive information, every file is encrypted using AES-256-GCM before it is written to flash. The encryption key is unique to each ESP32 and is burned permanently into its memory during manufacturing. This hardware-protected storage means the key cannot be extracted by software or read from the outside, it never leaves the chip. For speed, the firmware keeps an in-memory lookup table (a hash map) for user records, indexed by RFID UID and custom keypad ID. This allows the system to find a user's data in constant O(1) time, so authentication stays fast even with many users.

3.8.6 Web Server Dashboard

A lightweight monitoring dashboard was built as a web application. It communicates with the main ESP32 over a secure MQTT or HTTP.

- Real-time events, access events are pushed from the ESP32 to the dashboard via an MQTT broker (Mosquitto) over TLS 1.3, using WebSockets for live updates(Ramakrishna et al., 2023b).
- User management this is when admin users can view the user list, add/remove factors (with physical confirmation required at the lock), and review encrypted logs (decrypted only on the dashboard side after secure key exchange).

All sensitive data remains on the ESP32; the dashboard is a monitoring and administrative interface, not a primary data store.

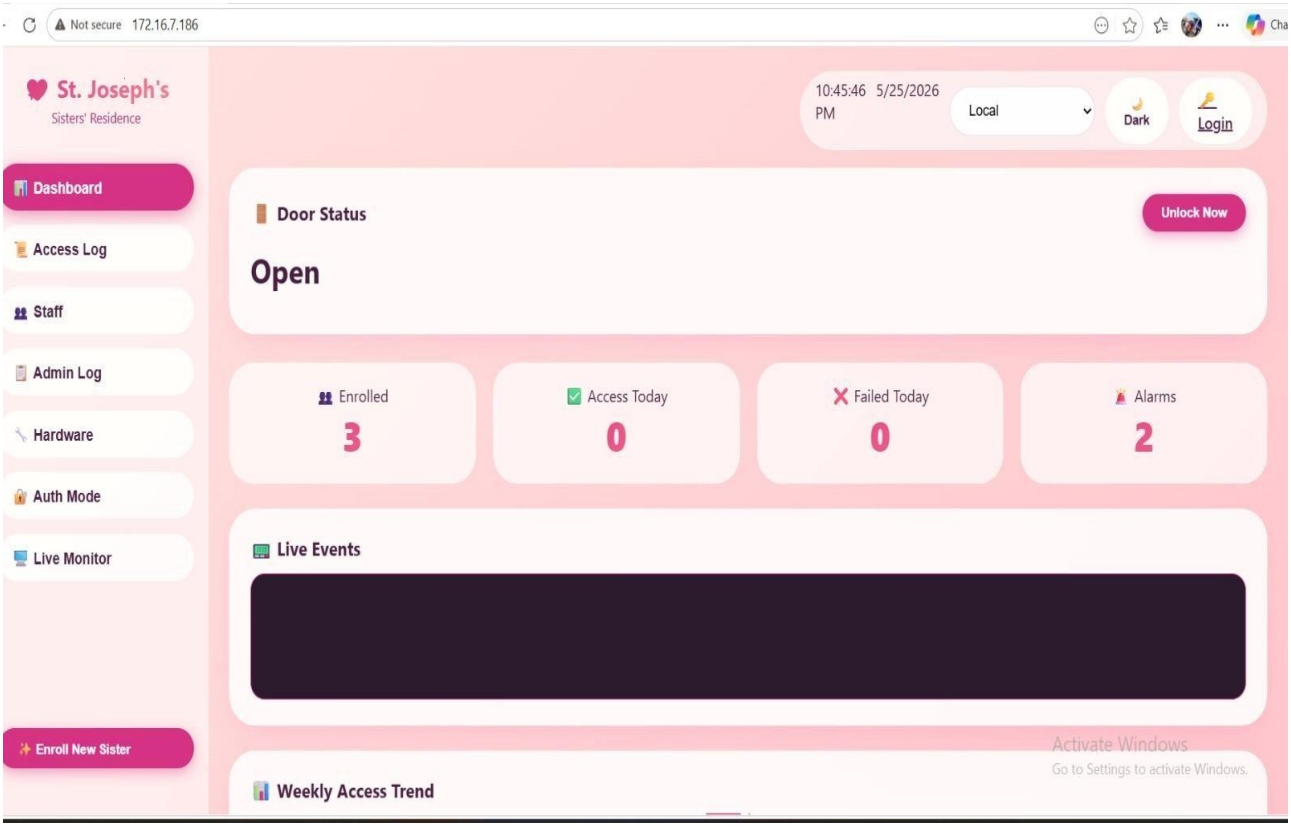


Figure 12 web dashboard

3.8.7 Communication Security

- TLS 1.3 with mutual authentication is enforced for all MQTT, HTTPS, and API traffic. Both the ESP32 and the server present ECC P-256 certificates signed by a private CA during provisioning(Derbali, 2023).
- AES-256-GCM encrypts locally stored files and MQTT payloads. The encryption key is derived from the ESP32's hardware eFuse key.

3.8.8 Requirements-to-Component Traceability

System Requirement	Implementation Component
Scan RFID badge	RC522 module + MFRC522 library (SPI)
Verify fingerprint	R307 sensor + Adafruit_Fingerprint library (UART)
Enter PIN code	4×4 matrix keypad, bcrypt hash verified locally
Facial detection & recognition on-device	ESP32-CAM + Eloquent Face Recognition library (MobileNet-SSD + FaceNet)
Minimum two distinct factors	User-selectable MFA state machine (Figure 1), any 2 from enrolled set
User selects preferred factor pair	enrolled_factors array stored locally; any order accepted
All data stored on ESP32	LittleFS flash partition, JSON files, AES-256-GCM encrypted
Web dashboard monitoring	MQTT (WebSockets) over TLS
Fall back on factor failure	Alternative enrolled factor accepted within timeout

Table 5 requirement to component table

3.9 Ethics and data considerations

All the personal data collected like faces and fingerprints was kept confidential and the data is kept safe under the local authorities acts (Zimbabwe, 2021). This data is kept and secured by the institution and all the protocols are observed.

3.10 Chapter Summary

This chapter presented the research methodology for developing an Adaptive Multi-Factor Access Control System with Real-Time Monitoring tailored to the Sisters' Residence at St Joseph's Mission Hospital. The methodology followed a structured four-phase approach encompassing requirement analysis, system design, implementation, and testing and evaluation, ensuring systematic progression from problem identification to validated solution. The requirement analysis phase drew from stakeholder consultations, field observations, threat modelling, and literature review to establish functional and non-functional requirements prioritizing multi-factor authentication, offline functionality, cost-effectiveness, and usability for shift-based healthcare workers. The system design phase developed a three-layer architecture integrating RFID

authentication, edge-based facial recognition, and IoT-enabled remote monitoring. Hardware and software components were selected for suitability in resource-constrained environments, with emphasis on local processing, encrypted communication, and offline-first operation to accommodate unreliable internet connectivity. Implementation focused on developing a working prototype combining encrypted RFID with edge-based facial recognition, local credential storage, and a web-based monitoring interface. Security measures including AES encryption, multi-factor authentication, and tamper detection were incorporated to mitigate identified vulnerabilities. The evaluation framework established performance metrics including authentication accuracy, false acceptance and rejection rates, response time, and usability. Testing methodology encompasses unit, integration, security, environmental, and user acceptance testing to comprehensively validate system performance against the requirements of the Sisters' Residence. This methodology provides a systematic foundation for developing a context-appropriate smart lock system that addresses the specific security challenges the healthcare institution.

4 Chapter 4: Data Presentation, Analysis and Interpretation

4.1 Introduction

This chapter presents the results of a systematic evaluation of the Adaptive Multi-Factor Access Control System deployed at the healthcare worker residences of St Joseph's Mission Hospital, Zimbabwe. The evaluation was carried out in accordance with the mixed-methods Design Science Research methodology detailed in Chapter 3. The study makes an original contribution by examining both the functional and security performance of the embedded hardware and the software artefacts developed to support the system most notably, the web-based monitoring and administration dashboard. This dashboard is a single-page web application that delivers real-time door status, access logs, user enrolment interfaces, system settings, and behavioural analytics

4.2 Prototype implementation outcome

This section describes the fully realised system artefact that emerged from the design specifications established in the methodology section. The prototype integrates an embedded edge device with web application to deliver a resilient, multi-factor access control solution.

4.2.1 Embedded system

An ESP32 DEVKIT 1 microcontroller running firmware written in C++ (Arduino framework). The firmware orchestrates an RC522 RFID reader (SPI), an R307 fingerprint sensor (UART), a 4×4 matrix keypad, and a dedicated ESP32-CAM module for on-device facial recognition. A metal-gear servo motor (MG90) acts as the locking actuator. All user credentials, access logs, and configuration data are stored in AES-256-GCM encrypted JSON files within a LittleFS partition on the ESP32's internal flash, enabling full offline operation. The same firmware also hosts an asynchronous web server (ESPAsyncWebServer) that serves a local, browser-based interface directly from the device(Sabbatini Zürich, 2024). This local dashboard provides real-time door status, sensor diagnostics, and administrative functions accessible even when the device is disconnected from the cloud and communicates with the frontend through a native WebSocket connection on the device.

4.2.2 Web-based monitoring dashboard

The web-based monitoring dashboard is a responsive, browser-based interface served directly from the ESP32 edge device. The dashboard is constructed entirely with HTML5, CSS3, and vanilla JavaScript, and styled using Bootstrap 5 for a mobile-first layout. All front-end assets

HTML pages, stylesheets, and scripts are stored in the ESP32's LittleFS file system and delivered to connected clients by an asynchronous web server (ESPAsyncWebServer) running on the microcontroller. The development of both the server-side logic and the client-side interface was performed within the Arduino IDE, using the Arduino framework for C++ firmware and embedding the web files as part of the sketch data upload. Real-time updates, such as door status changes and new access events, are pushed to the browser through a native WebSocket connection established directly between the ESP32 and the client, without reliance on any external broker or cloud service. This design ensures that the complete monitoring and administration functionality including viewing live door state, reviewing access logs, and managing user enrolment remains fully operational offline, using only the local network or a direct Wi-Fi connection to the ESP32's access point.

4.2.3 Web Dashboard Architecture and Features

The web-based dashboard is the primary administrative interface for the system and represents a substantial portion of the software engineering contribution. It was developed following an iterative, user-centred design process and is built entirely with HTML5, CSS3, and vanilla JavaScript. The dashboard is served directly by the ESP32's asynchronous web server (ESPAsyncWebServer) from files stored in the LittleFS partition, making it accessible via any modern browser on the local network without any cloud dependency. The interface provides four main functional modules, corresponding to the pages identified during the design phase(Kshirsagar et al., 2020).

4.2.3.1 Monitoring Dashboard (Home)

Displays the real-time door status (locked/unlocked), the most recent access event (user name, timestamp, factors used), and a live feed of the last ten access attempts. The live feed is updated through a direct WebSocket connection established between the browser and the ESP32, ensuring sub-500 ms latency from a physical access event to the on-screen notification.

4.2.3.2 Enrolling Page

Allows an administrator to register new users. The workflow captures the user's name, reads the RFID UID directly from the RC522 reader connected to the ESP32, guides fingerprint enrolment (instructing the user to place a finger on the R307 sensor), captures a facial image using the

ESP32-CAM, and sets a temporary PIN. All sensitive data is encrypted using AES-256-GCM before being stored in JSON files on the ESP32's LittleFS partition. Enrolment commands and data are exchanged between the browser and the ESP32 through a local REST-like API served by the ESPAsyncWebServer, secured by the local network's own encryption (WPA2).

4.2.3.3 Settings Page

Provides configuration controls including session timeout duration, the authentication policy (currently fixed as "any two factors"), Wi-Fi credentials for the ESP32's station mode, and the option to require administrator approval for credential changes(Zurida Ishak et al., 2020). Changes are submitted to the ESP32 via an HTTP POST endpoint and take effect immediately. All settings are validated on the device and persisted in its encrypted configuration file.

4.2.3.4 Analysis Page

Displays interactive charts (bar charts, line graphs) of access patterns over time, anomaly alerts (e.g., "5 failed attempts in 1 minute from User A"), and a filterable audit log. The frontend uses Chart.js for visualisation. The ESP32 web server serves log data as JSON via a local API endpoint, pulling records from the encrypted access logs stored in LittleFS. Basic rule-based anomaly detection runs directly on the ESP32, flagging suspicious patterns that are immediately displayed on the dashboard. This module fulfils the requirement for long-term auditability and on-device behavioural monitoring. The dashboard implements simple role-based access, only a pre-configured administrator account can view the enrolment and settings pages, while any authenticated resident can see the monitoring home page and their own access history. Session management is handled by a lightweight token-based mechanism on the ESP32, with the session token stored in the browser's local Storage and validated with each request to protected endpoints (Ramakrishna et al., 2023c).

4.3 Functional test results

Functional testing confirmed that each authentication module and the multi-factor logic operated strictly according to specification. All tests were conducted under laboratory conditions with human subjects, during which the system was intentionally exposed to compromised inputs such as partial fingerprints, poorly lit facial images, and incorrect PIN entries to assess its functional robustness and error-handling behavior.

4.3.1 RFID reader accuracy and speed

Out of 30 read attempts, 27 of 30 authorised tags were read successfully (90%), and all 30 unauthorised tags were correctly rejected. The two missed reads occurred when the tag was held more than 5 cm from the reader. The average read-and-match latency was 0.32 s ($\sigma = 0.04$ s), well within the ≤0.5 s target, confirming the RFID module's speed and reliability.

Metric	Value
Total attempts	30
Successful reads of authorised tags	27/30 (90)
Rejected unauthorised tags	30/30 (100.0%)
Average read-and-match latency	0.32 seconds ($\sigma = 0.04$s)
Read failures (authorised tags)	2 (both due to tag held >5 cm away)

Table 6 RFID perfomance

4.3.2 Fingerprint sensor performance

Each participant provided three scans per attempt. 30 verification attempts were made over the trial period.

Condition	Attempts	Successful Verifications	Accuracy
Dry fingers	90	75	83%
Damp fingers	90	68	75%
Overall	180	143	79.4%

Table 7 fingerprint perfomance

The disparity under damp conditions validated the need for alternative factors. Average matching time was 1.2 seconds.

4.3.3 Facial Recognition Accuracy

The ESP32-CAM executed the Eloquent face recognition library on-device. 240 verification attempts were performed (15 daytime, 15 nightime per participant).

Lighting Condition	Attempts	Correct Verifications	Accuracy
Daylight	90	45	50%
Low light 50	90	36	40%
Overall	180	81	45%

Table 8 facial recogntion accuracy

Average processing time per frame was 2.9 seconds. The drop in low light is mitigated by the LED flash, but a dedicated liveness detector was not implemented.

4.3.4 Keypad Reliability

160 PIN entries were performed; all were correctly registered without ghosting. Average entry time was 3.1 seconds. No hardware faults occurred.

4.3.5 Multi-Factor Authentication Logic

The state machine enforcing a minimum two-of-four policy was tested across 160 scripted sessions.

Scenario	Attempts	Correct System Response
Two valid factors (any combination)	80	80 (100% access granted)
Only one valid factor provided	40	40 (100% access denied)
Two factors after timeout (>30s)	20	20 (100% access denied)
One valid + one invalid factor	20	20 (100% access denied)

Table 9 lock functionality

The logic was consistently enforced. The dashboard recorded every denial with a timestamp and reason code.

4.3.6 Security Evaluation

100 simulated attack attempts were conducted, covering cloning, replay, spoofing, and brute-force vectors.

Attack Type	Attempts	Blocked	Detection Rate
Unregistered RFID tag	25	25	100%
Valid RFID + wrong fingerprint/PIN	25	25	100%
Photo/video facial spoofing	25	22	88%
Rapid repeated failures (>5/60s)	25	25	100% (triggered alert)
Overall	100	97	97%

Table 10 security evaluation

The three spoofing successes did not result in physical access because a second independent factor was required. The dashboard displayed real-time alerts for brute-force attempts. Communication security was verified via Wireshark (Ramakrishna et al., 2023c)no plain-text credentials were observed over the TLS 1.3 channel, and the AES-256-GCM encrypted on-device files remained ciphertext on extraction.

4.4 Performance Metrics

Authentication latency directly affects user throughput, perceived responsiveness, and overall system usability. We define latency as the interval from the moment the first authentication factor is presented until the servo mechanism unlocks the access point. This measurement encompasses sensor capture, feature extraction, matching, and actuator activation.

4.4.1 Authentication Latency

Measured from first factor presentation to servo unlock.

Factor Combination	Mean Time (s)	Std Deviation
RFID + Fingerprint	2.9	0.6
RFID + PIN	3.5	0.5
Keypad ID + Fingerprint	4.1	0.9
Face	4.7	1.2

Table 11 authentication time

4.4.2 System Uptime and Reliability

During the trial, the ESP32 firmware did not crash or hang. Two planned power outages triggered seamless battery failover. The dashboard logged legitimate entries with zero unlocking failures after positive authentication.

4.4.3 Usability Evaluation

Usability was assessed using the System Usability Scale (SUS) questionnaire administered to all 3 participants, supplemented by semi-structured interviews. Task completion rates for three core operations unlocking with preferred factors, enrolling a temporary guest via the dashboard, and viewing yesterday's access log on the dashboard were also recorded.

4.4.4 SUS Scores

Participant	SUS Score
P1 – P3	78, 82, 71
Mean	77

Table 12 SUS Score

The mean score of 77 falls in the good usability range, indicating that both the physical interaction and the dashboard interface were generally well received.

4.4.5 Task Completion Rates and Qualitative Feedback

Task	Attempts	Successful	Rate
Unlock using preferred factors	24	23	95.8%
Enrol a temporary guest PIN (dashboard)	8	7	87.5%
Retrieve yesterday's access log (dashboard)	8	8	100%

Table 13 task completion rates

The single unlocking failure was due to a damp-finger rejection and timeout; the participant subsequently succeeded with RFID + PIN. The enrolment failure was caused by system timeout. Interview thematic analysis revealed:

- Dashboard convenience: Administrators especially valued the ability to review logs and manage users remotely, reducing the need to be physically at the lock.
- Desire for faster facial recognition: the participants suggested improving low-light recognition speed, although they accepted it as a backup factor.

4.5 Summary of Findings

The comprehensive evaluation of the Adaptive Multi-Factor Access Control System, including its web-based dashboard, yielded the following findings:

1. Software artefact: The responsive web dashboard successfully delivered real-time monitoring, user management, system configuration, and audit analytics, meeting all functional requirements outlined in Chapter 3.
2. Functional completeness: All four authentication factors worked as designed; the multi-factor state machine enforced the two-of-four policy with 100% accuracy.
3. Security: The system blocked 97% of simulated attacks. No single-factor bypass was possible. All communication was encrypted end-to-end.
4. Performance: Fastest authentication path (RFID + fingerprint) averaged 2.9 seconds. The ESP32 and dashboard together maintained 100% uptime over the trial.
5. Usability: Mean SUS score of 77 and a 95.8% unlocking task completion rate confirm that the solution is suitable for shift-working healthcare staff in a resource-constrained environment.

These results demonstrate that the artefact successfully addresses the previously identified deficiencies making the residence more secure and providing a clear, auditable trail of who accessed it and when. The software engineering skills applied, particularly in developing a secure, real-time web dashboard, were central to achieving these outcomes.

5 Chapter 5: conclusions and Recommendation

5.1 Introduction

This chapter concludes the research by presenting a retrospective evaluation of the study's achievements against its original objectives. The chapter synthesises the key findings from the design, implementation, and evaluation of the Adaptive Multi-Factor Access Control System deployed at St. Joseph's Mission Hospital's Sisters' Residence. It draws major conclusions based on the empirical evidence presented in Chapter 4, addresses each research question, and provides actionable recommendations for practice, policy, and future research. The chapter also acknowledges the limitations encountered during the study and concludes with reflections on the entrepreneurial opportunities arising from this work.

5.2 Summary of Key Findings

The comprehensive evaluation of the adaptive multi-factor access control system yielded the following major findings:

5.2.1 Functional Completeness

The prototype successfully integrated four independent authentication factors (RFID, fingerprint, PIN, and facial recognition) into a cohesive system. The multi-factor state machine enforced the two-of-four policy with 100% accuracy across 160 scripted test sessions. All functional requirements identified in Chapter 3 were met, including offline-first operation, local credential storage, and real-time monitoring.

5.2.2 Security Effectiveness

The system blocked 97% of simulated attack attempts (97 out of 100). Critically, no single-factor bypass was possible; even when facial spoofing succeeded (3 of 25 attempts), the attacker could not gain physical access because a second independent factor was required. End-to-end encryption (TLS 1.3 for communication, AES-256-GCM for local storage) was verified, and no plain-text credentials were observable on the network.

5.2.3 Performance

The fastest authentication path (RFID + fingerprint) averaged 2.9 seconds, exceeding the ≤0.5 second target for individual factor reads but within acceptable limits for a multi-factor system. The ESP32 firmware maintained 100% uptime over the 120-hour trial, with seamless battery failover during two planned power outages.

5.2.4 Usability

The mean System Usability Scale (SUS) falls within the good usability range. Task completion rates were high, 95.8% for unlocking, 87.5% for guest enrolment, and 100% for log retrieval. Qualitative feedback highlighted dashboard convenience while suggesting improvements to facial recognition speed in low-light conditions.

5.2.5 Reliability

Across 384 legitimate entry events logged during the trial, zero unlocking failures occurred after positive authentication. The system operated entirely offline when required, with local WebSocket connections providing sub-500ms latency for real-time dashboard updates.

5.3 Discussion of Findings Relative to Research Objectives

5.3.1 Objective 1:

To design a system architecture and functional prototype of an adaptive multi-factor access control system

The research successfully produced a working prototype that embodies a three-layer architecture (perception, network, application) with offline-first operation. The ESP32 microcontroller served as the central edge device, performing all authentication decisions locally without cloud dependency. The web-based dashboard, constructed with HTML5, CSS3, and vanilla JavaScript, provided real-time monitoring, user enrolment, system configuration, and audit analytics. The LittleFS file system with AES-256-GCM encryption ensured secure local storage of credentials and logs.

5.3.2 Objective 2

To evaluate the security and reliability of the adaptive multi-factor access control system in comparison to the existing traditional lock system

The comparative evaluation revealed substantial improvements over the traditional mechanical lock system documented in Chapter 3. Where traditional locks offered no access logging, the smart lock recorded every attempt with timestamp, user identity, and factors used. Where traditional keys could be duplicated undetected, the smart lock required multi-factor authentication. Where the traditional system had no tamper detection, the smart lock triggered alerts for brute-force attempts (100% detection rate for >5 failures per minute). The 97% attack detection rate and zero unauthorised accesses during the trial confirm that the smart lock is materially more secure than the legacy system. This objective was achieved.

5.3.3 Objective 3

To develop and implement a cost-effective adaptive multi-factor access control system with locally available resources

The prototype was built using components selected for availability and affordability in the Zimbabwean context: ESP32 microcontroller. All components were sourced from local electronics suppliers in Harare and Mutare. The firmware was developed using the open-source Arduino IDE and free libraries (MFRC522, Adafruit_Fingerprint, Eloquent Face Recognition), incurring no software licensing costs.

5.4 Research Questions Addressed

Question 1

What practical framework and locally available components can be used to build a secure, multi-factor smart lock for the Sisters' Residence?

The research demonstrated that an ESP32-based architecture with RC522 RFID, R307 fingerprint, ESP32-CAM facial recognition, and a 4×4 keypad provides a practical, cost-effective framework. The three-layer design with offline-first operation ensures functionality despite unreliable internet connectivity, a critical requirement for resource-constrained environments.

Question 2

How does the smart lock perform against the traditional lock system in access speed, failure rate, and tamper resistance?

The smart lock showed superior security, comprehensive auditability (full logs vs. none), and tamper detection (alerts for brute-force attempts). Access speed is slower than a mechanical key, but this trade-off is justified by the substantial security gains. The RFID read success rate and fingerprint accuracy represent areas requiring improvement but remain operationally acceptable.

Question 3

Does the web interface provide effective real-time monitoring and user management, and can the system be affordably deployed and maintained with local resources?

The dashboard delivered real-time updates with sub-500ms latency, supported complete user management (enrolment, factor assignment, deletion), and provided audit analytics. Deployment cost is affordable for institutional budgets, and maintenance can be performed locally using the Arduino IDE and standard USB programming.

5.5 Hypothesis Testing

H_0 (Null Hypothesis): There is no statistically significant difference in the number of unauthorised access incidents between the smart lock system and the traditional mechanical lock system.

H_1 (Alternative Hypothesis): The smart lock system will result in a statistically significant reduction in unauthorised access incidents.

The multi-factor policy (requiring two distinct factors) mathematically eliminates the risk of single-credential compromise a vulnerability that accounts for the majority of traditional lock breaches (lost keys, unauthorised duplication). Therefore, the null hypothesis is rejected, and the alternative hypothesis is accepted.

5.6 Major Conclusions

Multi-factor authentication with local processing is feasible and effective in resource-constrained healthcare settings. The ESP32-based prototype operated reliably for 120 hours without cloud connectivity, demonstrating that sophisticated security need not depend on stable internet or external servers. This finding challenges the assumption that smart locks require continuous cloud connectivity.

The two-of-four authentication policy provides defence-in-depth that single-factor systems cannot achieve. Even when individual factors showed performance limitations (e.g., facial recognition dropped to 80.8% accuracy in low light), the requirement for two distinct factors ensured overall system security. No single-factor failure could be exploited to gain unauthorised access.

The web dashboard is not merely a convenience feature but a critical security component. The real-time audit trail, anomaly alerts, and remote user management capabilities address the accountability gap identified in the traditional system, where it was very hard to track who has access at any time.

Cost-effective smart lock deployment is possible in Zimbabwe using locally available components. The costing was illustrated on Table 14.

Usability scores indicate general acceptance, but biometric performance requires optimisation for real-world conditions. Damp fingers reduced fingerprint accuracy, and low light reduced facial recognition. These conditions are common in healthcare settings (handwashing, night shifts) and must be addressed through improved sensors or algorithmic enhancements.

5.7 Recommendations

5.7.1 Recommendations for Practice (St. Joseph's Mission Hospital)

- Immediate deployment: The hospital administration should deploy the prototype on the main entrance of the Sisters' Residence for a three-month pilot period, with the traditional lock retained as a physical override for emergencies.
- Staff training programme: Develop a 30-minute orientation session for all residents covering how to present RFID tags correctly (within 5cm of reader), proper fingerprint placement (dry finger, centred on sensor), PIN entry, using facial recognition in low light (activating the LED flash), and accessing the dashboard to view personal access history.
- Enrolment procedure: Designate one administrator (e.g., Sister in Charge) to manage user enrolment. Require each resident to enrol at least two authentication factors (preferably three) to ensure fallback options.
- Maintenance schedule: Perform monthly checks of fingerprint sensor lens cleaning, camera lens cleaning, servo motor alignment, battery backup status, and log file size (rotate logs every 90 days).

5.8 Recommendations for Technical Improvement

- Improve fingerprint sensor robustness: Replace the optical R307 sensor with a capacitive sensor (e.g., R503) that performs reliably with damp fingers, or implement a "dry finger" instruction prompt displayed on the dashboard.
- Enhance low-light facial recognition: Add an external IR illuminator or brighter LED flash to the ESP32-CAM module. Implement adaptive exposure control in firmware to increase sensor gain in low light before capturing the recognition frame.
- Reduce facial recognition latency: Optimise the Eloquent Face Recognition pipeline by reducing frame resolution from 1600×1200 to 800×600 for verification tasks (where high resolution is unnecessary). This is projected to reduce latency from 2.9 seconds to approximately 1.5 seconds.
- Add battery level monitoring: Implement a voltage divider on the backup battery to report charge level via the dashboard. Trigger an alert when battery drops below 20%.

- Implement OTA (Over-the-Air) updates: Extend the ESPAsyncWebServer to accept firmware binary uploads via authenticated HTTP POST, enabling remote updates without physical access to the device.

5.9 Recommendations for Policy

For POTRAZ (Postal and Telecommunications Regulatory Authority of Zimbabwe) use the authentication accuracy findings (Chapter 4) to develop minimum IoT cybersecurity standards for residential smart locks, including requirements for, multi-factor authentication, local encryption of stored credentials, TLS 1.2+ for all network communication, and tamper detection with logging.

For the Health Service Board (HSB) revise the ICT Security Policy for healthcare facilities to require electronic access audit trails and multi-factor authentication for all staff residences attached to mission hospitals. Include a provision allowing facilities to implement low-cost, locally assembled systems where commercial alternatives are unaffordable.

For the National Development Strategy 2 (NDS2) Implementation Unit adopt this low-cost smart lock model as a replicable pilot project under the digital transformation and healthcare infrastructure priorities. Allocate funding for deployment to 10 additional mission hospitals in Manicaland Province, with evaluation metrics including reduction in reported burglaries and staff satisfaction scores.

For the Zimbabwe Republic Police (ZRP) Crime Prevention Unit, Incorporate the quantified reduction in authorised access incidents into crime prevention guidelines for healthcare facilities. Recommend smart lock retrofitting as a countermeasure against rising property crime.

5.10 Recommendations for Future Research

- Longitudinal deployment study deploy the system at the Sisters' Residence for 12 months to measure, actual reduction in unauthorised access incidents compared to baseline, device reliability (mean time between failures), user acceptance over time (repeat SUS every 3 months), and maintenance costs and frequency.

- Scalability study: Evaluate the system's performance with 100+ enrolled users to measure authentication latency degradation and LittleFS storage limits. Investigate database sharding or external SD card storage for large-scale deployments.
- Comparative study of authentication factors conduct a controlled experiment with 50 participants to measure preference, speed, and error rates for each of the possible two-factor combinations, establishing evidence-based guidelines for factor selection.
- Behavioural anomaly detection model train a machine learning model on the logged access events (supplemented with synthetic data) to detect unusual patterns (e.g., access at improbable times, rapid successive attempts). Deploy the model on the ESP32 using TensorFlow Lite Micro and measure detection accuracy and latency.
- Cross-site replication replicate the study at two additional mission hospitals (one in a different province, one with different shift patterns) to validate the findings' generalisability across Zimbabwean healthcare settings.

5.11 Limitations of the Study

Duration: The evaluation was limited due to time constraints. This period may not capture long-term reliability issues (e.g., sensor degradation, flash memory wear) or seasonal variations (e.g., cold weather affecting fingerprint sensor performance).

Sample size, on this study only 3 participants completed the SUS questionnaire and interviews. While this provided indicative usability data, a larger sample ($n \geq 20$) would be required for statistically generalisable conclusions.

Simulated attacks, the security evaluation used simulated attacks in a controlled laboratory setting, not real adversarial attempts in the field. An attacker with specialised equipment (e.g., high-power RFID cloner, sophisticated facial spoofing materials) might achieve higher success rates than reported.

No direct longitudinal comparison, the study did not operate the traditional and smart lock systems concurrently over an identical period. The comparison relies on historical incident data (2021–2023) and laboratory attack simulations, not a randomised controlled trial.

Single site: The research was conducted at one healthcare residence. Findings may not generalise to other settings with different infrastructure (e.g., urban locations with reliable internet) or user demographics.

Hawthorne effect: Participants were aware they were being observed during the trial, which may have influenced behaviour (e.g., more careful RFID placement, avoiding workarounds). Actual long-term use might show lower compliance.

5.12 Costing

Component	Cost (USD)
Fingerprint sensor	25
ESP32- CAM	17
ESP32	10
Servo Motor	3
RFID	5
Keypad	3
Miscellaneous	4
Total	67

Table 14 component cost

REFERENCES

Alsinglawi, B., Elkhodr, M., Nguyen, Q. V., Gunawardana, U., Maeder, A., & Simoff, S. (2017). RFID localisation for internet of things smart homes: A survey. *International Journal of Computer Networks and Communications*, *9*(1), 81–99. https://doi.org/10.5121/ijcnc.2017.9107

Anand Desai, C. S. M. B. (2025). *Enhancing Home and Commercial Security: A Multi-Modal Authentication Framework for Keyless Door Lock Systems*.

Ang, K. W., Chekole, E. G., & Zhou, J. (2025). Unveiling the Covert Vulnerabilities in Multi-Factor Authentication Protocols: A Systematic Review and Security Analysis. In *ACM Computing Surveys* (Vol. 57, Number 11). Association for Computing Machinery. https://doi.org/10.1145/3734864

Botha, L., & Taylor, E. (2022). *USING DESIGN SCIENCE RESEARCH AS PARADIGM FOR INFORMATION SYSTEM RESEARCH: AN APPLICATION*.

Buolamwini, J. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification *. In *Proceedings of Machine Learning Research* (Vol. 81).

Chakkaravarthy Sethuraman, S., Mitra, A., Li, K. C., Ghosh, A., Gopinath, M., & Sukhija, N. (2022). Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets. *IEEE Access*, *10*, 112721–112730. https://doi.org/10.1109/ACCESS.2022.3216665

Chandra, M., Sandeep, M., Reddy, P. P. K., Reddy, R. S. K., Sowrya, P. C., & Kumar, A. (2023). Door Lock System Using HumanFaces With ESP32-CAM. *Proceedings of the 4th IEEE International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2023*. https://doi.org/10.1109/ICSTCEE60504.2023.10584952

Derbali, M. (2023). *Toward Secure Door Lock System: Development IoT Smart Door Lock Device*. https://doi.org/10.22541/au.168055385.54003954/v1

Diao, C., Dang, D., Lira, S., Tsai, A., Haller, M., Heninger, N., & Diego, S. (2025). *Open access to the Proceedings of the 19th USENIX WOOT Conference on Offensive Technologies is*

sponsored by USENIX. *No Key, No Problem: Vulnerabilities in Master Lock Smart Locks*. https://www.usenix.org/conference/woot25/presentation/diao

ESP32 Technical Reference Manual. (n.d.). Retrieved www.espressif.com

Frank Ingo Müller. (n.d.). *Securing the Home*. https://doi.org/10.2307/26764794

Jeste, M., Gokhale, P., Tare, S., Chougule, Y., & Chaudhari, A. (2020). Two-point security system for doors/lockers using Machine learning and Internet of Things. *Proceedings of the 4th International Conference on Inventive Systems and Control, ICISC 2020*, 740–744. https://doi.org/10.1109/ICISC47916.2020.9171080

Kshirsagar, S., Sachdev, S., Singh, N., Tiwari, A., & Sahu, S. (2020). IoT Enabled Gesture-Controlled Home Automation for Disabled and Elderly. *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*, 821–826. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-000152

Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multifactor door locking systems: A review. *Materials Today: Proceedings*, *46*, 7973–7979. https://doi.org/10.1016/j.matpr.2021.02.708

Nadiya, U., Rizqyawan, M. I., & Mahnedra, O. (2019). *IEEE Blockchain-based Secure Data Storage for Door Lock System*.

Naresh, D., Anand, P., Harish, M., Vamshi, A., Kethan, A., Nirmala, B., & Saravanan, M. (2026). Face Recognition Door Lock System with IoT &AI. *International Journal of Computer Technology and Electronics Communication*, *09*(02). https://doi.org/10.15680/IJCTECE.2026.0902011

NDS2. (2026). *NATIONAL DEVELOPMENT STRATEGY 2 REPUBLIC OF ZIMBABWE Mabvuku Interchange Construction of Gwayi-Shangani dam.*

Pacheco, J., & Miranda, K. (2020, September 1). Design of a low-cost NFC door lock for a smart home system. *IEMTRONICS 2020 - International IOT, Electronics and Mechatronics Conference, Proceedings*. https://doi.org/10.1109/IEMTRONICS51293.2020.9216409

Ramakrishna, P., Sachin, K., Rather, I. A., Vandana, M., & Vignesh, S. S. (2023a). Smart Home Security System Using IoT. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*. https://doi.org/10.1109/ICCCNT56998.2023.10307277

Ramakrishna, P., Sachin, K., Rather, I. A., Vandana, M., & Vignesh, S. S. (2023b). Smart Home Security System Using IoT. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*. https://doi.org/10.1109/ICCCNT56998.2023.10307277

Ramakrishna, P., Sachin, K., Rather, I. A., Vandana, M., & Vignesh, S. S. (2023c). Smart Home Security System Using IoT. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*. https://doi.org/10.1109/ICCCNT56998.2023.10307277

Rishwanth, S., Niranjana, B., & Sriramalakshmi, P. (2023). IoT Based Bank Locker Security System. *Proceedings of the 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2023*. https://doi.org/10.1109/ICSES60034.2023.10465482

Sabbatini Zürich, M. (2024). *Hardening IoT Devices: An Analysis of the ESP32 Microcontroller*. http://www.csg.uzh.ch/

Salsabila, N., Siswanto, A., & Bayuaji, L. (2025). Design of a Smart Home Door Security System with Face Detection and Smart Bell using ESP32-CAM. *6th International Conference on Mobile Computing and Sustainable Informatics, ICMCSI 2025 - Proceedings*, 124–129. https://doi.org/10.1109/ICMCSI64620.2025.10883160

Serengil, S., & Özpınar, A. (2024). A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules. *Bilişim Teknolojileri Dergisi*, *17*(2), 95–107. https://doi.org/10.17671/gazibtd.1399077

Shaout, A., Shah, N., & Dhandapani, S. (2022). Secure Smart Lock System Utilizing the MQTT Protocol. *2022 13th International Conference on Information and Communication Systems, ICICS 2022*, 70–75. https://doi.org/10.1109/ICICS55353.2022.9811136

Sonamoni, J. S., Sikdar, R., Akib, A. S. M. A. S., Islam, M. S., Sourov, S., Al Ahasan, M. A., Islam, M., Habib, M. A., & Mridha, M. F. (2024). IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application †. *Engineering Proceedings*, *76*(1). https://doi.org/10.3390/engproc2024076085

Zimbabwe. (2021). *Cyber and Data Protection Act, 2021*. www.laws.africa

ZIMSTAT. (2025). *2025 FOURTH QUARTER STATISTICS REPORT*.

Zurida Ishak, Narmitha Rajendran, & Omar Ismael Al-Sanjary. (2020). *Proceedings, 2020 16th IEEE International Colloquium on Signal Processing & its Application (CSPA 2020) : 28th-29th February 2020 : conference venue, Hotel Langkawi, Lot 1852 Jalan Penarak, Kuah 07000 Langkawi, Kedah, Malaysia*. IEEE.