A hybrid early warning system for the prevention of mobile asset theft: case of laptops in South African government buildings

by

Thabiso John Matsemela

Dissertation submitted in fulfilment of the requirements for the degree

MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING

in the

Department of Electrical, Electronic and Computer Engineering

Faculty of Engineering, Built Environment and Information Technology

at the

Central University of Technology, Free State

Bloemfontein

Supervisor: Prof ED Markus

2025

DECLARATION

I, Matsemela Thabiso John (Student Number _____) hereby declare that this research project which has been submitted to the Central University of Technology, Free State for the degree MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING, is my own independent work, complies with the Code of Academic Integrity, as well as other relevant policies, procedures, rules and regulations of the Central University of Technology, Free State, and has not been submitted before by any person in fulfilment (or partial fulfilment) of the requirements for the attainment of any qualification.

Student Signature:

Date:

ACKNOWLEDGEMENTS

I wish to take this opportunity to thank the almighty God of The Twelve Apostles Church in Trinity for guiding me throughout the journey of my academics.

I also wish to thank Mr. Masheane Lebohang, a Mechanical Engineering lecturer at the Central University of Technology, Free State (CUT, FS) for encouraging me and mostly making it possible to meet with my core study supervisor Prof E.D. Markus.

My sincere thanks to my supervisor, Prof. E.D. Markus for his selfless behaviour. Prof E.D. Markus has supported me from the inception of the study when we were talking about the proposal. I thank Prof E.D. Markus for turning my dream into reality. I am deeply grateful for his guidance and support. He is an inspiration and a mentor to me. It would not be possible to adequately repay him for his kindness and generosity.

Without the understanding and support of my wife, Nomathemba Yvonne FEITJIE, and my children, Bokamoso and Lehakwe, this study would not have been possible. I am grateful for your sacrifice and encouragement.

Finally, I would want to dedicate the entire research to my late mother (Maria Mamoqekele MATETE), who passed away on September 8, 2023, while I was working on this study. Despite the fact that you were not educated, you ensured that I had a high-quality education, and I am grateful for everything you have done for me. I dedicate the remainder of my studies to you. I hold you in the highest regard. I hope my research makes a modest contribution to you. Thank you for your unwavering love and support.

ABSTRACT

The growing threat of mobile asset theft in South African government establishments presents serious risks to information security and public sector performance. Mobile assets such as laptops and similar devices increasingly store sensitive and operational data, ensuring their protection has become critical. This study addresses the problem by proposing a hybrid early warning detection and prevention system designed to monitor and respond to unauthorised access and unlawful handling of mobile assets in real time. The system integrates a biometric fingerprint authentication, intelligent camera surveillance, infrared motion detection, a microcontroller-managed limit switch, smart lock, and wireless notification devices, forming a multi-layered security system. Developed using the Design Science Research Methodology (DSRM), the system was tested under simulated conditions to evaluate its reliability and responsiveness. MATLAB was used extensively for component-level simulation, while MikroC facilitated the programming of a PIC16F628A microcontroller to coordinate all system functions. A backup power supply capable of 48-hour operation was also included to ensure uninterrupted monitoring during power outages. Analyses, including chi-square testing, were applied to assess the significance of biometric authentication and system performance across two government buildings, with additional validation using theoretical scoring and multivariable performance models under varied conditions. The results showed over 97, 5% accuracy, a response time of 95 milliseconds during breach events, and consistent behaviour across test environments. The intelligent camera only activates under threat conditions, preserving user privacy, and a manual override provides operational flexibility. These findings confirm the system's viability as a scalable, intelligent security solution for mobile asset protection in government and potentially private sector environments.

ABBREVIATIONS

AC	Alternating Current
AI	Artificial Intelligence
BIOS/UEFI	Basic Input / Output System/ Unified Extensible Firmware Interface
BLE	Bluetooth Low Energy
CCTV	Closed Circuit Television
C-NO	Common to Normally Open
C-NC	Common to Normally Close
CUT	Central University of Technology, Free State
DC	Direct Current
DPW&I	Department of Public Works & Infrastructure
GPS	Global Positioning System
GPRS	General Packet Radio Service.
GSM	Global System for Mobile communication
ICT	Information Communication Technology
IP	Internet Protocol
IoT	Internet of Things
LED	Light Emitting Diode
IDS	Intrusion Detection System
IR	Infrared
ISP	Internet Service Provider
PTZ	Pan Tilt Zoom
MAC	Media Access Control
PIC	Peripheral Interface Controller
PIF	PIC Input Frequency
PMU	Project Management Unit
PTZ	Pan Tilt Zoom
RFID	Radio Frequency Identification

SIM	Subscriber Identification Module
SMS	Short Message Services
TCF	Tick Counter Frequency
TSC	Theoretical Score Calculation
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

SYMBOL

Chi-Square Statistic Formula	$x^2 = \sum_{i=1}^{n} \frac{(Oi-Ei)^2}{Ei}$
Threat Score Calculation	$T = \alpha(1 - B) + \beta M + \gamma C$
True Acceptance Rate	$TAR = \frac{True\ Acceptance}{Total\ Attemps}\ X\ 100$
False Acceptance Rate	$FAR = \frac{False\ Acceptance}{Total\ Attemps}\ X\ 100$
False Rejection Rate	$FRR = \frac{False\ Rejection}{Total\ Attemps}\ X\ 100$
Delay	Tincrement $= Prescaler\ X\ Tcycle$
DF	Degree of Factor
N	Holding Force
ms	milliseconds
System's Accuracy	$Accuracy = \frac{Correct}{N}$

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

As innovation advances, the security and administration of mobile assets such as laptops and tablets inside government departments have become critically significant [1]. various measures have been taken to guarantee that the mobile assets are well protected. Recently, the Free State's Department of Public Works and Infrastructure (DPW&I) implemented a comprehensive electronic security system that includes closed circuit television (CCTV) and access control in their prime buildings, OR Tambo and Fidel Castro, to prevent mobile asset theft. The protection of these assets is crucial as they contain sensitive information about service delivery and intellectual property that belongs to the government and national security. The DPW&I's security director took the initiative to create a memorandum requiring all officials to lock their offices whenever they leave, regardless of how long they plan to stay outside their offices. In response to the challenge of mobile assets theft, the integration of intelligent security systems that can detect, prevent, and report the unauthorised removal or manipulation of mobile assets has emerged as a viable solution.
This study proposes a tailor-made solution of an early warning detection and prevention of mobile assets in government establishments in South Africa. The proposed system integrates various electronic components including a microcontroller for issuing of instructions [2] and biometric fingerprint authentication for activating and deactivating of the system [3], a limit switch station for a placement of mobile assets, infrared (IR) sensor for authorised employee detection, intelligent camera for remote viewing and information gathering [4] and Wi-Fi switch with Google Home user’s interface software to facilitate real-time remote reporting, thereby enabling rapid response from security personnel during attempted breaches [5].

The proposed system also includes a warning mechanism that uses a door-mounted magnetic switch, buzzer and status strobe light emitting diode (LED) [6]. When the authorised user attempts to leave the office without properly securing the mobile asset after activation, the buzzer emits a persistent alert and strobe light continues to flash. This

ensures the user places the mobile asset in the secured location and confirms security activation via biometric verification.

Furthermore, the intelligent camera remains off at all times during normal operation to preserve privacy of the office occupant. However, when the system detects no motion of the authorised employee at the workstation for a predefined duration, it sends a signal to turn on an intelligent camera, however, the camera issues a reminder voice to prompt the user to confirm their presence before it can allow remote viewing. This is to ensure that the privacy of the user is not compromised. If no confirmation is received, the camera activates, and the system transmits live footage for security personnel at the control room. Simultaneously, it sends an addressable alert including the building name, room number, and office number.

Simulation of this study was conducted at the two establishments of the DPW&I (Project Management Unit building and Security Section. The DPW&I control room is situated at the Fidel Castro Building in the Free State. The security personnel manages outdoor incidents through LED-mounted surveillance screens. The system incorporates outdoor PTZ camera [7], bullet cameras and facial recognition [8] for access control into facilities. However, the existing setup lacks notification devices to notify security personnel of live burglary and theft incidents. This study aims to integrate and enhance the current infrastructure by introducing an intelligent, responsive indoor monitoring system capable of notifying personnel proactively during security threats.

The study features a smart locking mechanism [9] situated at the main entrance of the establishment. Under normal operating conditions, this lock remains de-magnetised. However, it is automatically activated upon the detection of unauthorised removal of mobile assets from its designated position. In such instances, the system magnetizes lock, thereby restricting egress from the premises. This temporary lockdown enables security personnel in the control room to promptly communicate perpetrator information with in-house security, thereby expediting the asset recovery process. The door will remain locked

for a predefined duration and unlock itself after that period, however, control room security personnel can extend the duration if the asset is not recovered or if the perpetrator is not apprehended.

The system also includes a warning mechanism that uses a door-mounted magnetic switch, buzzer and status strobe light emitting diode (LED). When the authorised user attempts to leave the office without properly securing the mobile asset after activation, the buzzer emits a persistent alert and strobe light keeps on flashing. This ensures the user places the mobile asset in the secured location and confirms security activation via biometric verification.

This multidisciplinary arrangement bridges the spaces of electronic security (access control and alarm systems), embedded systems, and smart surveillance, offering a layered and intelligent approach [10] to protecting government-owned mobile assets from unauthorised access and theft. Furthermore, this solution can also be applied in higher education institutions such as the Central University of Technology (CUT) (Free State Library) to ensure that students' mobile assets are properly secured when they leave their workstations to go to the bathroom or take a lunch break. Currently, (CUT) uses radio frequency identification (RFID) system [11] for access control. Furthermore, this system can also be used in the private offices to ensure that mobile assets are secured.

1.2 MOTIVATION

The study was motivated by the pressing need to develop an integrated electronic security [12] that will be able to think for itself when it feels that it is under threat and to mitigate the mobile asset security risks in public sector establishments. The South African government sector experiences a recurring loss of technical resources due to inadequate work environments, from the state and national sectors to local and local municipalities. Minister of Public Works raised a serious concern after 30 laptops that were stolen were recovered, which worth R 300 million. It is implied that either these computers were taken out of the department illegally or were used in a cyber-theft plan.

Despite the availability of various electronic security systems, existing solutions remain largely ineffective as they lack an element of customisation they are either manual or limited to commercial off-the-shelf solutions not specifically designed for mobile asset security. Biometric systems are often restricted to access control at entry points [13], and live monitoring with real time clock [14] is seldom extended to mobile asset theft. Consequently, the lack of a comprehensive, integrated approach makes these environments vulnerable to misuse and theft of valuable equipment.

A striking example of this vulnerability occurred in 2023 at the office of the Director of Public Prosecution (DPP) in Bloemfontein where a criminal broke into office and stole voice recorders and four (4) laptops. Another recent incident happened at one of the largest banks in South Africa, where a thief unlawfully took a mobile asset belonging to a banking consultant while there was no one at the consultation cubicle. Although the perpetrator was later seen on the bank CCTV footage, this only happened after they had already fled the scene, by which point the asset was lost. The absence of a real-time early warning detection system meant that no alarm was triggered, and no immediate action could be taken by security personnel to intervene. This incident underscores the urgent need for intelligent systems that can proactively detect unauthorised movement and notify responders instantly before an asset is permanently lost.

Mobile assets are essential in public sector, especially for technical personnel as some employees operate in the field and must have continual online meetings with their managers and contractors about project progress and other technical difficulties. If these are not properly secured, it becomes a challenge for one to do their work if the assets are stolen. Some of these technical personnel take their work home to guarantee that it is completed on time, and without a laptop, this becomes a serious challenge. Government laptops are expensive because of the software they contain, and when they are stolen, taxpayers suffer financial losses. The expense of replacing stolen computers adds to the financial strain, diverting monies that could have gone toward other public services.

This study is further motivated by the researcher to scale up the solution within the operational realities of South African government and private sectors by designing and producing a solution that is not only robust but also practical and cost-effective. Furthermore, the system has potential for deployment in colleges, universities and public libraries, where students frequently leave their belongings unattended for short breaks.

1.3 PROBLEM STATEMENT

The safeguarding of mobile assets in South African government departments is compromised by the lack of real-time monitoring, intelligent detection [15] of unauthorised personnel, and automated prevention mechanisms. This results in significant security gaps, leaving mobile assets vulnerable to perpetrators. The existing electronic security solutions lack entwinement between biometric authentication, real-time intrusion detection and prevention, and remote alerting, components that are crucial for comprehensive asset security in modern government operations.

Sub-problem 1:

How can biometric fingerprint authentication [16] be effectively integrated to manage system activation and deactivation, ensuring that only authorised personnel interact with mobile assets?

Sub-problem 2:

What mechanisms can be employed to reliably detect and log the physical removal or repositioning of a mobile asset in real time?

Sub-problem 3:

How can wireless communication technologies, and intelligent camera [18], be leveraged to facilitate remote monitoring and instant reporting of threats to security personnel?

1.4 AIM AND OBJECTIVES

The primary aim of this study is to develop a hybrid early warning security system for mobile assets, specifically laptops within South African government offices in the Free State Province. This study aims to develop a microcontroller-based solution that integrates biometric authentication, intelligent surveillance, and wireless communication technologies to proactively detect and report unauthorised access or movement around mobile assets. The goal is to enhance both physical and data security through a system capable of real-time threat identification and response.

The objectives of the study are as follows:

To design and develop a hybrid early warning intelligent microcontroller-based [19] hardware platform that distinguishes between authorised personnel and potential intruders through biometric fingerprint identification, ensuring that only authorised users can have access to the mobile asset and additionally, authorised personnel can only activate and deactivate the system. This addresses sub-problem 1.

To integrate a limit switch and intelligent camera for mobile asset removal and intelligent surveillance system, with capabilities for issuing voice alerts, detecting, tracking, and analysing movement within the office space when a security breach is suspected within a predefined duration, thereby enabling contextual awareness and real-time threat assessment to the remote security personnel. This addresses sub-problem 2.

To design a microcontroller-based system that enables seamless communication between an infrared (IR) sensor, a Wi-Fi communication module, and an intelligent camera for the purpose of detecting potential threats to mobile assets. The system should be capable of generating and transmitting addressable alerts detailing the specific office number and location of the intrusion to designated security personnel. Furthermore, it allows for real-time remote visual verification of the asset within 10 seconds of the event and initiates immediate wireless alarm notifications upon detection of unauthorised access. This address sub-problem 3.

To ensure the system includes robust security features such as safety supplies, user-friendly control interfaces, and compliance with applicable government information and communication technology (ICT) and data protection standards, supporting continuous and user-friendly operation under a variety of conditions. To conduct a pilot implementation and performance evaluation of the complete system in the DPW&I offices in Bloemfontein, assessing its effectiveness, reliability, and adaptability.

1.5 RESEARCH METHODOLOGY

This study uses the Design Science Research Methods (DSRM) [20] to guide the development, implementation and evaluation of early warning security systems for mobile assets in South African government agencies. The DSRM approach is suitable for technical research, including the creation of intelligent inventions to solve identified problems. The methodology passes through the following stages:

1.5.1 Problem Identification and Motivation

A comprehensive literature review and needs assessment will be conducted to identify the specific vulnerabilities associated with mobile asset theft in government offices. This phase includes consultations with ICT and information security [21] in selected government departments across South Africa to validate the real-world relevance of the identified sub-problems.

1.5.2 Definition of Objectives for a Solution

Based on problem analysis, this study defines functional and non-functional requirements for hybrid security systems. The most important design parameters include biometric integration, sensor selection (such as IR and limit switches), intelligent camera capabilities, and wireless communication standards.

1.5.3 Design and Development

This phase focuses on engineering and integration of the components of the system.

- Microcontroller-based systems: The microcontroller acts as a control unit for handling sensor inputs and control output devices.
- Biometric fingerprint module for activation and deactivation of safe systems by authorised personnel.
- Sensor Network: IR sensors and border switches recognise unauthorised financial movements.
- Intelligent Camera System: Incorporated to pursue movement and communicate potential threats to microcontrollers [22].
- Wi-Fi Communication Module: Sends real-time alerts to remote security personnel and protocol activities [23].
- Security Current System: A rechargeable battery and voltage regulation circuitry are installed to ensure uninterrupted functionality in the event of a power failure [24].

Prototyping tools such as Proteus and Matlab/Simulink [25] are used for circuit simulation, while conversations or embedded C in MPLAB X IDE and PIC assemblies are used for firmware development.

1.5.4 Evaluation

The system will be evaluated based on:

- Access to biometric detection.
- Sensor response to non-exempt asset movement.
- Speed and reliability of wireless communication.
- Security components.

1.6 RESEARCH OUTPUT

The following paper was published as part of the study:

Matsemela Thabiso and, Elisha Didam Markus, Hybrid early warning system for prevention of mobile asset theft: case of laptops in South African government buildings. Accepted to *2025 Information Communication Technology & Society Conference (ICTAS).*

1.7 SUMMARY

This chapter presented an integrated overview of designing and developing an early warning detection and prevention system for mobile assets within South African government establishments. Commencing with the background and motivation for the study, it established the growing concern over the loss and theft of government-issued laptops and other portable equipment, particularly in environments where existing systems such as RFID-based asset tracking have proven insufficient for real-time threat mitigation. These mobile assets are used by professionals such as engineers, architects and quantity surveyors to conduct their day-to-day business and to engage with contractors and consultants. This challenge of theft affects service delivery, furthermore, it affects the holistic information security of government. The problem statement was clearly articulated and divided into three sub-problems focusing on the need for secure activation through biometric fingerprint authentication, mechanism employed to reliably detect removal of assets, wireless communication and remote viewing by Wi-Fi communication module and intelligent camera. These sub-problems guided the formulation of the study's aims and objectives, which sought to design and implement a hybrid solution integrating microcontroller-based hardware, intelligent camera for remote viewing, biometric modules, and Wi-Fi-enabled caution systems.

The dissertation is structured as follows: Chapter 2 discusses the comprehensive literature review conducted during the study. In chapter 3, the methodology and design process are explained. Chapter 4 presents the results, demonstrating that the system functioned in alignment with the objectives outlined in Chapter 1. The system's performance was simulated using MATLAB, confirming its capability to detect unauthorised access, trigger alarms, and communicate alerts effectively. Finally, Chapter 5 concludes the study by summarising key findings and emphasising the practical significance of the proposed system. This study is paramount for implementation in environments where mobile asset security is a critical concern to mitigate theft and improve accountability through intelligent, automated monitoring and control mechanisms.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

This chapter presents a comprehensive study of current research and advancements in the field of electronic security systems, with a particular emphasis on detection and protection of mobile assets at government facilities. It focuses on the progress of security technology, major findings from prior research, and gaps in present security frameworks. Furthermore, it conducts a thorough literature study, defines mobile assets electronic security systems in government organisations, and analyses several strategies for improving those systems. It emphasises the significance of integrating advanced technologies by making the system intelligent, using both biometric fingerprints, remote viewing, live monitoring and smart locking during incursion to ensure that assets are effectively protected and that the intruder is identified instantly if tampering occurs.

Laptops are important instruments for daily operations in government offices particularly design office and supply chain management, as they store large volumes of sensitive and confidential information such as design drawings, specifications, tender information, etc. Laptops' portability, while useful to flexibility and mobility, makes them great candidates for theft and unwanted access. As a result, securing laptop security has become a major concern for enterprises, especially in workplaces where data breaches can cause considerable financial and reputational damage.

The security of mobile assets has become a pressing issue in both government and private sectors due to increased mobility and vulnerability to theft and unlawful access. This literature review critically examines existing technologies and methods used for early warning detection and prevention of laptop theft and unauthorised use. The review spans mechanical, software-based, sensor-based, and hybrid solutions, revealing existing gaps and motivations for proposing a novel hybrid system integrating biometric, infrared, GSM/GPRS, and intelligent video surveillance technologies.

2.2 PREVIOUS RESEARCH ON MOBILE ASSETS SECURITY

Previous research on mobile assets has shown that they are successful; nonetheless, there are several drawbacks that allow intruders or thieves to steal computers in the office without being detected by security. This study encompasses:

2.3.1 Physical Laptop Lock

The Kensington Lock [26], also known as the K-Slot, is one of the oldest mechanical security devices for laptops that physically locks a laptop to a fixed object like an office table. It is widely used in government offices to deter theft. The lock is made up of a cable with one end that connects to the laptop through a small, rectangular security slot (known as the Kensington Security Slot), and the other end that can be looped around an immovable object like a desk or pole. However, the tables or working stations are not equipped with impermeable protection to keep the laptop safe in unattended locations. Lock-picking and cable cutting are two tactics that can be used to bypass physical laptop security, making it easier for intruders to tamper or steal laptops.

Moreover, the lock's efficiency is determined by the strength of the item to which the laptop is locked. If the table is easily moveable or breakable, the lock's security becomes less effective. The other problem is the keys, as seen in Figure 1 below; if the keys are lost or forgotten, the laptop is not protected. The system lacks any form of intelligent detection or notification, rendering it reactive rather than proactive. The key study gap here is the absence of digital alerting mechanisms or real-time status monitoring.

Figure 1: Physical laptop security using Kensington lock [26]

Overall, Kensington locks are not the best option for laptop security, especially in government workplaces where sensitive information is stored. If the physical lock is not maintained, an intruder may steal the data. Government departments and municipalities should invest in more security methods, such as biometrics. These safeguards are far more difficult to breach and offer increased protection.

2.3.2 Absolute Lojack Review

Absolute LoJack [27], also known as Absolute Home and Office, is a security programme that protects laptops, tablets, and cell-phones from theft, as seen in Figure 2 below. It uses embedded firmware that communicates with monitoring servers to report location and enable remote wiping or locking. It also offers real-time monitoring and notifications when the device is used outside of its intended area. Absolute LoJack also offers a range of assistance services to help owners recover lost or stolen devices. This service includes assisting police with the recovery of stolen devices.

Figure 2: Absolute Home and Office protection software for electronic devices [27]

However, this technique has certain drawbacks, including the possibility that information technology attackers will abuse the program and the difficulty of uninstalling it because it is built into many devices' Unified Basic Input/ Output system/Extensible Firmware Interface (BIOS/UEFI) [28]. Although this protects the software's endurance, someone who no longer wants to utilise the service may have difficulty deleting it. Absolute LoJack can help you recover stolen devices, but it may not always be effective at preventing theft. A skilled burglar may disable the software's tracking features. This makes it difficult to recover the device or track down the thief.

Absolute LoJack is also vulnerable to cyber-attacks, which could compromise the security of the software. Furthermore, Absolute LoJack's efficiency is primarily dependent on the device's internet connection. If the stolen gadget is not connected to the internet, the program will be unable to record its location or accept remote commands, delaying recovery efforts. These shortcomings indicate that, while Absolute LoJack can be an effective tool for device recovery, it is not without risk factors and restrictions.

Its strength lies in stealth operation and persistence even after OS reinstallation [29]. Moreover, it is heavily dependent on internet access, limiting effectiveness in offline scenarios or where communication is intentionally blocked. Furthermore, it is reactive, with alerts only after theft. A key gap is the lack of local alarms or pre-emptive detection mechanisms to stop theft at the point of breach.

2.3.3 IP Based Approach for tracing stolen laptop computer and Data Protection with media access control (MAC) address

An internet protocol (IP) -based technique combined with a MAC address [30] is a great means to locate a stolen laptop and secure data. When a stolen laptop connects to the internet, the internet service provider (ISP) assigns it an IP address. IP tracking software [31], which is frequently installed on the laptop prior to theft, can send the laptop's IP address back to a central server when it connects online. The IP address can also be used to approximate the laptop's geographic position, allowing police to better identify and track the device. The tracking program may continuously report IP addresses and other network-related data, leaving a trail of where the laptop was used. This laptop recovery strategy, as illustrated in Figure 3, provides additional benefits such as the option to remotely delete or encrypt critical information if the laptop is stolen. This can be triggered when the laptop connects to the internet and sends its location. It also promptly locks down or erases the laptop's data if it detects that it is being used in an unauthorised location or has been reported stolen.

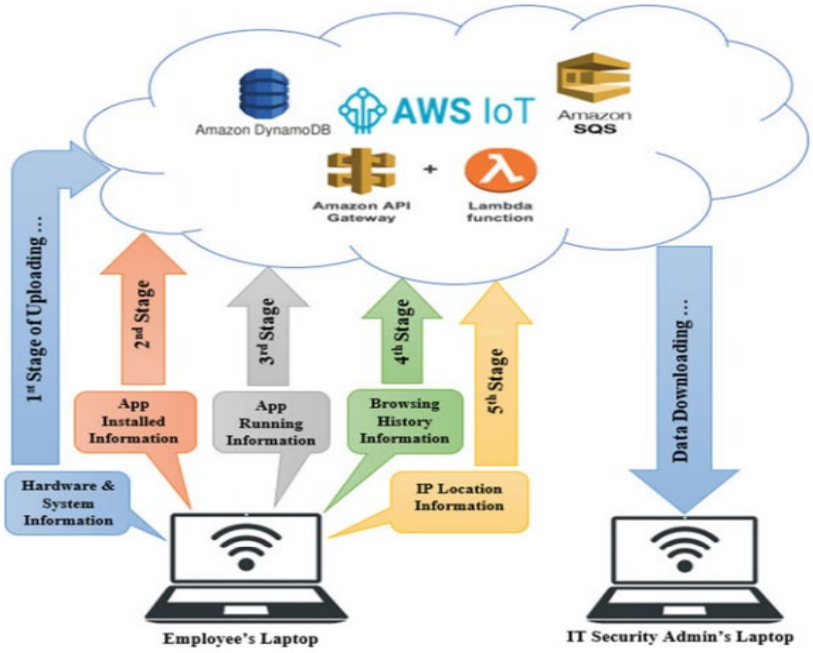


Figure 3: Basic block diagram of the laptop tracking system using cloud computing and Internet of Things (IoT) [32]

This technique of prevention has various limitations as it is dependent on an online connection. If the perpetrator does not connect to the internet, the owner will have a tough time locating a laptop. This method also requires the owner to have internet connectivity in order to track the laptop. Finally, the owner must have technical knowledge to configure the tracking software. The limitations include:

- IP Spoofing [33] and Virtual private networks (VPNs): Thieves can use VPNs [34] or other means to hide the laptop's real IP address, making monitoring more difficult.
- MAC Address Cloning [35]: While more complicated, it is practical to replicate a MAC address, making identification difficult.
- Physical Network Restrictions [36]: MAC address logging is only operational on networks that have visibility of the device, so it may not be useful if the laptop is used on a network that does not monitor or log MAC addresses.

2.3.4 Motion Detection Laptop Protection Using Raspberry Pi

The usage of Raspberry Pi in smart motion detection systems [37] provides a low-cost and versatile option for laptop security and other security applications. Using Passive Infrared (PIR) sensors and cameras, the Raspberry Pi can detect and alert to unwanted motion. PIR sensors detect changes in the infrared radiation generated by objects such as humans and animals. They are widely utilized in government offices security systems since they are inexpensive and reliable. PIR sensors have many applications, including lighting automation and intruder detection [38]. Figure 4 depicts the attachment of the PIR sensor to the Raspberry Pi. Recent advancements of Raspberry Pi in smart motion detection systems include the use of machine learning (ML) techniques [39] to detect more subtle movements and anomalies in the offices.

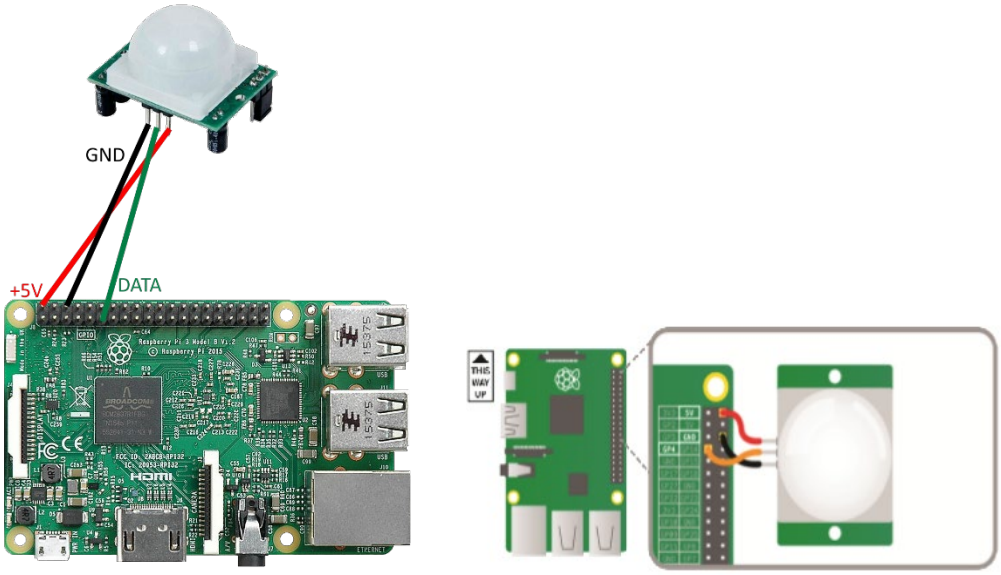


Figure 4: Raspberry Pi with PIR for motion detection in the office [40]

However, this solution has a limited processing capacity, generates false warnings, and is vulnerable to network attack. Furthermore, physical security for the Raspberry Pi [41] and its sensors need to be considered. Proper installation and tamper resistance are required. Furthermore, the Raspberry Pi must be connected to the internet in order to use the warning system, leaving it vulnerable to cyber-attacks. It is vital to consider all of these considerations while designing a Raspberry Pi-based computer laptop security solution for government agencies. Proper security precautions, such as employing strong passwords and encrypted communication methods [42], are necessary. Regular software updates and backups should be performed.

Despite these promising features, practical deployment in portable scenarios remains limited due to bulkiness, external wiring, power supply constraints [43], and difficulty integrating with the laptop chassis. Moreover, Raspberry Pi-based systems are rarely integrated with user-specific authentication like biometrics, nor do they provide surveillance feedback such as real-time video streaming to remote personnel. This reveals a study gap in embedding Pi-based systems into compact, fully integrated hybrid

architectures that combine motion sensing with remote intelligence and secure user authentication.

2.3.5 Transient Authentication

Transient authentication (TA) with a wearable token [44] for laptop security is a novel solution that uses wearable gadgets to enable continuous, real-time authentication. This solution improves security by ensuring that access to the laptop is only granted while the user is there and authenticated using the wearable token. A wearable token could be a smart watch, fitness tracker, smart ring, or any other wearable gadget capable of communicating with the laptop. The token serves as a physical authentication factor, identifying the user by proximity or other biometric information. The laptop continuously tracks the distance between itself and the wearable token. This is commonly accomplished via Bluetooth Low Energy (BLE) [45]. When the wearable is within a predetermined range, the user gets authorised while the laptop remains unlocked.

When a wearable token is lost, stolen, or removed, the system notifies the user and may even wipe specific data from the laptop after a set period of time to prevent unauthorised access as shown in the Figure 5 below. Wearable tokens provide a seamless and user-friendly experience. Users do not have to repeatedly enter their credentials or physically lock and unlock their laptops because the process is automatic and proximity based. This allows users to access their laptops quickly and easily, without having to memorise complex passwords or PIN numbers. Furthermore, the use of wearable tokens reduces the risk of data breaches and identity theft.

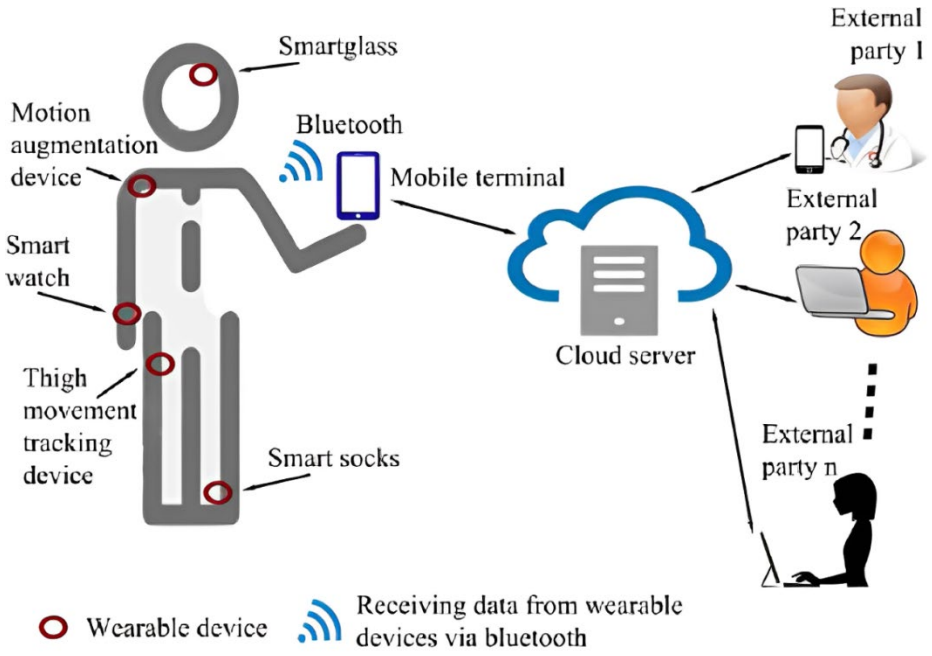


Figure 5: Verification procedure for ensuring security on mobile devices like laptop [46]

Transient authentication raises physical security concerns for laptops. One major challenge is battery life, as wearable devices [47] have a limited battery life. Continuous usage of Bluetooth and biometric sensors may deplete the battery, leading the token to fail when needed most. Another problem could be signal interference. The use of Bluetooth signals for proximity sensing emphasises the significance of maintaining a solid connection between the laptop and the wearable device to provide consistent authentication, regardless of any interference or physical barriers. It is critical to guarantee that the data saved on the gadget is properly encrypted [48] and that the device itself is secure. Furthermore, the device should be frequently scanned for potential vulnerabilities. These challenges makes TA unsuitable for this study as it lacks physical intrusion detection or alarm generation.

2.3.6 Computrace by Absolute Software

Absolute's exclusive persistence technology ensures that the software can withstand hard drive reformatting and operating system reinstallations [49]. This approach is included into a device's firmware, ensuring that the software remains active and functional even when

attempted to be deleted. Computrace provides real-time tracking of stolen laptops. When a gadget connects to the internet, it may report its location and IP address. This information is crucial for the department's security and information technology teams to retrieve stolen laptop(s). Computrace includes tools for remotely wiping data and locking devices. This helps to protect sensitive data from unauthorised access in the event of theft. Furthermore, to avoid laptop loss, laptops are connected to the main server, and each laptop is tagged with a "Proximity card" that functions similarly to an access control card [50].

Computrace demands that the laptop connect to the internet in order to report its location and other information. If the perpetrator never connects the device to the internet, tracking becomes extremely tough. To ensure successful tracking, the laptop must be linked to the internet at all times. This is a significant challenge since it can make laptop recovery difficult if the culprit does not connect the laptop to the internet. Furthermore, firmware agent could be potentially exploited by hackers due to weak authentication layers. This poses a dual threat: device theft and digital vulnerability. Thus, the system fails to provide layered physical-digital hybrid security.

2.3.7 Hardware based models for an asset monitoring

A hardware-based concept for an asset monitoring and tracking system is introduced [51]. This method is primarily concerned with tracking the stolen laptop, as indicated in Figure 6. The tracking model proposed is software-based. For this system to perform properly, it must first be integrated with common Global Positioning System and General Packet Radio Service (GPRS) hardware. Asset monitoring and tracking solutions are crucial for firms that want to manage and secure their physical and digital assets. The growing mobility of electronics such as laptops has increased the potential of theft, leading to the development of a number of technologies for tracking and retrieving these assets. Asset tracking solutions can provide real-time location updates, alert organisations if a laptop is stolen, and aid in the recovery of lost or stolen laptop computers. This solution can also assist corporations keep track of their laptops, improving inventory and maintenance efficiency.

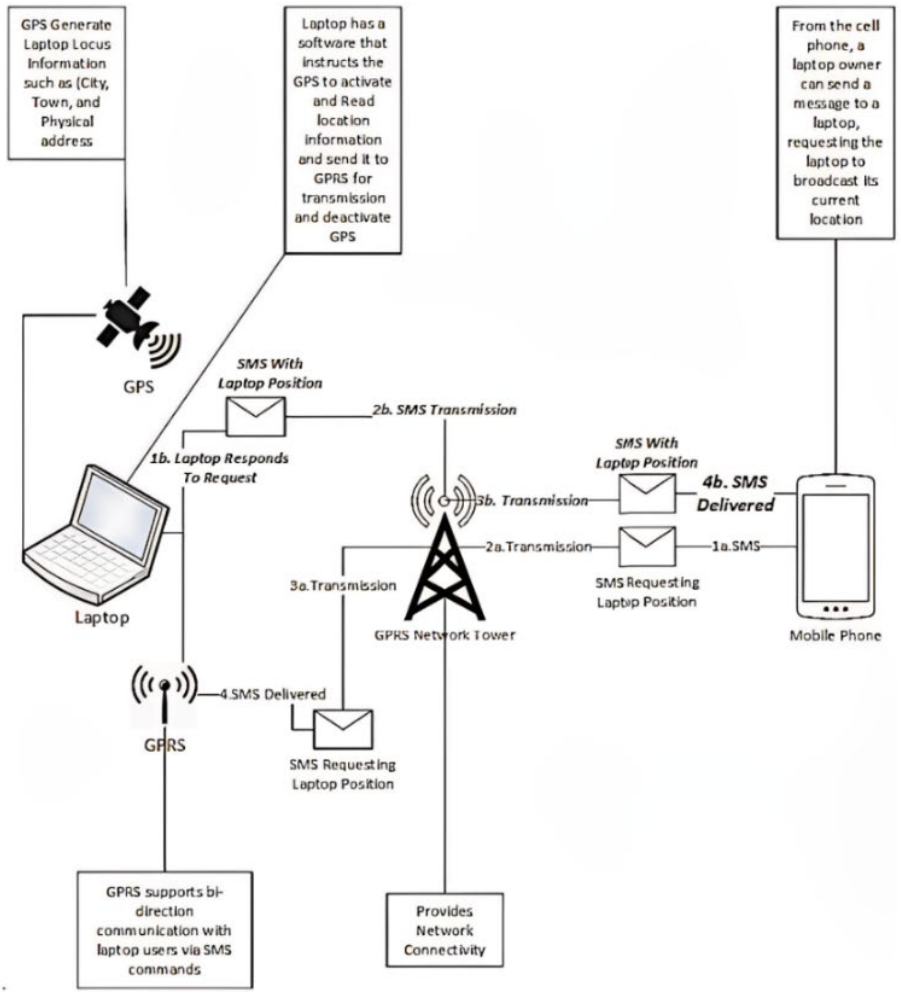


Figure 6: Hardware based laptop tracking model [51]

This method can be costly to establish and sustain, especially on a big scale. Furthermore, GPS [52] and other active tracking technologies require electricity, which might be a problem if the device's battery runs low. The solution is geared for laptop recovery rather than protection, and it requires an internet connection to function. If a laptop is not connected to the internet, retrieval will be difficult. This technology may not be as secure as physical tracking devices, as hackers may be able to intercept and exploit the data, resulting in the offender downloading a new operating system and using it for personal benefit.

2.3.8 A smart household touch sensitive locker security system based on GSM technology

A smart household touch sensitive locker security system based on global system for mobile communication (GSM) technology portable domestic locker security system was proposed in [53]. The combination of touch-sensitive access and GSM-based [54] alerts significantly enhances the security level. Users are immediately notified of any unauthorised attempts to access the locker, allowing for quick responses. Figure 7 depicts the solution designed in such a way that when unexpected user touches the box, a feedback system will be turned on immediately. The system will alert the owner by short message services (SMS) about the unexpected user and triggers the alarm. The alarm will only be switched off by the user via SMS. The system is based on the GSM technology, which means it cannot be easily hacked as it involves only a mobile network.

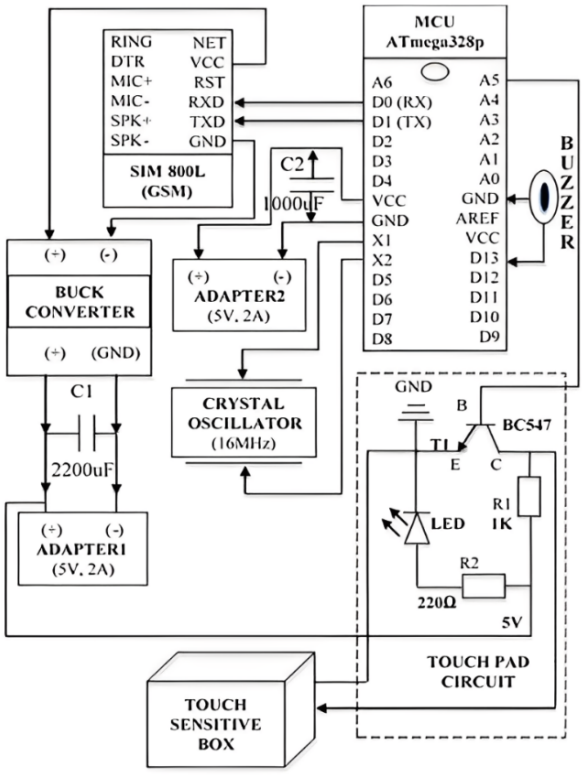


Figure 7: System overview of smart household touch sensitive locker security system based on GSM technology [53]

The efficacy of GSM-based warnings is dependent on the availability and dependability of the GSM network and (SMS); if no SMS or bundles are loaded on the device, the user or security will not receive a notification when intrusion has occurred. In areas with limited network coverage, the system's ability to provide notifications may be threatened. An attacker can clone a Subscriber Identification Module (SIM) card, gain unauthorised access to the GSM network using the same identity, tamper with the box, and steal the laptop. Furthermore, this solution lacks remote monitoring features. The technology, which combines unique access control techniques such as biometric fingerprints, intelligent camera with remote monitoring capabilities and smart lock, has the potential to provide a robust solution for laptop security in the office environment.

2.3.9 Infrared sensor-based Laptop Security Systems

This system often sounds alarms or begins other security processes when they detect unwanted movement or presence, preventing potential theft or misuse. Infrared (IR) sensors [55] detect infrared radiation generated by objects within their range, allowing them to determine movement and vicinity. Their capacity to detect even minor changes in the infrared spectrum makes them appropriate for a wide range of applications, including security systems designed to safeguard laptop computers from theft and misuse.

This system works effectively, but it has weaknesses that allow others to tamper with or steal the laptop. Limitations include a limited range and sensitivity. Furthermore, the detection range of IR sensors is limited, potentially leaving some areas unmonitored. Moreover, this solution is insufficient as the computer (hardware) cannot recognise or discriminate between the user and the intruder. As a result, this solution is susceptible to outside tampering and may not offer comprehensive protection.

2.3.10 Encryption Software System

Encryption protects data by requiring a password [56] or encryption key for access. Encryption protects data content rather than preventing unauthorised transmission, interception, or access. This technology is used by intelligence and security organisations,

as well as personal security applications to protect user data. The Encryption/ Decryption process file is shown in Figure 8. Advanced Encryption Algorithm is a symmetric encryption method that uses the same key for both encryption and decryption.

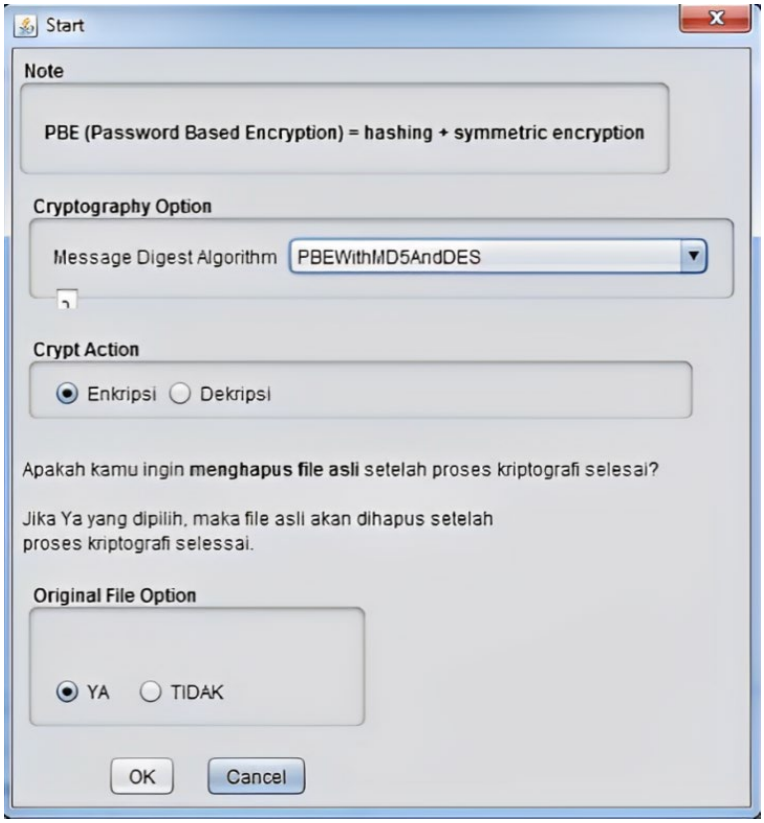


Figure 8: Encryption / Description Process in the form of file. [57]

While encryption software is critical for securing sensitive data, it can have drawbacks such as poor performance, complicated key management, and compatibility concerns. Encryption software can be expensive and time-consuming to develop, as well as complex to maintain. Furthermore, the lack of integration with physical hardware electronic security mechanisms is the central gap, limiting their usefulness in hybrid systems.

2.3.11 RFID-Based Mobile Security Systems

RFID technology is increasingly explored as a non-intrusive method for enhancing mobile asset security, particularly in corporate office environments [58]. A compelling use case is RFID-based Asset Monitoring (RFID-AM) systems, which automatically secure

computing devices such as laptops, tablet and desktops when users physically distance themselves from their workstations [59] as it assumes that the user is no longer present in the office. These systems involve embedding an RFID reader in the workstation and having employees carry RFID tags (button tag, pocket tag or key tag).

However, study gaps persist: current RFID-AM [60] executions need integration with notification mechanisms, intrusion detection, or surveillance feedback, which limits their application in high-security zones where physical asset tracking and post-breach auditing are essential. Additionally, RFID systems may be susceptible to spoofing or signal interception if not combined with encryption or multifactor authentication. These gaps underscore the potential of incorporating RFID as one module within a larger hybrid security framework that includes biometric verification, motion and infrared sensing, and Wi-Fi communication module for comprehensive laptop protection.

2.3.12 Multi-factor Authentication for Laptops

Multi-factor authentication (MFA) [61] has risen as one of the most compelling methods for securing mobile assets such as laptops against unlawful access, particularly in enterprise and government environments. Unlike traditional single-factor confirmation methods such as password only, MFA requires authorised users to show two or more distinct types of credentials, typically a combination of personal pin, and biometric fingerprint or facial recognition. This layered approach greatly reduces the risk of compromise, especially in scenarios involving stolen devices or password breaches. Many operating systems and enterprise platforms, such as Windows Hello (biometric-based authentication system) [62] or Google Advanced Protection Program (high-security account protection service), have adopted MFA frameworks to harden endpoint security.

However, while MFA is a powerful tool for access control, it typically focuses only on authentication at the point of login, not on physical protection of asset. Moreover, MFA alone does not address threats such as unauthorised movements around assets, tampering, and unlawful handling. These limitations point to a study gap in combining MFA with

physical intrusion detection, motion sensing and Wi-Fi-based communication model real-time alerts [63] — a hybridisation that could protect both data and hardware in mobile computing environments. This gap further supports the case for an integrated early warning and prevention system that merges software-level controls like MFA with hardware-level detection and communication capabilities.

2.4 PROBLEM IDENTIFICATION AND STUDY GAP

Reviewing these 12 systems reveals a common theme, most are either reactive. None offer a comprehensive, hybrid solution that includes early detection [64] when the asset is under threat, user-based activation and deactivation through biometric fingerprint with reminder feature, live monitoring with response time of 10 seconds and recording, real-time reporting with automatic door locking when incursion has occurred. This literature gap justifies the need for a hybrid early warning system that will detect and prevent mobile asset theft, unlawful handling and theft through biometric activation, physical intrusion detection, intelligent camera surveillance, and real-time alerts using mobile networks, local alarms and smart locking.

2.5 CHAPTER CONCLUSION

This chapter has investigated a different body of insightful and innovative literature encompassing the security of mobile assets, particularly laptops, in situations where information secrecy, physical control, and accountability are vital. It included a range of standalone and integrated approaches including mechanical locking mechanisms such as the Kensington Lock; software-based solutions like Absolute's LoJack and Computrace; IP-based and GPRS tracking systems; biometric authentication and encryption; RFID-based automation; infrared and motion detection using Raspberry Pi; smart touch-sensitive lockers; multi-factor authentication protocols; and cloud-based identity protection systems such as Windows Hello and Google's Advanced Protection Program.

However, through this detailed literature review, a study gap was identified across all reviewed electronic security systems and no single solution offers an integrated, proactive,

and intelligent early warning detection and prevention system that combines physical tamper detection, user-specific authentication, real-time notifications, environmental awareness, and surveillance capability and automatic door locking. Most systems are either reactive (engaging after a breach), limited in scope (e.g., password security without physical security), or require significant user intervention (e.g., remembering to lock devices). Additionally, certain technologies, such as RFID-AM or MFA, excel in secure user verification but fail to address physical asset displacement or tampering. Infrared and PIR systems can detect movement but cannot identify whether such movement constitutes a legitimate access or a breach.

Finally, this review highlights the necessity of a hybrid early warning detection and prevention system. The findings of this chapter provide the conceptual foundation for the research design and technical implementation outlined in the chapters that follow.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter discusses the system design process for mobile assets, which includes the integration of various electronic components to meet the requirements given in the study objectives. The design science research (DSR) methodology [65] was used in the study as a systematic approach, which encompasses hardware and software design, assumptions, system calculations, simulations, and testing methods. This chapter further provides an alternative solution to existing electronic security by ensuring that mobile assets are secure even when the user is not present at the workstation. The system is smart enough to detect when it is in danger and in a compromised situation.

3.2 MOBILE ASSET SECURITY SYSTEM ASSUMPTIONS

Several assumptions are considered when designing an early warning system of mobile devices. In most of these systems, authorised users register their fingerprint in the system database prior to use. This ensures seamless authentication, security, and access management to the mobile asset. The fingerprint authentication procedure is depicted in the graph in Figure 9, which supports important assumptions in mobile early warning systems. Fingerprint scans over time are represented by the blue dashed line, with each scan being either an allowed (1) or unauthorised (0) fingerprint. The system's authentication decision is shown by the red stem plot, which grants access (1) to known users and denies it (0) to fingerprints that are not registered. The biometric fingerprint sensor used supports multiple fingerprint registrations and features a dual LED indicator, which illuminates green when a fingerprint is recognized and red when it is not recognized. This supports the notion that the system is secure because only users who have registered can access it. The early warning system that stops unwanted access and improves security management is supported by the rejection of illegal attempts.

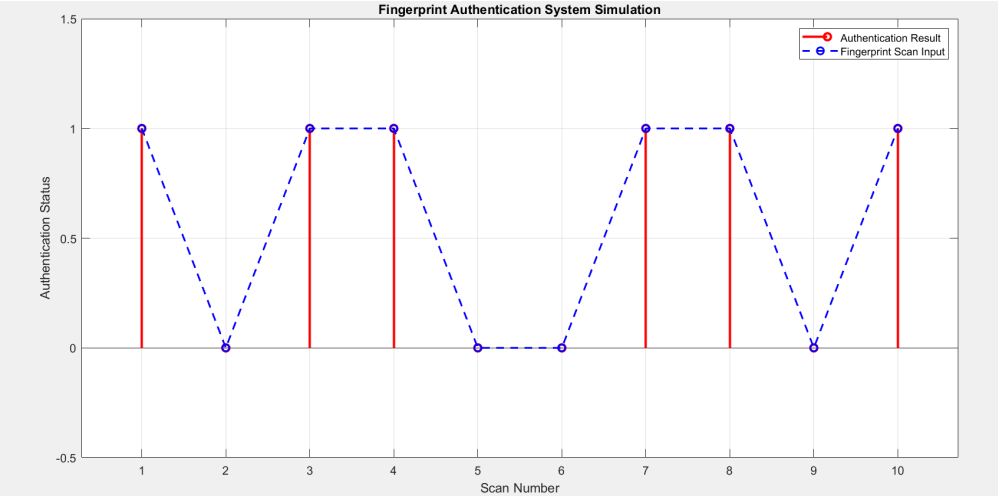


Figure 9: Fingerprint Authentication Process

The other assumption is the response of the intelligent intruder detection system [66]. This assumption includes infrared sensor, intelligent camera, Wi-Fi communication module [67] for reporting the location of where the asset is and smart lock that locks the main access door during intrusion [68]. This assumption simulated various behaviour of the system under different scenarios as depicted in Figure 10 below.

The horizontal axis (X-axis) represents time, measured in discrete time steps and real-time seconds. This axis tracks how the system's responses evolve as different events occur, such as user departure, intrusion detection, and security actions taken. The vertical axis (Y-axis) represents system activation states, ranging between 0 (inactive) and 1 (active) for each component.

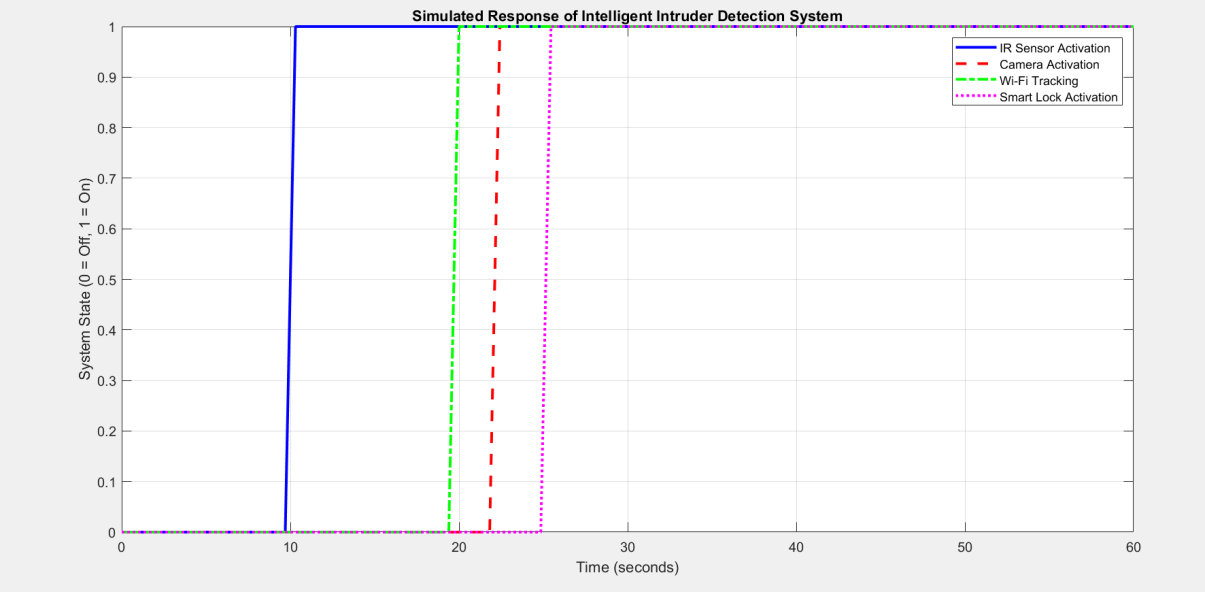


Figure 10: Behaviour of an Early Warning System

Infrared Sensor (IR) activation (Blue Line) at time t = 0, it represents that IR sensor is not active as the authorised user is still at the working station in the office. As soon as the user leaves the working station for a predefined period, the sensor activates (1) to detect unauthorised motion and sends a signal to an intelligent Camera to activate (Red Dotted Line). The camera remains off (0) while the authorised user is in the office. When the system recognises that the user has left for a predefined period, the camera is automatically turned on (1) for real-time remote monitoring. If an intruder is detected, the camera remains active to capture evidence and a Wi-Fi communication module also gets activated (Green Line) to send an addressable location.

If the mobile asset remains within the office, reporting state fluctuates between 0 and 1 as it actively monitors and transmits location data. If the asset is moved without authorisation, the system locks main access door (1) electronically. Smart Lock Activation (Purple Dashed Line) at time t = 0, the smart lock is inactive (0) since the user is present. Once the user leaves and the system detects an intrusion, the smart lock activates (1) to electronically secure the main access door, preventing the intruder from exiting. The lock remains engaged until a reset command is issued by the authorised user or security personnel.

3.3 DESIGN SCIENCE RESEARCH METHODOLOGY

The Design Science Research (DSR) methodology was used in this study to develop and evaluate an intelligent early warning system for preventing the theft of mobile assets, specifically laptops in South African government buildings. The DSR approach was particularly suitable because it focuses on designing and implementing artifacts (such as security systems) that solve real-world problems through iterative development, simulation, and evaluation.

3.3.1 Design & Development of the System

The core system components of the hybrid early warning system for the prevention of mobile asset theft were designed and developed using MATLAB, Simulink, and MikroC [69]. MATLAB and Simulink provided a powerful platform for simulating the system's behaviour under various conditions, while MikroC was used to program a PIC16F628A-microcontroller [70] that coordinated all system components. This approach ensured that both the hardware and software elements were seamlessly integrated, allowing for efficient testing, validation, and refinement of the system design. The limit switch (mechanical lever-type, SPDT, rated for 250V AC/5A and operating at 5V logic level) serves as an input to the microcontroller and is used to detect the presence or absence of the mobile asset. As soon as the mobile asset is removed after system activation, the limit switch returns to its default state and activates the microcontroller input, which in turn triggers the intelligent camera, siren, and intelligent door relay. Its key role is to ensure that the asset is continuously monitored once the system is activated via biometric fingerprint. Furthermore, the door sensor (magnetic reed switch type, normally closed, operating at 3–12V DC) also functions as an input to the microcontroller. It is activated when the door opens for the first time, prompting the user to activate asset security using the biometric fingerprint. Once the asset security is activated, the door sensor is immediately deactivated, allowing the user to open and close the door freely. The system overview is shown in Figure 11.

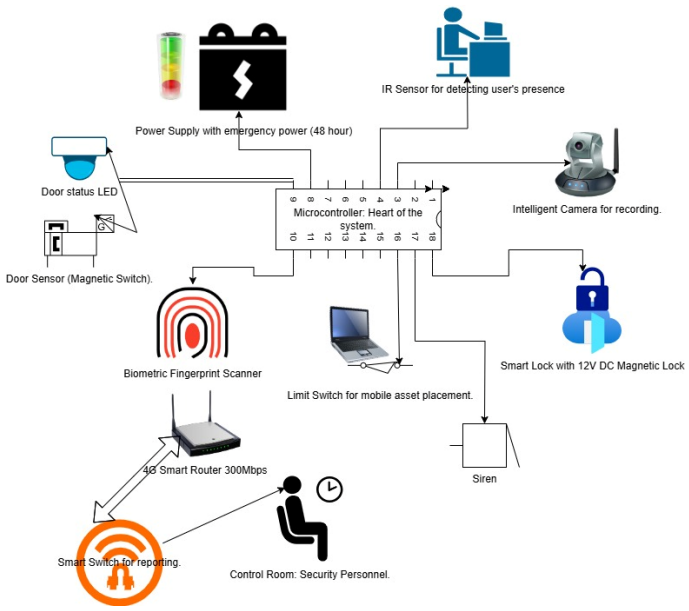


Figure 11: System Overview

System Component Representation

Microcontroller (PIC16F628A): Simulated using a custom logic block in Simulink representing its key I/O behaviours, state transitions, and timing. The firmware logic programmed in MikroC was also used to simulate live system results.

Biometric Fingerprint Module: Represented as a digital input block that provides a high signal upon recognition of an authorized fingerprint and a low signal otherwise. This simulated user login events.

Limit Switch: Modelled as a binary switch block. The presence of the laptop (asset) kept the switch in an active (closed) state. Once the laptop was removed, the switch transitioned to an open state, simulating asset removal.

Door Sensor: Simulated as a digital pulse input to represent door opening. The first pulse triggered a prompt for user biometric activation. If biometric input was not received within a predefined period, an alert sequence was initiated.

Intelligent Camera: Represented as a subsystem that activated upon signal from the microcontroller, when an authorized user has left the working station for a predefined period. It included voice alert output and object tracking simulation, using vision processing blocks to mimic motion detection logic.

Wi-Fi Communication Module and System's Notification: Output ports in Simulink were used to simulate message transmission and alarm triggering. Alert messages were displayed in the simulation output when a breach was detected.

Smart Lock: Upon detection of unauthorized access or asset removal, the smart lock was simulated to engage, locking the door electronically to prevent physical escape and ensure that no one leaves the premises until mobile asset is recovered.

Backup Power Supply: Represented as a system-level constant ensuring uninterrupted operation of the simulated components. The simulation assumed a backup battery capable of powering the system for 48 continuous hours in the event of a main power failure.

Scenario Triggering

- **Initial State**: Door sensor is idle, limit switch is closed (asset present), and system is inactive.
- **Scenario 1 – Door Opens**: Door sensor activates microcontroller waits for biometric authentication.
- **Scenario 2 – Biometric Input**: Fingerprint module is triggered system is activated.
- **Scenario 3 – Asset Removal**: Limit switch changes state microcontroller identifies breach activates intelligent camera and Wi-Fi alert system.
- **Scenario 4 – No Biometric Input**: If the door sensor activates but no biometric input follows within a set time, the system triggers alerts automatically.

- **Scenario 5 – Unauthorized Entry**: If the door is opened without biometric activation, or IR sensor detects no presence, system triggers alarm, smart lock, and camera.
- **Scenario 6 – Lawful Mobile Asset Removal**: If authorized fingerprint is placed on top of the biometric fingerprint again, it deactivates to allow the user to remove the asset lawfully.

3.3.2 Evaluation of the System

Simulation-based evaluation included a MATLAB and Simulink simulations which provided a virtual testing environment to evaluate the system's response under various scenarios. For example, how the system behaves when an authorised user is detected, and how it responds when an unauthorised intrusion occurs. The evaluation focused on system performance metrics like detection time, accuracy of sensor readings, and system responsiveness.

Physical evaluation was conducted after a virtual simulation, the physical evaluation involved deploying the developed code on the microcontroller and testing it in a physical prototype setup. This stage evaluated how well the system functions in real-world conditions as it was tested in two offices of Department of Public Works and Infrastructure (Security Section and Project Management Unit). Evaluation metrics included system reliability, speed of response, and the robustness of the communication between the sensors and the microcontroller.

The iterative nature of Design Science Research Methodology (DSRM) allowed for continuous refinements in both the design and implementation of the system based on evaluation feedback, ensuring that the system met all functional requirements. Figure 12 represents the system response based on DSR approach when an authorised user is detected (represented by 0), the alarm remains off throughout the simulation period, indicating normal operation. However, if an unauthorised intrusion is detected (represented by 1), the alarm is triggered immediately after the intrusion is identified, which is clearly reflected in

the resulting graph. This revision clarifies the expected behaviour of the system during both authorised and unauthorised conditions.

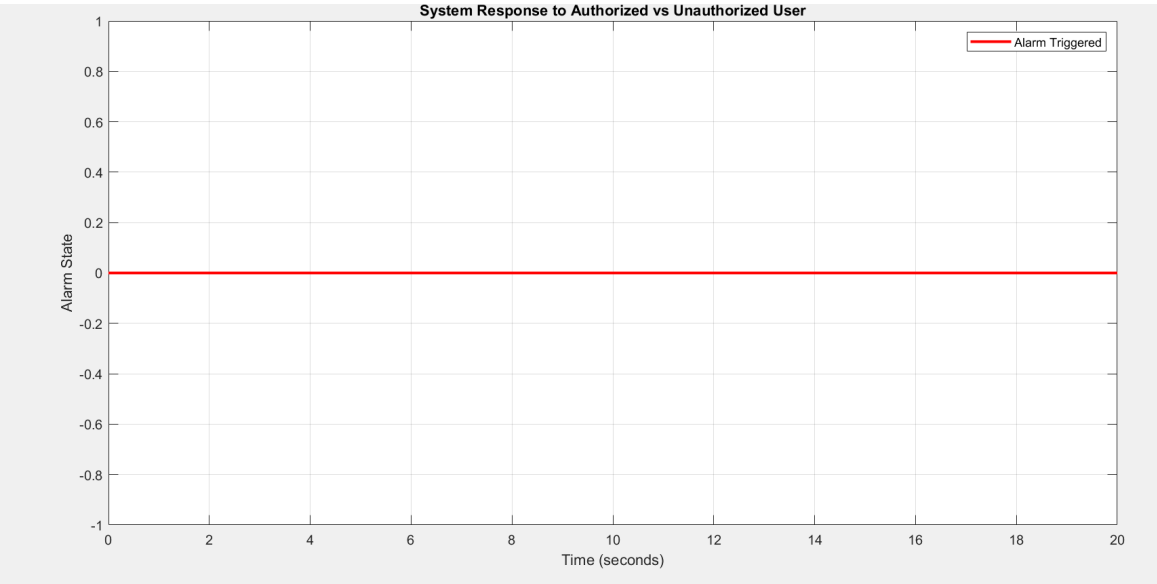


Figure 12: System Response

3.4 SYSTEM FLOWCHARTS

System flowchart shows how the microcontroller coordinated the various system components.

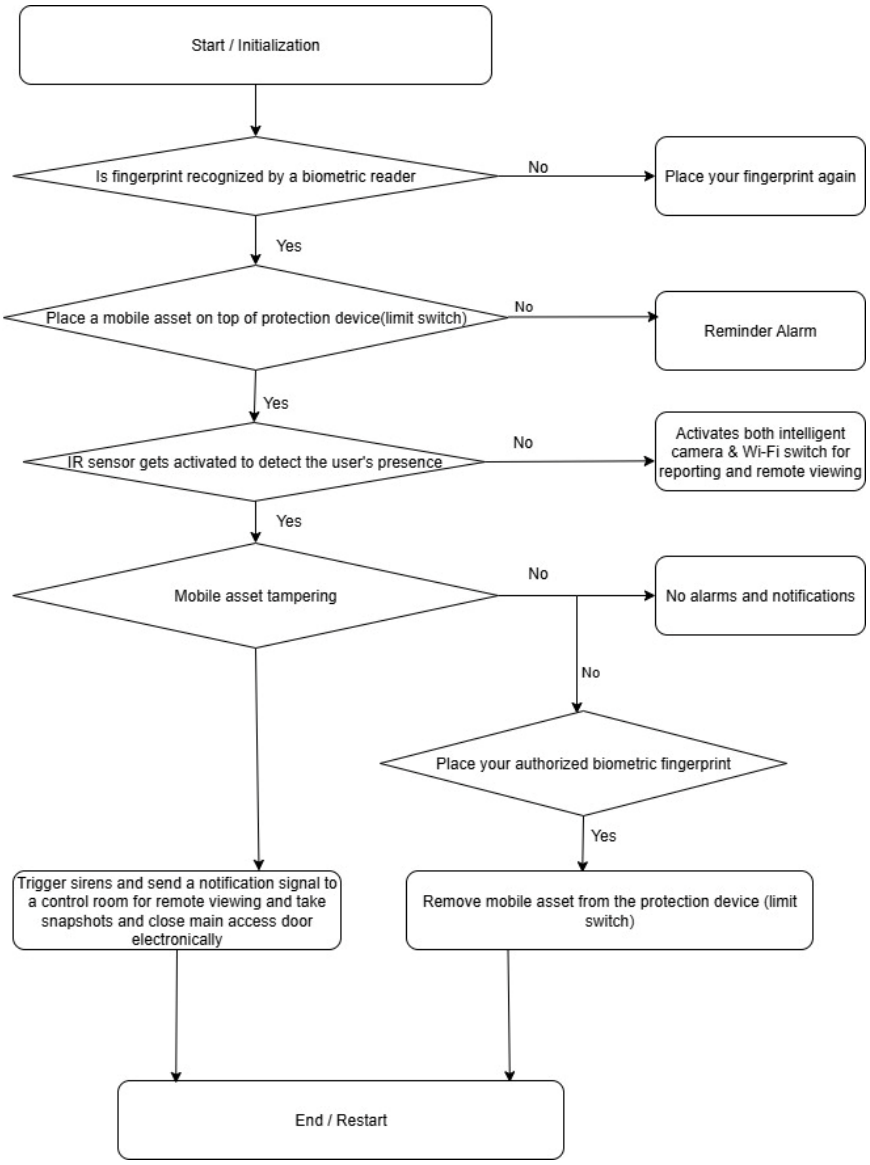


Figure 13: System Flow Chart

Start/ Initialisation:

The system starts by initialising the microcontroller and setting up all system components.

Read Input from Biometric Sensor:

The microcontroller continuously reads input from the authorised personnel.

The biometric fingerprint reads a fingerprint to authenticate the security system of a mobile asset.

Authorised User Check:

The system first checks if an authorised user is detected using a biometric sensor.

- If an authorised user is detected: The system activates and allows for mobile asset placement.
- If no authorised user is detected: The system gives the user to place a fingerprint again.

Mobile Asset Placement Check:

The system checks if the mobile asset has been placed in the correct position.

- If the asset is not placed within a predefined period the warning alarm gets initiated to remind the user to place assets in the correct position.
- If the asset is not placed a warning alarm will keep going on every time the office door is opened to remind the user to place the mobile asset in the correct position.

IR Sensor Activation Check:

The system checks for IR sensor activation after mobile asset placement in the correct position.

- If the IR sensors detects that the authorised user is not present in the working station, both Wi-Fi switch and intelligent camera turns on to alert control room staff about the mobile asset threat.
- If the IR sensor detects authorised movements both Wi-Fi switch and intelligent camera turn off.

Mobile Asset Tampering Check:

The system checks if the mobile asset is not tampered with.

- If the asset is not tampered then there are no alarm and notifications initiated.

- If the asset is tampered the microcontroller sends a notification signal to main access door to be electronically closed and both Wi-Fi switch and intelligent camera get activated for remote viewing and recording.

Mobile Asset Authorized Removal:

The system checks if the mobile asset is removed successfully by an authorized user.

- If mobile asset is not tampered there are no alarms and notifications initiated.
- If authorized fingerprint is placed successfully on the biometric reader then remove the mobile asset using biometric fingerprint again.

3.5 MICROCONTROLLER CODE

Figure 14 shows the snapshot of MikroC code. Intrusion Sensor: Reads the sensor status (1 = intrusion detected, 0 = no intrusion). Relay Lock: Controls the electronic door lock (1 = locked, 0 = unlocked). Alarm: Activates the security alarm upon intrusion detection. Camera: Turns on the camera after 60 seconds if an intrusion is detected. Delay_ms (60000): Introduces a 60-second delay before activating the camera. The system locks the doors upon detecting an intrusion and turns on the surveillance camera after a predefined delay.

```
if (BIOMETRIC_IN == 1) {
   systemArmed = 1;
} else {
   systemArmed = 0;
   BUZZER = 0;
   LED_ALARM = 0;
   CAMERA_TRIG = 0;
}

if (systemArmed) {
   if (IR_SENSOR == 1 || LIMIT_SWITCH == 0) {
      BUZZER = 1;
      LED_ALARM = 1;
      CAMERA_TRIG = 1;
      sendAlert("INTRUSION DETECTED: Check office #23");
      Delay_ms(10000); // Alert duration
      BUZZER = 0;
      LED_ALARM = 0;
      CAMERA_TRIG = 0;
```

Figure 14: MikroC Summary Code

3.6 SYSTEM COORDINATION

All of the components were coordinated by the microcontroller to ensure that they all worked as intended, especially when it came to protecting the mobile asset. A green status indicator indicates that the primary access door, which is typically open, is electrically unlocked, as seen in the Figure 15 below. The door automatically locks itself when it detects an entry, blocking access for a certain amount of time to enable a thorough inspection. This capability was simulated in MATLAB prior to microcontroller programming in order to confirm its efficacy and guarantee smooth integration.

Figure 15: Main Access Door Alarm Status

The alarm status of the main access door is shown over time in the MATLAB graph in Figure 16. The door status is shown by the green line, with 1 indicating an unlocked state and 0 showing the locked door. The door locks for a certain amount of time when an intrusion is detected as indicated with the red line. When the security check is finished, the lock is released, restoring regular access, as depicted by the blue line.

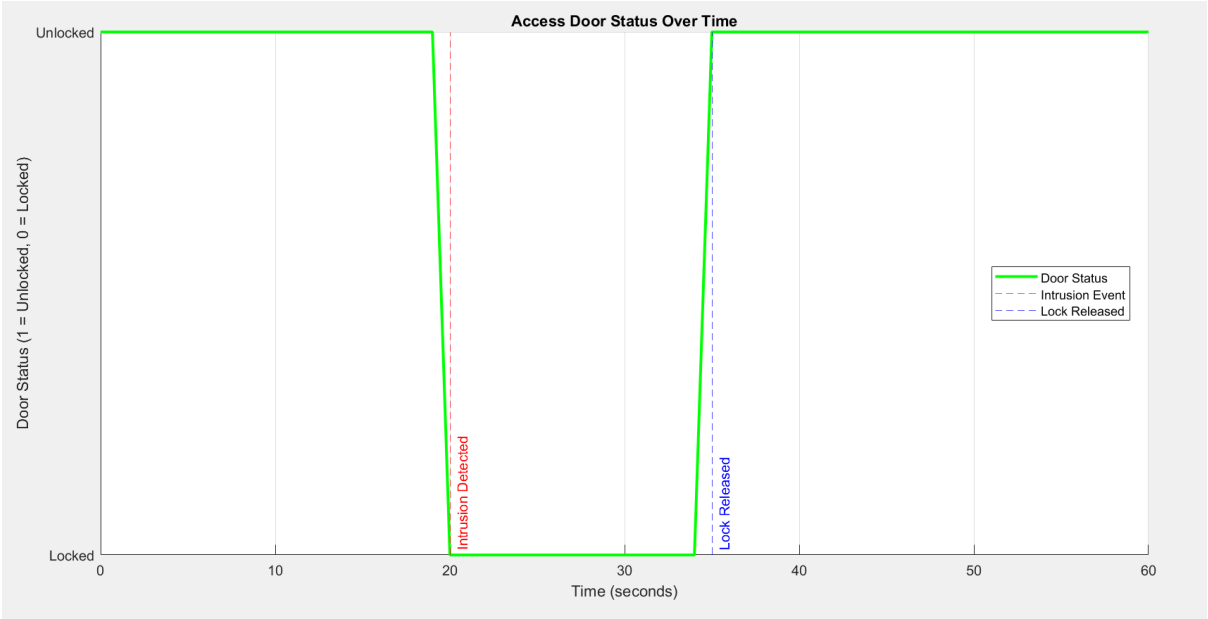


Figure 16: Access Door Status

3.7 SYSTEM TIMING CONSIDERATIONS FOR CAMERA

Variables:

T_Leave: Time when the user leaves the office / working station.

T_Camera_on: Time (60 seconds) when the camera is turned on.

T_Camera_off: Time (< 60 seconds) when the camera is turned off.

T_Period: Predefined time (counter) set in the microcontroller.

Formulas:

Cameras turn on when the predefined period exceeds 60 seconds.

$$T\_Camera\_off = T\_Leave + T\_Period \quad (1)$$

T_Leave = 30 + counter (10 seconds)

= 40 seconds: less than predefined period therefore camera remains off.

$$T\_Camera\_on = T\_Leave + T\_Period \quad (2)$$

T_Leave = 60 + counter (10 seconds)

= 70 seconds: more than predefined period therefore camera on.

Based on the aforementioned delay estimations, Figure 17 shows the camera's delay. The camera status is shown by the green line. The predetermined 60-second threshold is indicated by the red dashed line. The camera stays off, as indicated by the blue marker at 40 seconds. The magenta marker at 70s indicates that the camera activates when the predetermined amount of time has passed. The camera only turns on if the user is gone for more than 60 seconds, as this example demonstrates.

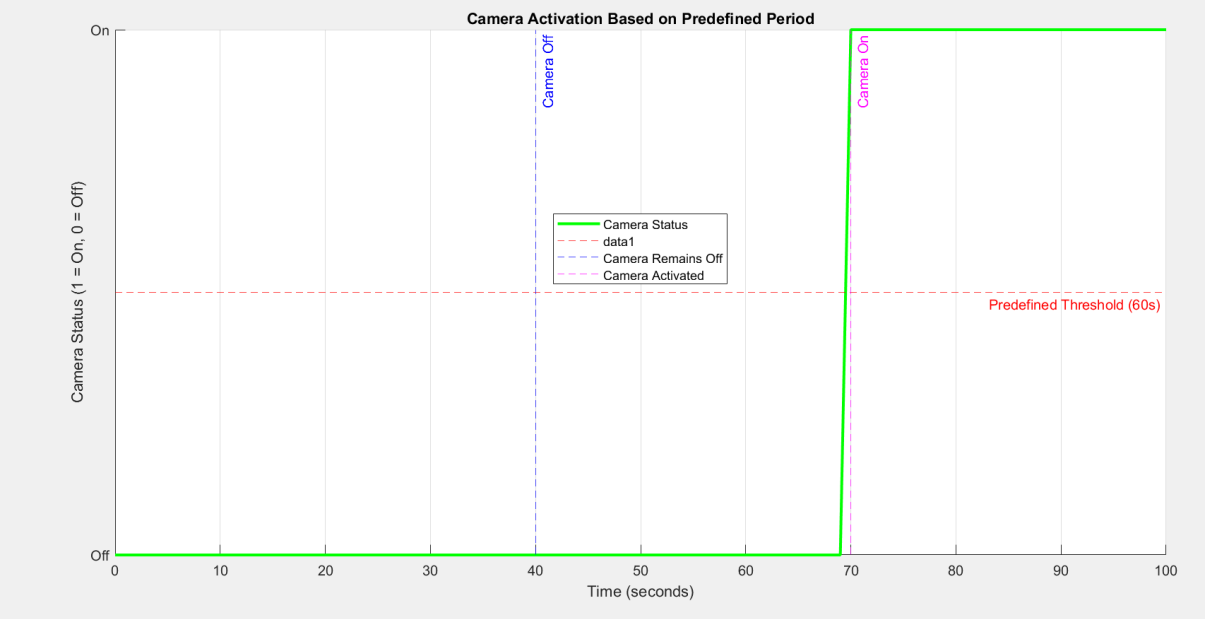


Figure 17: Intelligent Camera Delay

3.8 SYSTEM TIMING CONSIDERATIONS FOR SYSTEM LOCKING MAIN ACCESS DOOR

Variables:

Intrusion: Time (0s) when intrusion has occurred

T_Relay_on: Time (240 seconds)

T_Relay_off: Time (0s).

T_Period: Predefined time (counter) set in the microcontroller.

Formulas:

Relays turn on when the predefined period intrusion occurs, meaning when T_intrusion is greater than 1

$$T\_Relay\_on = Intrusion + T\_Period \quad (3)$$

$$= 1 + 0$$

$$= 1 \text{ seconds}$$

$$T\_Relay\_off = Intrusion + T\_Period \quad (4)$$

$$= 0 + 0$$

$$= 0 \text{ seconds}$$

The relay turns on when an incursion occurs at T_Relay_on = 1s and stays off otherwise, as shown in Figure 18. With 1 denoting ON and 0 denoting OFF, the green line shows the relay status over time. The blue dashed line at 1s shows the precise instant the relay goes on, while the red dashed line at 1s represents the intrusion event that activates the relay. The relay confirms the expected behaviour by staying off for one second before and then staying on for one second after that.

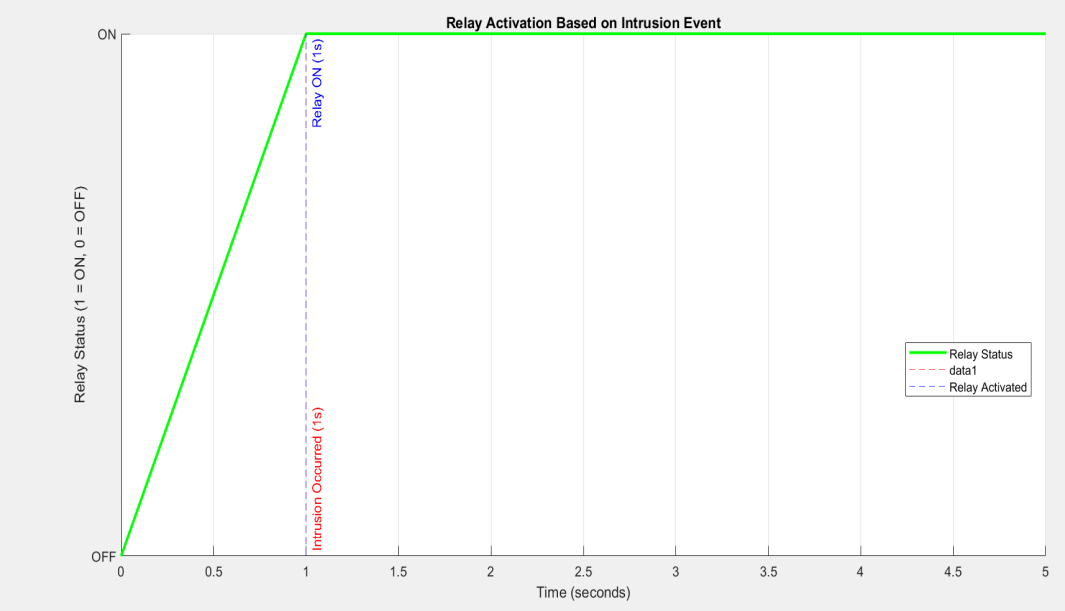


Figure 18: Relay Activation Delay

3.9 SYSTEM TIMING CONSIDERATIONS MICROCONTROLLER DELAY

The Table 1 below shows how delay calculations were done for this study. Timer0 of the microcontroller is configured with the maximum prescaler of 1:256 [71], slowing the effective clock to 1 tick every 256 µs. Since one full overflow takes 256 ticks, each overflow takes 65.536 ms; thus, by counting 15 overflows (15 × 65.536 ms ≈ 983 ms), a delay close to 1 second is achieved.

- Clock Frequency (Fosc): 4 MHz (typical internal oscillator)
- Prescaler: 1:256 (to slow down the timer)
- Timer 0 Register: 8-bit (256 counts)
- Instruction Cycle Time:

Timer Overflow Calculation

The Timer 0 increments every:

$$\text{Tincrement} = Prescaler\ X\ Tcycle \quad (5)$$
$$= 256\ X\ 1us$$
$$= 256us$$

For a full Timer 0 overflow (256 counts):

$$\text{Toverflow} = 256\ X\ 256us \quad (6)$$
$$= 65.5ms$$

To achieve a **1-second delay**:

$65.5ms\ X\ 15\ (overflows)$

=983,04ms

That's almost **1 second (1000 ms)**.

Table 1: Delay Calculation

Prescaler	**Overflow Time (ms)**	**Overflows Needed for 1s**
1:2	0.512 ms	1953
1:4	1.024 ms	977
1:8	2.048 ms	488
1:16	4.096 ms	244
1:32	8.192 ms	122
1:64	16.384 ms	61
1:128	32.768 ms	30.5
1:256	**65.536 ms**	**15.26**

Delay calculations ensure proper sequencing of operations, such as waiting for fingerprint authentication before arming the system or providing a grace period before alert activation,

giving authorised users time to disengage the system. Thus, delays help balance security sensitivity and user convenience**,** making the system both effective and practical.

3.10 SCHEMATIC DIAGRAM

The schematic diagram for the mobile asset security system is depicted below in Figure 19. The microcontroller PIC16F628A serves as the main component. All other components are either inputs or outputs to this microcontroller, and their interactions are based on the system's logic for detecting, authenticating, monitoring, and responding to security breaches.

1. Inputs to the Microcontroller:

- **Biometric Fingerprint Module**
  - Connected to digital input pins of the microcontroller as serves as a major input.
  - Provides a high signal to the microcontroller upon successful authentication and activates the green status LED to ensure that the system is successfully authenticated.
- **Magnetic Door Sensor**
  - Installed on the main office door.
  - Serve as an input to the microcontroller
  - If the door is open and the system is not activated via fingerprint, the microcontroller output activates the relay, which triggers a buzzer.
  - If the system is authenticated, the door sensor becomes inactive.
- **Limit Switch**
  - Mounted beneath the mobile asset.
  - When the mobile asset is removed, the limit switch changes state (from pressed to released or vice versa), sending a signal to the microcontroller, which activates relays to send notifications and smart lock mechanism.
  - Works only when the system is armed.

- **Infrared (IR) Sensor**
  - Positioned to detect the user's presence at the working station.
  - Activated by the microcontroller only when the biometric and limit switch conditions are satisfied.
  - Sends a digital signal to the microcontroller to activate the camera's relay when the movement is absent for a predefined period.

2. Outputs from the Microcontroller:

- **Warning Buzzer**
  - Connected to a digital output pin of a microcontroller via 12V relay.
  - Activated when the door is open and the system is unarmed to remind the user to activate the mobile asset security.
- **Intelligent Camera**
  - Activated when the IR sensor detects absence beyond the allowed predefined period.
  - Provides visual monitoring and audio notification via speaker.
- **Wi-Fi Communication Module**
  - Connected via UART or digital I/O.
  - Sends signals to Google Home upon a tampering event.
- **12V Electromagnetic Door Lock**
  - Controlled via relay driver circuit or transistor switch from microcontroller output pin.
  - Activated automatically during unauthorized access events.
  - Remains locked during a breach to secure the premises.

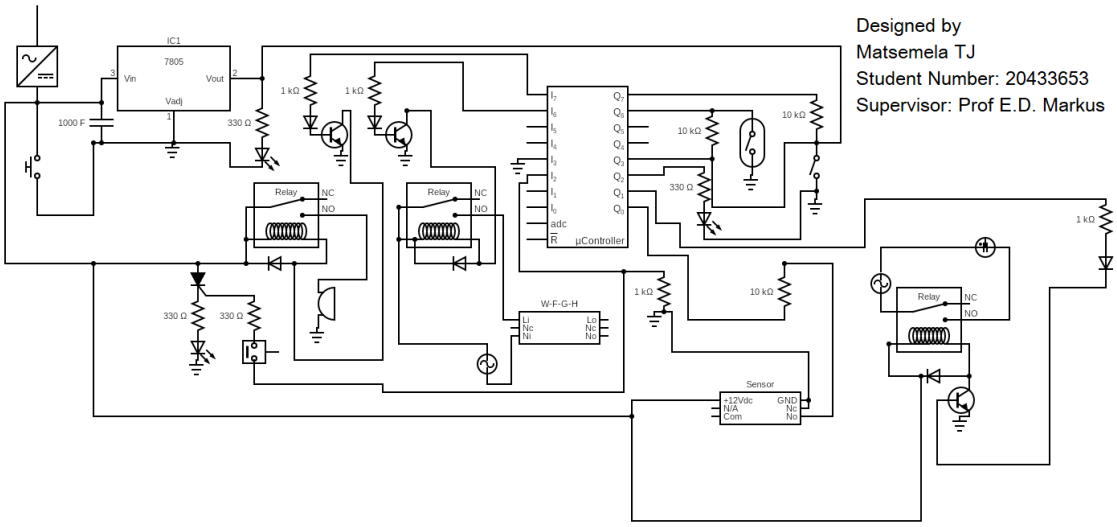


Figure 19: System Schematic Diagram

3.11 CHAPTER CONCLUSION

The PMU and Security department facilities in the Free State Province Department of Public Works and Infrastructure were the subject of this study's successful development and simulation of an early warning detection and prevention system for mobile asset theft in South Africa. The solution was created to offer an early warning detection and prevention of a mobile asset using a real-time intrusion detection, and remote monitoring features, guaranteeing improved protection for priceless mobile assets.

In order to ensure a thorough assessment of system performance, the methods used in this study included a variety of design and simulation methodologies in an organised manner. The development process was directed by the Design Science Research (DSR) approach, which enabled iterative improvements and validation of the system's effectiveness. To guarantee the dependability of the suggested security framework, a number of hypotheses and computations were taken into account. Real-time simulations were made possible by the MATLAB Simulink and modelling environment, which allowed for an accurate evaluation of the system's reaction to intrusion events. The microcontroller firmware was created using the MikroC programming environment, which guarantees smooth communication between sensors, relays, and alarm systems.

The goals of the study were fulfilled as a result of the combination of these elements. The microcontroller was essential in controlling a number of security elements, such as automated door locks, alarm triggers, intruder detection sensors, and surveillance camera activation. The system successfully responded to predetermined security breaches, locking access points, turning on surveillance cameras, and sending out notifications based on the set thresholds, according to the MATLAB simulations. Delay mechanisms were incorporated to enable controlled reactions, minimising false alarms while preserving real-time monitoring capabilities.

Additionally, controlled simulations conducted inside the two chosen buildings confirmed the system's efficacy and showed that it could be used in actual security situations. The findings demonstrated that by automatically protecting access points and notifying security staff, the early warning system effectively stopped the unlawful removal of mobile assets. The results highlight how effective such a security framework can be in preventing asset theft in a range of business and governmental settings, providing a scalable and adaptable solution.

In summary, the study has shown that a comprehensive, microcontroller-based security system that is backed by sophisticated programming methods and MATLAB simulations offers a successful strategy for preventing mobile asset theft. A proactive security response is ensured by the use of automated lockdown features, real-time surveillance activation, and early warning systems. To further improve the system's flexibility and resilience in a variety of security scenarios, future studies might concentrate on combining cloud-based remote monitoring with AI-based threat identification.

CHAPTER 4: RESULTS

4.1 INTRODUCTION

This chapter demonstrates and interprets the results of the hybrid early warning mobile asset security system tested and evaluated in two provincial government buildings in Bloemfontein. The system is designed to provide a robust, layered electronic security solution for mobile assets, particularly laptops, using a blend of enhanced sensing technologies that will differentiate between authorised user and the intruder, embedded control systems, and real-time communication modules.

MATLAB simulations were utilised to visualise the interaction between different components affirming system usefulness under distinctive threat scenarios. These simulations confirmed the anticipated results before actual field testing.

The results are also demonstrated using a series of tables and figures, presenting various system states under both normal and intrusion conditions. The system's deployment in two provincial government buildings has proven its effectiveness. The technology showed real-time detection and response to intrusion, seamless communication with remote security personnel and automatic secure locking mechanisms using electromagnetic lock. These results of various components and microcontroller collectively confirm the system’s reliability and efficient mobile asset protection solution, with potential for broad applicability in areas where mobile asset security is a matter of concern.

Finally, this chapter provides a detailed evaluation and analysis of the experimental results, backed by visual simulations, which together offer strong support for the proposed hybrid security model.

4.2 BIOMETRIC SYSTEM PERFORMANCE

4.2.1 Biometric Analysis

The biometric fingerprint authentication system was analysed beneath changing finger conditions to assess and evaluate its matching performance against the fingerprints stored in the system database. A total of ten different test cases were conducted, as depicted in the Table 2 below, to demonstrate the fingerprint results.

Table 2: Biometric Fingerprint Authentication under Various Conditions

Test Case	Condition	Match Result	Matching Score	Evaluation
TC1	Clean dry finger	Match	98%	True Acceptance (TA)
TC2	Slightly moist finger	Match	95%	True Acceptance (TA)
TC3	Dirty finger	No Match	42%	False Rejection (FRR)
TC4	Clean dry finger	Match	99%	True Acceptance (TA)
TC5	Forged finger (image)	Match	81%	False Acceptance (FAR)
TC6	Clean dry finger	Match	97%	True Acceptance (TA)
TC7	Wet finger	No Match	39%	False Rejection (FRR)
TC8	Partial contact	No Match	45%	False Rejection (FRR)
TC9	Repeated valid scan	Match	99%	True Acceptance (TA)
TC10	Dry cracked skin	Match	92%	True Acceptance (TA)

The outcomes of the fingerprint authentication resulted in six (6) instances of True Acceptance (TA), three (3) instances of False Rejection (FR), and one (1) instance of False Acceptance (FA). These biometric results were further evaluated and analysed using the Chi-square method, based on a total of 120 authentication attempts. It achieved a True

Acceptance Rate (TAR) of 117, slightly exceeding the expected 114, indicating strong authentication performance. The False Acceptance Rate (FAR) was 2, which is better than the expected 3, reflecting improved resistance to unauthorized access. Additionally, the False Rejection Rate (FRR) was 1, outperforming the expected value of 3, suggesting minimal rejection of valid users. Overall, the observed results indicate the system performed better than expected across all key authentication metrics.

Formula:

$$x^2 = \sum_{i=1}^{n} \frac{(Oi-Ei)^2}{Ei} \quad [72] \tag{7}$$

Where:

x^2 = the Chi-square method.

Oi = observed frequency (actual data).

Ei = expected frequency.

x^2 = (0,0789) + (0,3333) + (1,3333)

= 1,7455

A degree of freedom has a value of -1

Three attempts categories include:

$$\text{Percentage} = \left(\frac{Row\ Count}{Total\ Attempts}\right) * 100 \tag{8}$$

TAR = 97.5%

FAR = 1.2%

FRR = 1.3%

$$TAR = \frac{True\ Acceptance}{Total\ Attemps}\ X\ 100 \tag{9}$$

$$= \frac{97.5}{100}\ X\ 120$$

$$= 117$$

$$FAR = \frac{False\ Acceptance}{Total\ Attemps}\ X\ 100 \tag{10}$$

$$= \frac{1.2}{100}\ X\ 120$$

$$= 1.44 \sim 1$$

$$FRR = \frac{False\ Rejection}{Total\ Attemps}\ X\ 100 \qquad (11)$$

$$= \frac{1.3}{100}\ X\ 120$$

$$= 1.56 \sim 2$$

Furthermore, the biometric fingerprint authentication was analysed using a MATLAB where blue dots represent the condition of the biometric fingerprint value. The fingerprint value of 1 or less indicates that the user's fingerprint is recognised by biometric, while any value greater than 1 depicted in red indicates that the fingerprint is not recognised by the biometric fingerprint reader and is rejected. The illustration in Figure 20 reveals that most of the blue dots represent values of 1 or below, contributing to an impressive 98% accuracy.

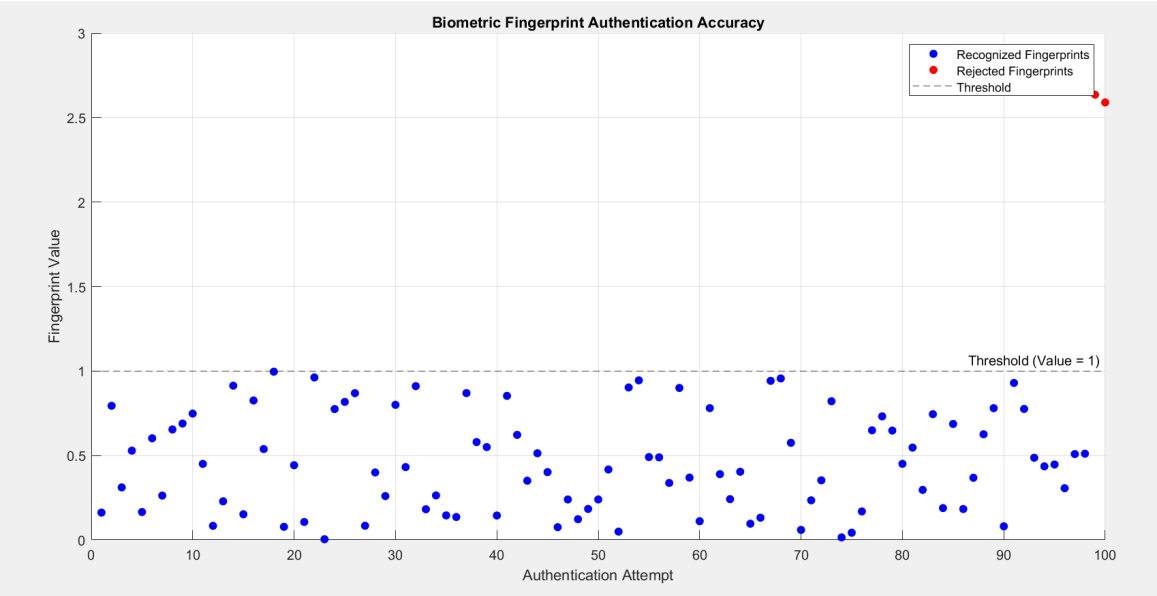


Figure 20: Biometric fingerprint Authentication Accuracy

The biometric authentication accuracy of 98% is sufficient to activate the device. This degree of precision is sufficient to activate and deactivate the mobile asset security. This is an important part of an early warning detection and prevention of a mobile device. The results depicted on Figure 21 shows status of a biometric with both green and red LEDs. When the biometric scanner successfully recognises a fingerprint, it turns on the green LED and authorises access by activating the system. This ensures that the user's fingerprint is

authenticated and is allowed to use a laptop since their biometric fingerprint matches with the one on the database.

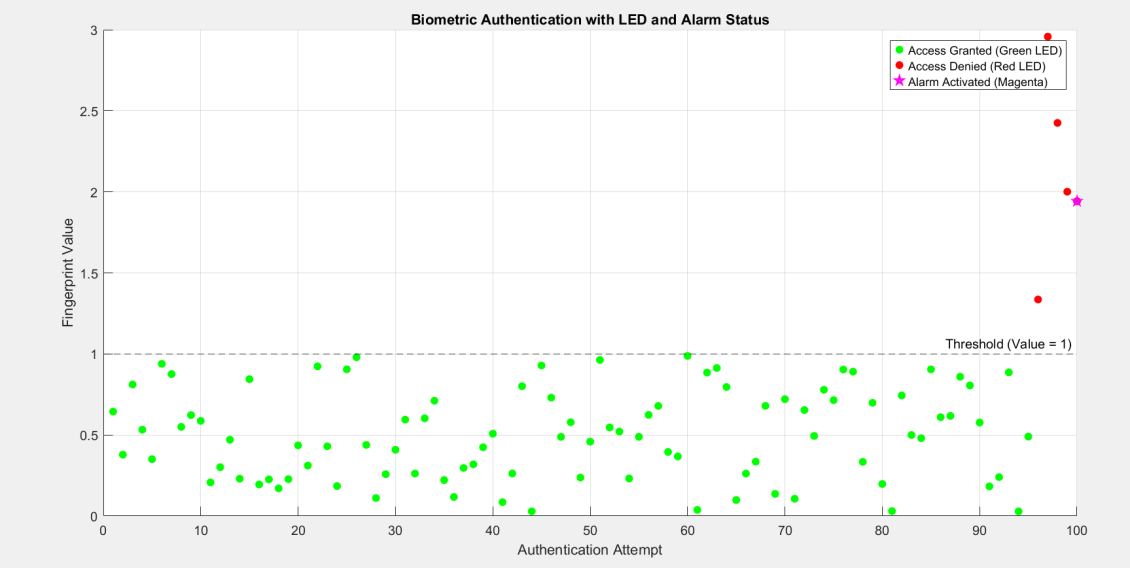


Figure 21: Biometric Authentication with Status LED

4.3 DOOR SENSOR STATUS INDICATOR PERFORMANCE ANALYSIS

Upon completion of biometric fingerprint authentication analysis and evaluation the office door sensor performance was also tested under distinct conditions to analyse the performance and if the door sensor will perform according to the specification outline in the literature review. The simulation tests were conducted in MATLAB as depicted in Figure 22, where red markers indicate the activation of the reminder buzzer, cyan indicates a closed door status, and blue dots shows an open door. The reminder buzzer gets activated only when the door is opened and the biometric mobile asset security is not authenticated. Conversely, when the biometric security system is active, the door sensor is deactivated, guaranteeing that door status changes do not activate the buzzer, thus preventing unnecessary alarms.

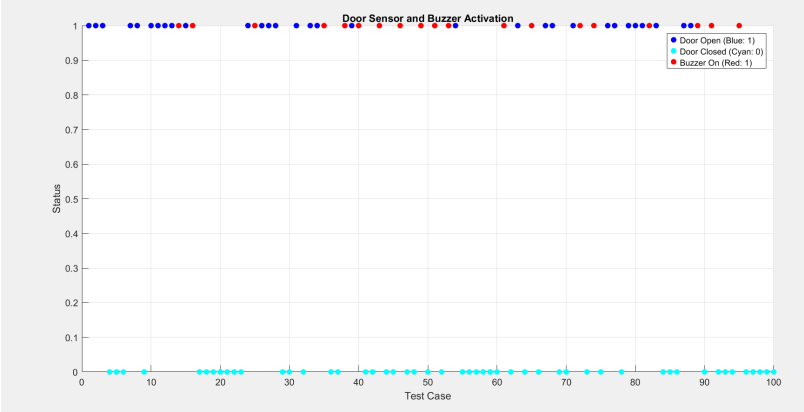


Figure 22: Door sensor status indicator

To evaluate the door sensor operation and reliability, two operational scenarios were tested:

1. Scenario A: Door opened while laptop security is *not* activated.
2. Scenario B: Door opened while laptop security *is* activated.

A total of 100 test runs were conducted the system accurately responded in 99 out of 100 cases, yielding an overall accuracy of 99%. Furthermore, the door sensor accuracy was evaluated using the formula below. Where:

- N = 100: Total Number of Experimental Trials.
- C_correct = 99: Correct system responses
- C_error=1: Incorrect system response),

Then the system accuracy is calculated as:

$$Accuracy = \frac{Correct}{N} \quad (12)$$

$$= \frac{99}{100} X100$$

$$= 99\%$$

Out of 100 simulated scenarios, the system performed as expected in 99 cases. Only one false positive was documented, where the buzzer activated despite the mobile asset security being activated. This corresponds to a 99% system accuracy, indicating excellent operation and dependability between the door sensor and biometric system.

4.4 LIMIT SWITCH PERFORMANCE ANALYSIS

In this hybrid intrusion detection and prevention system, the limit switch is used as a validation mechanism to ensure that a mobile asset (e.g., a laptop and tablet) has been physically placed to its designated placement after successful biometric fingerprint activation. The system integrates conditional logic that accounts for mobile asset placement and door status. If the mobile asset is not placed in the designated position at the working station and the door is opened after biometric authentication, the system triggers a buzzer to alert the authorised user to activate the security system as depicted in Figure 22. However, no alarm is triggered if the door remains closed or if the asset is correctly placed.

The performance analysis of limit switch was tested in four distinct scenarios as depicted in Figure 23 to evaluate the operational performance. The limit sensor's results remained consistent with expectations, reflecting correct logic execution in 99 out of 100 scenarios. A 99% accuracy score demonstrates a high level of reliability in identifying whether an asset is present or missing.

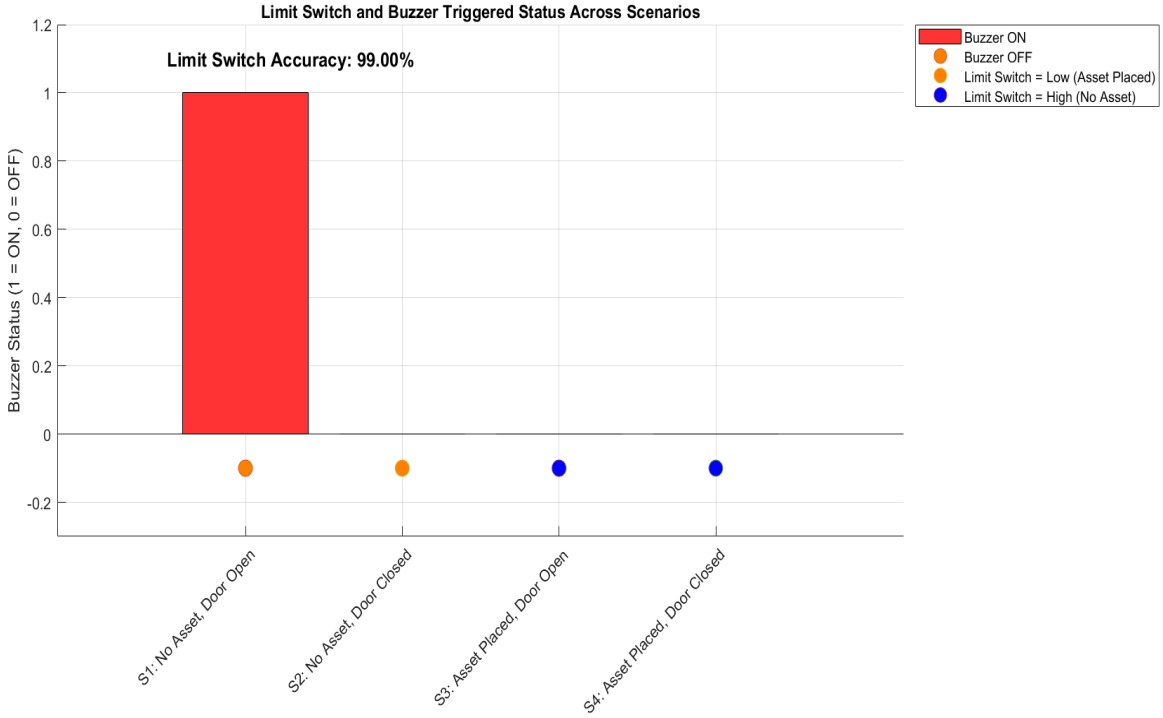


Figure 23: Limit Switch and Buzzer Status

$$Accuracy_{Limit}Switch = \frac{Correct\ Detections}{Total\ Tests} X100 \quad (13)$$

$$= \frac{99}{100}\ X\ 100$$

$$= 99\%$$

4.5 CONDITIONAL PERFORMANCE ANALYSIS OF A MULTI-COMPONENTS

The performance analysis of multi components comprises of IR sensor, intelligent camera and Wi-Fi communication module and was performed in a trial consisting of 50 authentication cycles. The IR sensor demonstrated an accuracy of 96% as depicted in Figure 24.

The intelligent camera, designed to activate solely in the absence of authorised user detection by the IR sensor, recorded an observed accuracy of 50% during the simulation. This result, however, does not imply that the camera's performance is lacking. Instead, it points to the limited scope for evaluation within the context of the simulation. Given that the IR sensor successfully detected user presence in the vast majority of cases (approximately 96% of trials), the camera was only triggered in a very small number of instances. As a result, the accuracy metric was derived from a significantly reduced sample, wherein the camera operated successfully in only one of the two applicable trials. This conditional activation constraint led to an underrepresentation of the camera’s actual performance capability, which under more extensive testing is expected to align with its specified operational accuracy of 94%.

The interrelated outcomes are presented in Table 4 with Wi-Fi communication module displaying an overall performance of and reliability of 98% missing only one incident as shown in scenario 4. The multi-layered results highlight the success in the combined security system, where every part is purposefully connected to enhance the reliability of the prior component. Furthermore, these results provides a reliable approach of detection, asset live monitoring and prompt response.

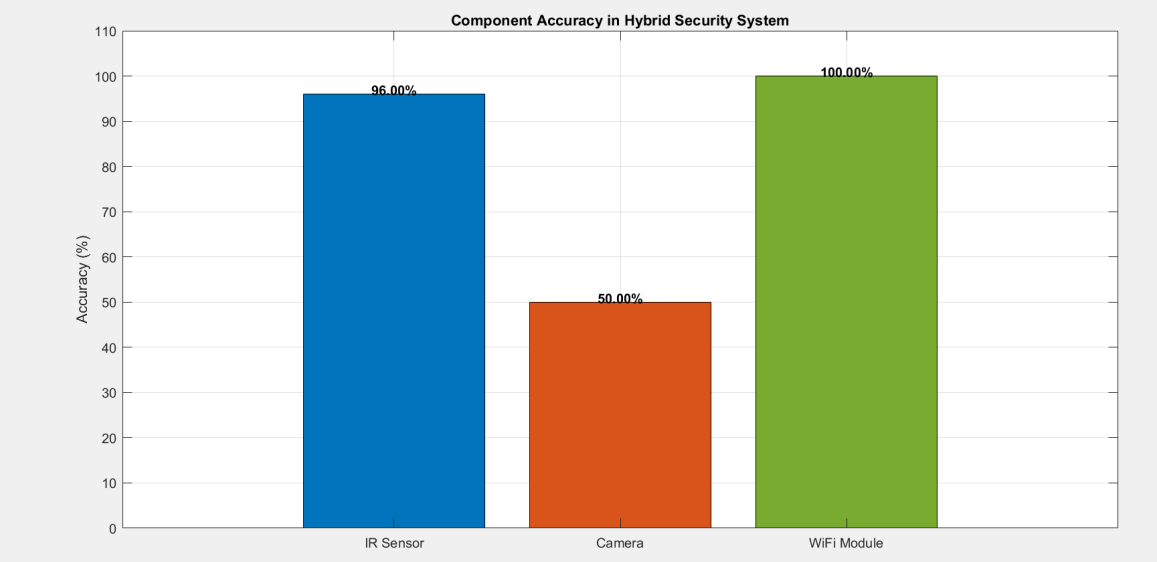


Figure 24: Evaluation of Component-Level Success Rates in a Multi-Layer Intrusion System

The formula used to test the multi-components is given as follows:

- N=50: Total number of test scenarios.
- IR_correct = 48: Correct IR detections
- CAM_correct = 47 Correct intelligent camera activations
- WiFi_correct= 49 Correct Wi-Fi alert transmissions

1. $\text{Accuracy\_IR} = \frac{IR}{N} X100$ (14)

$= \frac{48}{50} X100$

$= 96\%$

2. $\text{Accuracy\_CAM} = \frac{CAM}{N} X100$ (15)

$= \frac{47}{50} X100$

$= 94\%$

3. $\text{Accuracy\_Wi-Fi} = \frac{Wi-Fi}{N} X100$ (16)

$= \frac{49}{50} X100$

$= 98\%$

Table 3: Performance Results under Different Scenarios

Scenario	Biometric Authenticated	Asset Placed	Door Status	Limit Switch State	Buzzer Triggered	IR Detected	Camera Activated	WiFi Alert Sent	System Outcome	System Response Accuracy
S1	Yes	No	Open	High	Yes	Yes	No	No	Reminder triggered	Correct
S2	Yes	No	Closed	High	No	No	Yes	No	No action	Correct
S3	Yes	Yes	Open	Low	No	No	Yes	Yes	Asset confirmed	Correct
S4	Yes	Yes	Closed	Low	No	No	No (missed)	No	Asset confirmed	Incorrect (CAM failure)
S5	–	–	–	–	–	No	Yes	Yes	–	Correct
S6	–	–	–	–	–	Yes	No	No	–	Correct
S7	–	–	–	–	–	No	Yes			

Figure 25 depicts the tampering attempts detected by an intelligent camera. Tampering is demonstrated in red which, shows how many tampering attempts were discovered by the intelligent camera over a 24-hour period. Every hour, a red line representing the data points shows the status of the tampering detection. When tampering is detected, the line increases to a value of 1, and when it is not detected, the line reaches a value of 0. To imitate tampering detected between 10 and 15 hours, a blue mark is employed to show incursion with 99% as also shown in Figure 25. This also shows the camera's intelligence to monitor the mobile device for potential security breaches and activate only when necessary, ensuring efficient operation without unnecessary alerts during periods of no tampering.

The user's presence around the asset is depicted in the mobile device graph (below). The values of 1 (user present) and 0 (user absent) are alternated by the green line. The times that the user is not present at the workstation are shown by black indications. These outcomes mimic how the camera would function, which is to keep it off (0) in most situations to protect the privacy of the authorised user. The intelligent camera, on the other hand, activates tampering detecting systems to ensure the device's security when the user is absent for a predetermined amount of time (1). It will stay on 1 until the authorised user returns to the working station.

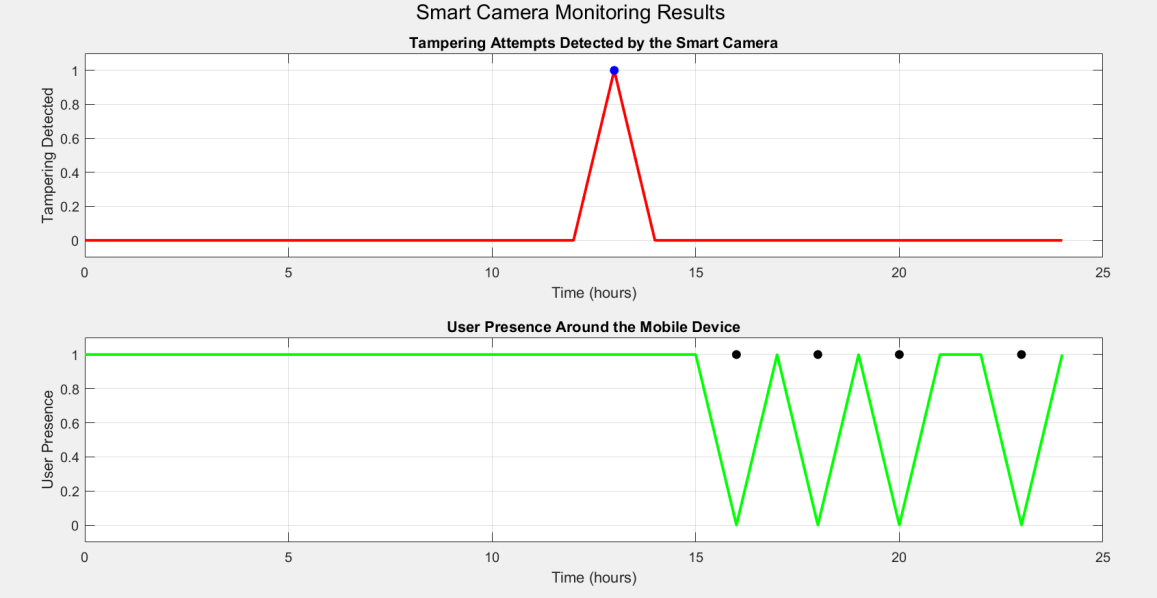


Figure 25: Tampering Attempts

4.6 THREAT PERFORMANCE ANALYSIS AND RESULTS

Upon completion of the performance analysis of the various system components, the vulnerability of the mobile asset was evaluated using a threat score calculation (TSC) in conjunction with the Chi-square (x^2) method to assess system reliability across multiple scenarios. For the purposes of this study, the threshold value for the threat score (T) was established at 0.6, indicating the minimum level at which the system is considered to exhibit a significant threat detection response. When the threat score reaches T=1, the system is configured to initiate both a notification alert and real-time monitoring procedures, in addition to automatically engaging the main door locking mechanism.

- B: Biometric authentication status.
  B=1 if authorized fingerprint is scanned.
  B=0 if no match or no input.

- M: Motion detection status.
  M=1 if unexpected motion is detected.
  M=0 if no motion or authorized movement.

- C: Camera detection confidence status.
  C=1 high threat confidence
  C=0 no threat

  Threat Score Calculation is given as

$$T = \alpha(1 - B) + \beta M + \gamma\, C \quad (17)$$

Assumption weights:

T = Threat Score Calculation.

α = 0.4

β = 0.3

γ = 0.3

a) Mobile Asset Threat Score Calculation: Authorized Access – No threat to mobile asset.

- Biometric Match and Handling of Mobile Asset: B=1
- Motion Detected: M=0
- Camera Detection: C=0

  T= 0.4(1-1) + 0.3(0) + 0.3(0)

  = 0

Outcome: Threat is zero (0), no alarms triggered and the main access door remains open for normal day to day operations.

b) Mobile Asset Threat Score Calculation: Authorized Access – Detection of threat to mobile asset.

- Biometric Match and Handling of Mobile Asset: B=1
- Motion Detected: M=1
- Camera Detection: C=1

T= 0.4(1-1) + 0.3(1) + 0.3(1)

= 0.6

Outcome: Threat is zero 0.6, no alarms triggered and the main door remains unlocked, however, the live viewing turns on to allow security personnel to view asset status.

c) Mobile Asset Threat Score Calculation: No Authorized Access – Mobile Asset under threat.

- Biometric Match and Handling of Mobile Asset: B=0
- Motion Detected: M=1
- Camera Detection: C=1

T= 0.4(1) + 0.3(1) + 0.3(1)

= 1

Outcome:

Threat is zero 1, all notification alarms are triggered and the main door locks electronically to allow security personnel to attend to the scene.

Figure 26: Differential Threat Score Analysis

Figure 26 illustrates the comparative threat levels generated under three different scenarios involving major system components biometric fingerprint authentication, motion detection with limit switch for asset mobile asset positioning and handling, and intelligent camera for remote viewing. Scenario (a), authorised access – no threat to mobile asset, resulted with a threat score of 0 - confirming that the mobile asset is not under threat. Scenario (b), motion detected around mobile asset with intention suspicious intentions, this scenario resulted in a score of 0.6, alerting remote security personnel to view the asset live from the control room and notify the in-house security personnel about possible threats of an asset. Scenario (c), unauthorised access and unlawful handling of an asset which resulted in activation of system notification devices and closing of main access door electronically.

This outcome confirms that the third objective, integrating an early warning detection and prevention algorithm is successfully met, as the system accurately differentiates between authorised user and unauthorised user based on a threshold value ($T \geq 0.6$). The implementation of such an algorithm is important not only in government establishments but in any working environment where laptops, tablets, etc are at risk. Its adaptive and multi-layered nature upgrades situational mindfulness, reduces wrong alerts, and

guarantees quick, intelligent responses from remote and in-house security personnel to real threats, making it universally applicable in modern security systems.

a) **Test Setup in Two Establishments (venue 1 and 2)**

Two establishments were monitored as depicted in Table 4. For each building, 30 independent security events were logged. Each event was categorised by the system as:

- Normal (T < 0.6)
- Monitor Only (T = 0.6)

Table 4: Mobile Asset Threat Analysis in Two Cases

Case 1			
Category	**Observed**	**Expected**	**$(O-E)^2 / E$**
Normal	13	15	0.27
Monitor Only	11	10	0.1
Alert	6	5	0.2
	30	30	***0.57***
Case 2			
Normal	14	15	0.067
Monitor Only	9	10	0.1
Alert	7	5	0.8
	30	30	***0.967***

Both Chi-square values are substantially below the standard critical value of 5.991 for degrees of freedom (df) = 2 at a significance level (α) of 0.05 [73]. This indicates that there is no statistically significant difference between the observed and expected frequencies. Consequently, these cases are regarded as optimal, as they reflect a high level of system accuracy and reliability under test conditions. The low Chi-square values support the null hypothesis, confirming that the system behaves in accordance with its design specifications.

4.7 SMART LOCK FOR CLOSING MAIN ACCESS DOOR IN CASE OF INTRUSION

The simulation results of Real-Time Monitoring and Notification of Security Breaches are depicted in Figure 27 in MATLAB. The simulation was conducted over a period of 10 seconds to test the response of notification system for remote security staff. The time is represented in x-axis in seconds. It was discovered that there was no latency during tests which gave the results of 100%. The y-axis indicates the system status, with 0 (low state) representing normal operation and 1 (high state) signifying an intrusion detection event. During the initial five seconds, the system remains in a normal operational state, indicated by green squares, meaning no tampering of mobile device has taken place. However, at time = 5 seconds, the early warning detection and prevention detects an illegal handling of device in the office, which triggers the Wi-Fi communication module relay to send a security notification. The incursion event is depicted by red diamonds, showing the system's response to unauthorised user. The high state persists for five seconds (from time = 5 to time = 10), ensuring that security personnel are notified remotely and able to respond promptly and alert the mobile user about the incident that has taken place.

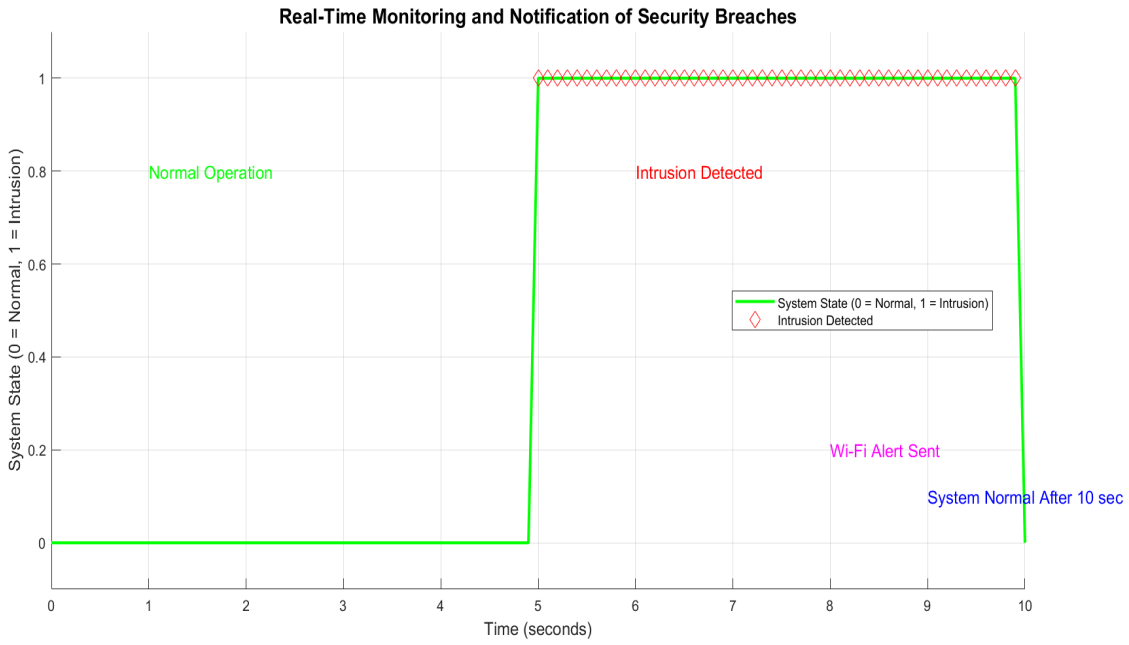


Figure 27: Notification System Analysis

The system relies on a power supply and necessitates backup power to operate effectively. It has been determined that the system requires a 500Ah battery and a 250VAC inverter to sustain functionality for 48 hours. The MATLAB simulation in Figure 28 illustrates the system's parameters and values and Figure 30 and 31 shows the system backup capacity. Additionally, the simulation reveals the lock status in the event of an intrusion. In such instances, the lock is programmed to remain in locked state, with both the 12V DC and 240VAC sirens activated, and the Wi-Fi- communication module alert system triggered. The details of back power are illustrated in the Figure below.

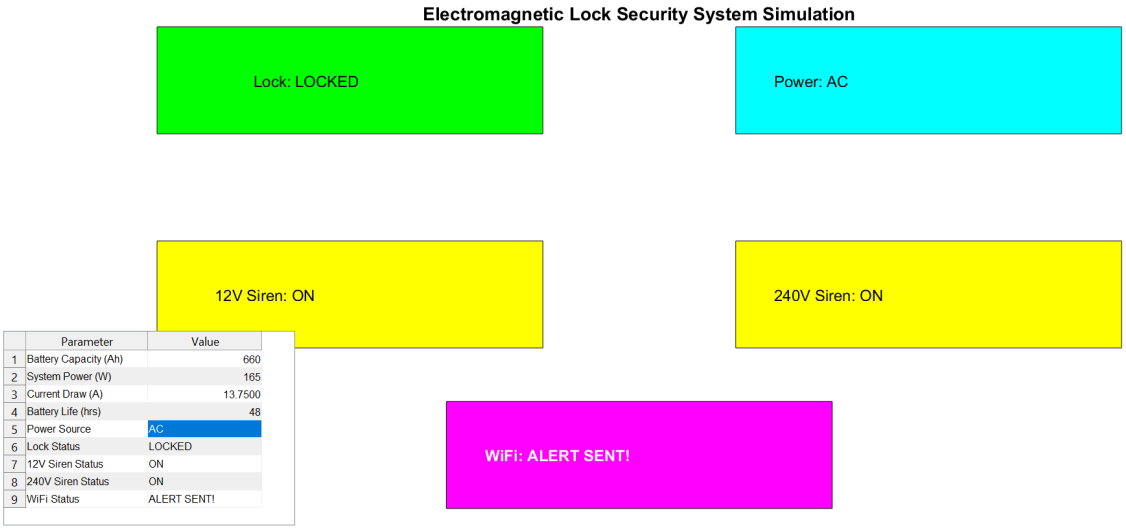


Figure 28: System Notification Devices

4.8 SYSTEM OVERALL PERFORMANCE

The mobile asset detection and protection system achieved a validated overall operational accuracy of 97.5% as derived from a weighted integration of six critical components. This level of performance shows an exceedingly dependable system capable of early detection and protecting mobile computing assets such as laptops and tablets in the working environment, which often contain sensitive data and proprietary information.

The overall system accuracy is computed using a simple arithmetic mean [74] of the individual accuracies:

$$Overall\ Accuracy = \frac{BF+LS+IC+IR+WCM+SL}{6} \quad (18)$$

$$= \frac{98+99+94+96+98+100}{6}$$

$$= 97.5\%$$

The overall system performance is depicted in Figure 29. A 97.5% system accuracy implies a failure probability of only 2.5%, or 2 in 80 events. In actual scenarios, this probability represents a very low risk profile for government establishments and working environment where data loss, theft, or breach could have significant financial or reputational consequences. Given that mobile assets are central to modern workflows, especially in sectors like supply chain management, departmental technical teams, legal, education, and research, a system with this level of security precision ensures that government employees can operate confidently in their offices with minimised mobile asset threat exposure. Even in a primary power failure from the utility, the whole system works 100% including electronic smart lock to ensure reliability and continuous protection of mobile asset, making the system autonomous and fail-safe.

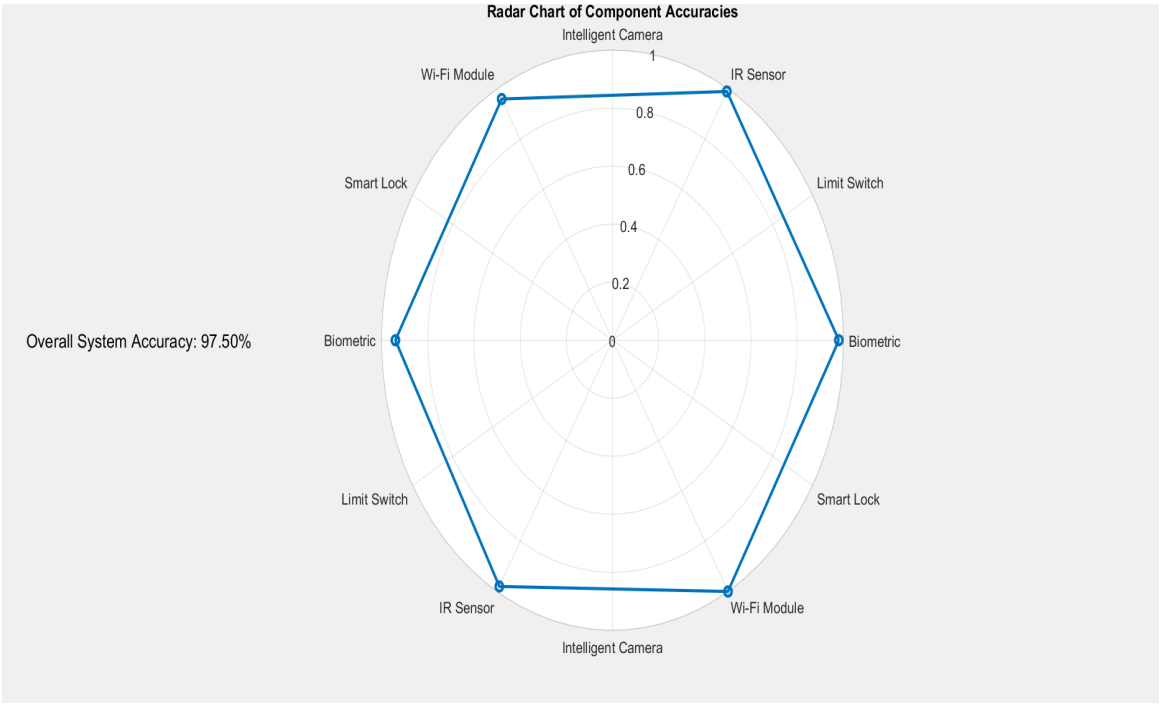


Figure 29: Overall System Accuracy

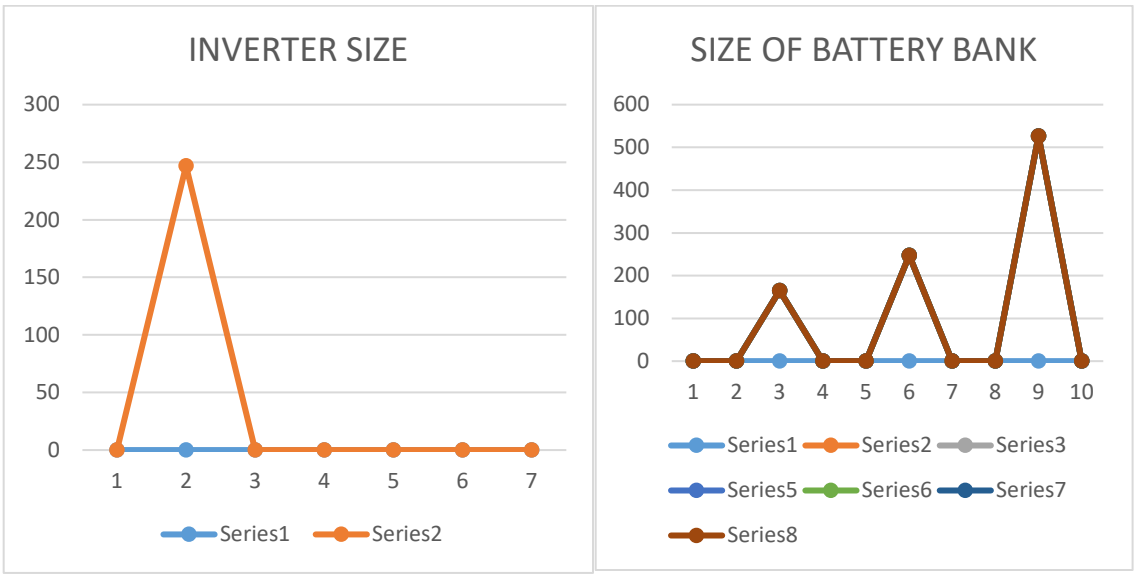


Figure 30: Emergency Power System Capacity

Electrical Load Detail						
Items	Quanity	Voltage	PF	Power		Unit
Microcontroller	1	5,5	0,8	0,01925		W
Magnetic Switch	1	12	0,8	6		W
Magnetic lock	1	12	0,8	7,2		W
Siren DC	1	12	0,8	15		W
Siren AC	1	230	0,8	92		W
Status LED	1	5,5	0,8	0,11		W
Wi-Fi Switch & Google Home	1	230	0,8	0,23		W
IR Sensors	1	5,5	0,8	0,11		W
Biometric Fingerprint Reader	1	5	0,8	1		W
Intelligent Camera	1	5	0,8	10		W
Total Power			**0,8**	**131,6693**		**W**

Inverter / Battery Bank Detail			
AF	Additional further load expansion (Al	20%	
Ie	Efficiency of inverter (Ie)	80%	
Duration	Required Battery Backup (	48	
LF	Loose connection / Wire loss factor 20%		20%
n	Battery Efficiency	90%	
DoD	Depth of Discharge	50%	
Battery Bank Voltage	**12**	**V**	

Load Calculation		
Residential Electrical Load	Load	Unit
	164,5865625	VA

Size of inverter
246,8798438

Size of Battery Bank	
526,677	**AH**

Figure 31: System Emergency Period

4.8 DELIMITATION

This study focuses on detection and protection of mobile assets such as laptops and tablets in government office settings. It prohibits other forms of assets such as vehicles, furniture, or immovable equipment. The system is planned for indoor assets and assumes availability of reliable Wi-Fi communication module.

Combining various components (biometric, IR, Wi-Fi communication module, intelligent camera, electromagnetic lock and IR sensors) into a consistent system poses technical complexity. Calibration for false positives or negatives, especially with IR and fingerprint authentication, requires meticulous testing and optimisation. Ensuring compatibility with existing infrastructure at control rooms and government offices may also introduce unforeseen implementation challenges.

4.10 CHAPTER CONCLUSION

The Results chapter demonstrated the simulation outcomes of a hybrid early warning system for the prevention of mobile asset theft in two various buildings to compare observed results with expected results. Each subsystem, ranging from fingerprint-based user verification, limit switch for mobile asset placement, Wi-Fi communication module, live monitoring, IR sensor motion detection and smart lock control—was systematically modelled and tested in MATLAB. In addition to the detailed scenario-based simulations, various techniques were employed to validate the system's performance. A Chi-square analysis was conducted to survey the unwavering quality of biometric fingerprint authentication, evaluating the True Acceptance Rate (TAR), False Acceptance Rate (FAR), and False Rejection Rate (FRR), thus providing insight into the strength of the fingerprint matching algorithm. A multivariable performance evaluation model was also implemented to analyse system accuracy and response time in time of mobile asset unlawful handling. Furthermore, a threat score calculation methodology was introduced to assess the mobile asset under three distinct scenarios (no threat, detection of threat and mobile asset under

threat. The integration of these tools improved the interpretability of simulation results and empowered a comprehensive performance assessment of the proposed security system. Graphical outputs generated in MATLAB visually demonstrated real-time performance for each component used including user interactions, system responses, and findings, thereby substantiating the system's reliability, accuracy, and rapid responsiveness in preventing unauthorised access or asset tampering.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

The operation of the developed hybrid early warning system for the prevention of mobile asset theft: case of laptops in South African government buildings was broadly examined. The system, which integrates a variety of progressed innovations such as intelligent cameras, infrared sensors, magnetic switches, a siren, biometric fingerprint scanners, limit switches, Wi-Fi communication module for reporting, has proven to be a dependable and versatile solution for protecting mobile assets, particularly laptops, in government establishments.

The system's multi-layered methodology covered a multiple of potential security concerns by coordinating real-time monitoring, illegal access detection, and rapid reaction capabilities. The use of biometric fingerprint reader ensures that only authorised users have access to mobile assets, while the combination of infrared sensor, intelligent camera and Wi-Fi communication module offers constant monitoring and limit switch ensures that the asset is placed in a correct position. The intelligent camera improves visual monitoring by capturing any suspicious behaviour, while the siren serves as a deterrent by bringing rapid attention to potential breaches and smart lock ensures that main access door to the establishment is electronically locked during incursion.

5.2 CONCLUSION

Implementing a hybrid early warning system for mobile asset theft prevention in government establishments has proven to be a convincing solution for improving mobile asset security. This solution executes a comprehensive and multilevel early detection and protection strategy, significantly mitigating the risk of theft and illegal and unlawful handling of mobile assets such as laptops and tablets in the workplace. Moreover, it provides the authorised user with peace of mind knowing that when they are away from their offices the system will be intelligent enough to think for itself and provide first-line

security (remote control room security personnel) with real time notification and live monitoring in case of unauthorised access in the office. The microcontroller serves as the major component as it issues multiple instructions, it also organises the functions of all various components, ensuring smooth communication between devices, and starting appropriate responses when a threat is recognised.

The door magnetic switch sensor with alarm alert monitors the opening and closing of the door. When the door is opened for the first time, a warning signal appears to remind the mobile asset user to activate the system using the biometric reader; once engaged, the door can be left open or closed as desired.

Biometric fingerprint reader guarantees that only authorized personnel can access mobile asset, providing a high level of security as proven by multiple tests took place in two various buildings. The high level of security is provided through a unique identification.

Infrared sensor detect the authorised user movement and presence around mobile asset at the working station. When the user's presence is no longer recognised for a predefined period, a microcontroller receives an instruction to activate an intelligent camera to alert the user through a voice message and if the response is not received from the user for a predefined period time it initiates recording and allow remote security personnel to view the asset.

The limit switch provides an additional layer of protection by monitoring the physical location of mobile assets, ensuring that they stay secure unless accessed by authorised personnel. When unauthorised users tamper with the mobile asset, a command is transmitted to a microcontroller, which activates the siren and smart lock, locking the main access door electronically. Furthermore, a Wi-Fi communication module is triggered, allowing security personnel to obtain relevant information about where the event occurred. Intelligent cameras convey real-time monitoring, capable of detecting suspicious activities as soon as the user or owner of the laptop leaves the working station for a predefined period;

it identifies unauthorised individuals and begins recording, changing directions and following the intruder's movements. It also improves system security by allowing security personnel to take a snapshot of the intruder.

One of the system's most prominent features is its networking and reporting capability. The integration of Wi-Fi communication module and Google Home Application Software enables remote monitoring and rapid alerts, guaranteeing that in house security personnel can be notified immediately and respond quickly to any event. This real-time communication is critical for preventing theft and safeguarding the security of important government assets.

Generally, the developed system successfully coordinates various components into a cohesive and intelligent security network, significantly enhancing the detection and protection of mobile assets. Its capacity to identify, alert, and react to potential theft attempts in real time makes it a valuable device for protecting valuable and sensitive equipment and sensitive information. This creates insights by monitoring itself and discriminating between the intended user and the intruder. It secures the environment for mobile assets while also preventing unwanted access to important government and employee information in facilities. Overall, the study argues that hybrid early warning systems for mobile assets: Case of laptops in South African government buildings is a significant expansion to mobile assets infrastructure in the offices. This solution also increases not only mobile asset security, but also workplace safety and security.

5.3 FUTURE WORK AND RECOMMENDATIONS

This solution can also be utilised in university libraries particularly CUT library where masters and doctoral students are allocated space to do their research, public libraries, and anywhere else where the security of mobile assets is a concern. The device can be put on the study table and allows the librarian to register the user's fingerprint for the duration of the study session, as well as their mobile phone, so they can check their assets and receive notifications when they are away from their study tables.

It also is advised that all system components, including hardware and software, be regularly maintained and updated by accredited personnel. This includes routine checks and tests of sensors, cameras, and switches, as well as the installation of the most recent firmware to defend against vulnerabilities and improve functionality.

Comprehensive training programs should be undertaken by all authorised users to familiarise themselves with the system operation. However, the system is designed to be user friendly and to be operated by anyone including those that are not technically inclined. Regular security practices and simulations are recommended to assess the system's reaction and staff readiness to deal with potential security breaches.

A 24/7 monitoring service and a robust incident response plan are recommended. This ensures that any security issues are noticed and resolved in a timely manner, reducing the risk of theft or damage to government assets.

This system can also be used as energy management and be connected to electrical circuits to turn off electrical appliances like lights, air-conditioners and heaters while the user is way from the office.

REFERENCES

[1] Lima, A., Sousa, B., Cruz, T. and Simoes, P., 2017, March. Security for mobile device assets: A survey. In *ICMLG2017 5th International Conference on Management Leadership and Governance, Academic Conferences and publishing limited* (p. 227).

[2] Dumaguit, J.M. and Salvador, A.R.C.C.C., 2022. Acceptability and relevance of an innovated Arduino-based microcontroller intrusion alarm system. *Sustainable Development*, *10*(2), pp.92-98.

[3] Alwahaishi, S. and Zdrálek, J., 2020, November. Biometric authentication security: an overview. In *2020 IEEE international conference on cloud computing in emerging markets (CCEM)* (pp. 87-91). IEEE.

[4] Chong, P.L., Ganesan, S., Than, Y.Y. and Ravi, P., 2022. Designing an Autonomous Triggering Control System via Motion Detection for IoT Based Smart Home Surveillance CCTV Camera. *Malaysian Journal of Science and Advanced Technology*, pp.80-88.

[5] Talal, M., Zaidan, A.A., Zaidan, B.B., Albahri, A.S., Alamoodi, A.H., Albahri, O.S., Alsalem, M.A., Lim, C.K., Tan, K.L., Shir, W.L. and Mohammed, K.I., 2019. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of Medical Systems*, *43*, pp.1-34.

[6] Al-Humairi, S.N.S., Selvamani, K.A. and Raya, L., 2022, December. Design and Development of an IoT Contactless Door Buzzer, Automation and Home Security Device. In *2022 IEEE 10th Conference on Systems, Process & Control (ICSPC)* (pp. 12-17). IEEE.

[7] Muñoz, J.D., Ruiz-Santaquiteria, J., Deniz, O. and Bueno, G., 2024, February. Weapon Detection Using PTZ Cameras. In *International Conference on Robotics, Computer Vision and Intelligent Systems* (pp. 100-114). Cham: Springer Nature Switzerland.

[8] Syafeeza, A.R., Alif, M.M.F., Athirah, Y.N., Jaafar, A.S., Norihan, A.H. and Saleha, M.S., 2020. IoT based facial recognition door access control home security

system using raspberry pi. *International Journal of Power Electronics and Drive Systems*, *11*(1), pp.417-424.

[9] Patil, K.A., Vittalkar, N., Hiremath, P. and Murthy, M.A., 2020. Smart door locking system using IoT. *International Research Journal on EngTechnol (IRJET)*, *7*(5), pp.3090-3094.

[10] Shi, Q., Zhang, Z., Yang, Y., Shan, X., Salam, B. and Lee, C., 2021. Artificial intelligence of things (AIoT) enabled floor monitoring system for smart home applications. *ACS Nano*, *15*(11), pp.18312-18326.

[11] Simukali, C.M., 2019. *Multi factor authentication access control for student and staff based on RFID, barcode and GIS* (Doctoral dissertation, University of Zambia).

[12] Malatinsky, A., 2023. Integration of alarm security systems. *Przegląd Elektrotechniczny*, *99*.

[13] Al-Doori, V.S., Maktoof, M.A.J., Abdulqader, A.F. and Lienkov, S., 2024, April. Securing Smart Buildings Using RFID and Fingerprint Technologies. In *2024 35th Conference of Open Innovations Association (FRUCT)* (pp. 71-81). IEEE.

[14] Sultana, T. and Wahid, K.A., 2019. IoT-guard: Event-driven fog-based video surveillance system for real-time security management. *IEEE Access*, *7*, pp.134881-134894.

[15] Kaja, N., Shaout, A. and Ma, D., 2019. An intelligent intrusion detection system. *Applied Intelligence*, *49*, pp.3235-3247.

[16] Hemalatha, S., 2020, February. A systematic review on Fingerprint based Biometric Authentication System. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-4). IEEE.

[17] Rogalski, A. and Chrzanowski, K., 2017. Infrared devices and techniques. In *Handbook of optoelectronics* (pp. 633-686). CRC Press.

[18] Zhaxalikov, A., Mombekov, A. and Sotsial, Z., 2024. Surveillance Camera Using Wi-Fi Connection. *Procedia Computer Science*, *231*, pp.721-726.

[19] Tsourma, M. and Dasygenis, M., 2016, August. Development of a hybrid defensive embedded system with face recognition. In *2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)* (pp. 154-157). IEEE.

[20] Haryanti, T., Rakhmawati, N.A., Subriadi, A.P. and Tjahyanto, A., 2022, November. The Design Science Research Methodology (DSRM) for self-assessing digital transformation maturity index in Indonesia. In *2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA)* (pp. 1-7). IEEE.

[21] Mirtsch, M., Blind, K., Koch, C. and Dudek, G., 2021. Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers & security*, *109*, p.102383.

[22] Taiwo, O. and Ezugwu, A.E., 2021. Internet of things-based intelligent smart home control system. *Security and Communication Networks*, *2021*(1), p.9928254.

[23] Su, C. and Chen, W., 2022. Design of Remote Real-Time Monitoring and Control Management System for Smart Home Equipment Based on Wireless Multihop Sensor Network. *Journal of Sensors*, *2022*(1), p.6228440.

[24] Ferraro, M., Brunaccini, G., Sergi, F., Aloisio, D., Randazzo, N. and Antonucci, V., 2020. From Uninterruptible Power Supply to resilient smart micro grid: The case of a battery storage at telecommunication station. *Journal of Energy Storage*, *28*, p.101207.

[25] Metcalfe, A., Green, D., Greenfield, T., Mansor, M., Smith, A. and Tuke, J., 2019. *Statistics in engineering: With examples in MATLAB® and R*. Chapman and Hall/CRC.

[26] Dimkov, T., Pieters, W. and Hartel, P., 2010, December. Effectiveness of physical, social and digital mechanisms against laptop theft in open organizations.

In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing* (pp. 727-732). IEEE.

[27] Datta, N., Malik, A., Agarwal, M. and Jhunjhunwala, A., 2019, April. Real time tracking and alert system for laptop through implementation of GPS, GSM, motion sensor and cloud services for antitheft purposes. In *2019 4th international conference on internet of things: smart innovation and usages (IoT-SIU)* (pp. 1-6). IEEE.

[28] Dave, H.H., 2021. *Automated Analysis and Verification of UEFI BIOS Stress and Stability Testing* (Doctoral dissertation, Institute of Technology).

[29] Luckett, P., McDonald, J.T., Glisson, W.B., Benton, R., Dawson, J. and Doyle, B.A., 2018. Identifying stealth malware using CPU power consumption and learning algorithms. *Journal of Computer Security*, *26*(5), pp.589-613.

[30] Saxon, J. and Feamster, N., 2022, March. GPS-based geolocation of consumer IP addresses. In *International conference on passive and active network measurement* (pp. 122-151). Cham: Springer International Publishing.

[31] Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R. and Lopatka, M., 2020, April. Don't count me out: On the relevance of IP address in the tracking ecosystem. In *Proceedings of The Web Conference 2020* (pp. 808-815).

[32] Chatterjee, S., 2022. Design and Implementation of Laptop Tracking System Based on Cloud Computing and IoT. In *ICT Systems and Sustainability: Proceedings of ICT4SD 2021, Volume 1* (pp. 205-215). Springer Singapore.

[33] Fonseca, O., Cunha, Í., Fazzion, E., Meira, W., da Silva, B.A., Ferreira, R.A. and Katz-Bassett, E., 2021. Identifying networks vulnerable to IP spoofing. *IEEE Transactions on Network and Service Management*, *18*(3), pp.3170-3183.

[34] Siyed, Z., 2023. A new cyber risk: how teens expose corporations in WFH era. *Journal of Information Security*, *14*(4), pp.396-421.

[35] Imam, M.A.Y. and Biswas, M.P.K., 2023. MAC Address Cloning Technique Results. *Contemporary Perspective on Science, Technology and Research*, p.120.

[36] Schenk, D. and Krummrich, P.M., 2016. A novel approach to reduce the impact of physical layer restrictions in dynamically switched transparent optical networks. *Journal of Lightwave Technology*, *34*(9), pp.2304-2310.

[37] Margapuri, V., 2020. Smart motion detection system using raspberry pi. *arXiv preprint arXiv:2006.06442*.

[38] Sahoo, K.C. and Pati, U.C., 2017, May. IoT based intrusion detection system using PIR sensor. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1641-1645). IEEE.

[39] Al-Jarwany, Q.A., Hamad, A.R., Sabbar, B.M., Mnati, M.J., Ali, A.H. and Van Den Bossche, A., 2024. System Design and Implementation for Machine Learning and Internet of Things Based Anomaly Detection in Patient Movement. *Journal of Electrical Systems*, *20*(5s), pp.2216-2232.

[40] Azhar, A.H., Othman, M.F.I., Bahaman, N., Mas'ud, M.Z. and Sa'aya, Z., 2021. Implementation of home security motion detector using Raspberry Pi and PIR sensor. *Journal of Advanced Computing Technology and Application (JACTA)*, *3*(2), pp.41-50.

[41] Mane, S.S. and Talmale, G.R., 2017. Raspberry-Pi based security system on IoT platform. In *International Conference on Recent Trends in Engineering Science and Technology* (Vol. 5, No. 1, pp. 17-20).

[42] Hazra, R., Chatterjee, P., Singh, Y., Podder, G. and Das, T., 2024. Data Encryption and Secure Communication Protocols. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 546-570). IGI Global.

[43] Karthikeyan, S., Raj, R.A., Cruz, M.V., Chen, L., Vishal, J.A. and Rohith, V.S., 2023. A systematic analysis on raspberry pi prototyping: Uses, challenges, benefits, and drawbacks. *IEEE Internet of Things Journal*, *10*(16), pp.14397-14417.

[44] Das, A.K., Zeadally, S. and Wazid, M., 2017. Lightweight authentication protocols for wearable devices. *Computers & Electrical Engineering*, *63*, pp.196-208.

[45] Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R. and Formica, D., 2017. Performance evaluation of bluetooth low energy: A systematic review. *Sensors*, *17*(12), p.2898.

[46] Das, A.K., Zeadally, S. and Wazid, M., 2017. Lightweight authentication protocols for wearable devices. *Computers & Electrical Engineering*, *63*, pp.196-208.

[47] Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M. and Seneviratne, A., 2017. A survey of wearable devices and challenges. *IEEE Communications Surveys & Tutorials*, *19*(4), pp.2573-2620.

[48] Prasant, P., Bhardwaj, S., Gupta, M., Srivastava, M., Singh, J. and Maurya, R.K., 2022. Role of internet of things in protecting different wearable gadgets and materials. *Materials Today: Proceedings*, *56*, pp.3387-3393.

[49] Foster, A.L., 2008. Increase in stolen laptops endangers data security. *The Chronicle of Higher Education*, pp.43-45.

[50] Simukali, C.M., 2019. *Multi factor authentication access control for student and staff based on RFID, barcode and GIS* (Doctoral dissertation, University of Zambia).

[51] Mhlaba, A. and Masinde, M., 2015, May. A hardware based model for an asset monitoring and tracking system: Case of laptops. In *2015 international conference on emerging trends in networks and computer communications (ETNCC)* (pp. 155-161). IEEE.

[52] Ismail, M.I.M., Dziyauddin, R.A., Ahmad, R., Ahmad, N., Ahmad, N.A. and Hamid, A.M.A., 2021. A review of energy harvesting in localization for wireless sensor node tracking. *IEEE Access*, *9*, pp.60108-60122.

[53] Zeyad, M., Ghosh, S. and Ahmed, S.M., 2019. Design prototype of a smart household touch sensitive locker security system based on GSM

technology. *International Journal of Power Electronics and Drive Systems*, *10*(4), p.1923.

[54] Ihedioha Ahmed, C. and Eneh Ifeanyichukwu, I., 2016. Home automation using global system for mobile communications (GSM). *Int J Emer Technol Eng Res (IJETER)*, *4*(1), pp.54-58.

[55] Sharma, A., Kumar, N. and Sharma, H., 2017. Infrared Sensor based Laptop Security System to Avoid Theft & Misuse: A Patented Idea. *International Journal of Advanced Research in Science and Engineering*, *6*(8).

[56] Dhany, H.W., Izhari, F., Fahmi, H., Tulus, M. and Sutarman, M., 2017, October. Encryption and decryption using password based encryption, MD5, and DES. In *International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017)* (pp. 278-283). Atlantis Press.

[57] Dhany, H.W., Izhari, F., Fahmi, H., Tulus, M. and Sutarman, M., 2017, October. Encryption and decryption using password based encryption, MD5, and DES. In *International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017)* (pp. 278-283). Atlantis Press.

[58] Putman, C.G.J., 2021. *A Requirements Based Selection Model for Future Proof Non-Intrusive Authentication Technologies in the Office* (Master's thesis, University of Twente).

[59] Syta, E., Kurkovsky, S. and Casano, B., 2010, January. RFID-based authentication middleware for mobile devices. In *2010 43rd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

[60] Álvarez López, Y., Franssen, J., Álvarez Narciandi, G., Pagnozzi, J., González-Pinto Arrillaga, I. and Las-Heras Andrés, F., 2018. RFID technology for management and tracking: E-health applications. *Sensors*, *18*(8), p.2663.

[61] Liu, Y., Zhong, Q., Chang, L., Xia, Z., He, D. and Cheng, C., 2017. A secure data backup scheme using multi-factor authentication. *IET Information security*, *11*(5), pp.250-255.

[62] Haddad, J., Pitropakis, N., Chrysoulas, C., Lemoudden, M. and Buchanan, W.J., 2023. Attacking Windows Hello for Business: Is It What We Were Promised? *Cryptography*, *7*(1), p.9.

[63] Rahman, M.A. and Forhad, M.S.A., 2019, December. Wi-Fi based real time communication for disaster and emergencies. In *2019 2nd international conference on innovation in engineering and technology (ICIET)* (pp. 1-6). IEEE.

[64] Almazroi, A.A. and Ayub, N., 2024. Deep learning hybridization for improved malware detection in smart Internet of Things. *Scientific reports*, *14*(1), p.7838.

[65] Vom Brocke, J., Hevner, A. and Maedche, A., 2020. Introduction to design science research. *Design science research. Cases*, pp.1-13.

[66] Vanin, P., Newe, T., Dhirani, L.L., O'Connell, E., O'Shea, D., Lee, B. and Rao, M., 2022. A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences*, *12*(22), p.11752.

[67] Kurniawan, F.A., Rochimawati, I., Saddiq, A., Saragih, Y. and Saragih, C.I., 2023, November. Implementation of an ESP-32 Wi-Fi CAM & Arduino-Based Robot for IoT Surveillance. In *Seminar Nasional Teknik Elektro*.

[68] Gadupu, H., Mokharji, O., Kankaria, R., Kumar, S. and Jayavel, K., 2021. ACCESS-IoT enabled smart lock. *International Journal of Reconfigurable and Embedded Systems*, *10*(3), p.176.

[69] Hussain, A., Hammad, M., Hafeez, K. and Zainab, T., 2016. Programming a microcontroller. *Int. J. Comput. Appl*, *155*(5), pp.21-26.

[70] Amusa, K.A., Adewusi, A., Nuga, O.O., Olanipekun, A.J. and Adewale, O.A., 2015. Pyro-Electric Infrared Sensor-Based Intrusion Detection and Reporting System. *Afr J. of Comp & ICTs*, *8*(2), pp.91-98.

[71] Aslam, S., Hannan, S., Haider, A. and Tariq, M.H., 2016. Exploring PIC 24F series Microcontroller using MPLAB and Proteus. *Journal of Current Research in Science*, *4*(2), p.164.

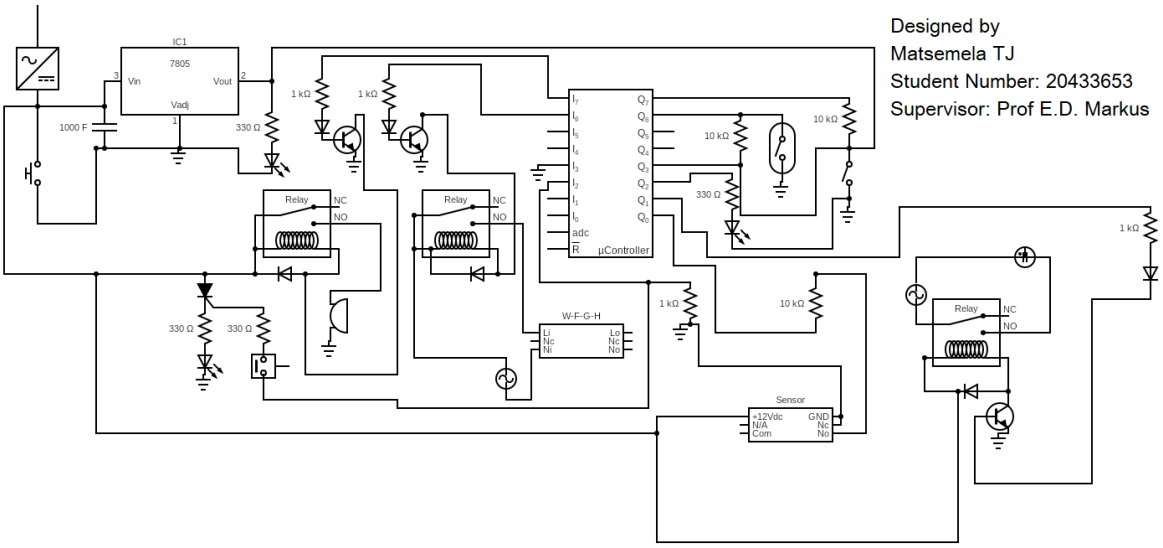
[72] Turhan, N.S., 2020. Karl Pearson's Chi-Square Tests. *Educational Research and Reviews*, *16*(9), pp.575-580.

[73] Olanusi, D.J. and Samuel, S.A., 2023. Application of Chi-Square Test to Determine Architectural Impact on Church Patronage. *International Journal of Research and Innovation in Social Science. https://doi. org/10.47772/ijriss*.

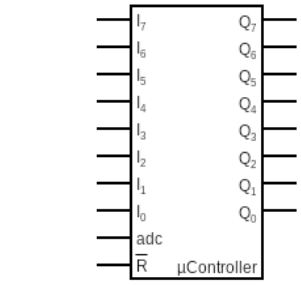
[74] Tian, S., Zhang, J., Chen, L., Liu, H. and Wang, Y., 2020. Random sampling-arithmetic mean: A simple method of meteorological data quality control based on random observation thought. *IEEE Access*, *8*, pp.226999-227013.

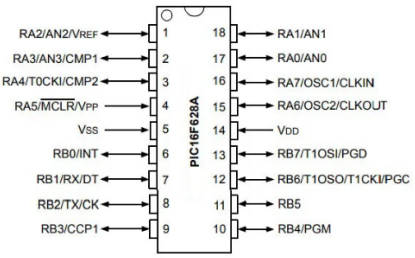
APPENDICES

6.1 SCHEMATIC DRAWING



Legend

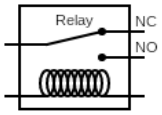
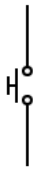
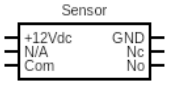
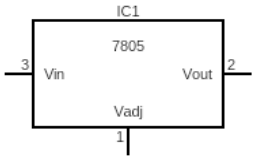


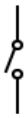


PIC16F628A

- I7: RA2
- I6: RA3
- I5: RA4
- I4: MCLR
- I3: GND
- I2: RB0
- I1: RB1
- I0: RB2
- ADC: RB3
- R: RB4
- Q0: RB5
- Q1: RB6

	• Q2: RB7 • Q3: VCC • Q4: RA6 • Q5: RA7 • Q6: RA0 • Q7: RA1
	Ground
	Power Supply 230 VAC – 12 VDC
	Reed Switch (Door Sensor)
	Resistor Quarter Watt
	12 VDC Siren
	5 VDC Biometric Reader
	5mm Light Emitting Diode

	12 VDC Coil; 10A;230VAC Contacts
	10A Wi-Fi Intelligent Switch
	1n4007 Diode
	Reset Key Switch
	230 VAC Power Supply
	12 VDC PIR Sensor
	2n2930 Transistor (NPN)
	Silicon Controlled Rectifier BT-151
	LM7805 Regulator
	1000 uF Capacitor

	Limit Switch for Laptop

6.2 MICROCONTROLLER – CODE

```
; ADDRESS    OPCODE       ASM
; ----------------------------------------
                    GOTO _main
          _main:

TRISB = 0B00100001;
MOVLW       33
BCF    STATUS, RP1
BSF    STATUS, RP0
MOVWF       TRISB
TRISA = 0B11110011;
MOVLW       243
MOVWF       TRISA
CMCON=0X07;
MOVLW       7
BCF    STATUS, RP0
MOVWF       CMCON
PORTA = 0X00;
CLRF  PORTA, 1
PORTB = 0X00;
CLRF  PORTB, 1
Delay_ms(1);
MOVLW       2
MOVWF       STACK_11
MOVLW       255
MOVWF       STACK_10
DECFSZ      STACK_11, F
GOTO $+2
```

```
GOTO $+4
                DECFSZ      STACK_10, F
GOTO $-1
            GOTO $-5
                MOVLW       74
            MOVWF       STACK_10
                DECFSZ      STACK_10, F
            GOTO $-1
            PORTB.F7=0;
            BCF    PORTB, 7
            PORTB.F3=1;
BSF    PORTB, 3
Delay_ms(5000);
MOVLW       26
MOVWF       STACK_12
MOVLW       255
MOVWF       STACK_11
MOVLW       255
MOVWF       STACK_10
                DECFSZ      STACK_12, F
                GOTO $+2
                GOTO $+8
                DECFSZ      STACK_11, F
                GOTO $+2
                GOTO $+4
                DECFSZ      STACK_10, F
                GOTO $-1
                GOTO $-5
            GOTO $-9
            MOVLW       127
```

```
                MOVWF       STACK_11
                MOVLW       255
                MOVWF       STACK_10
                        DECFSZ      STACK_11, F
                GOTO $+2
                GOTO $+4
        DECFSZ      STACK_10, F
                        GOTO $-1
                GOTO $-5
                        MOVLW       88
                MOVWF       STACK_10
                        DECFSZ      STACK_10, F
                        GOTO $-1
                NOP
                        NOP
PORTB.F3=0;
                BCF     PORTB, 3
Delay_ms(1000);
MOVLW       6
MOVWF       STACK_12
MOVLW       255
MOVWF       STACK_11
MOVLW       255
MOVWF       STACK_10
DECFSZ      STACK_12, F
GOTO $+2
GOTO $+8
DECFSZ      STACK_11, F
GOTO $+2
GOTO $+4
```

```
                DECFSZ      STACK_10, F
            GOTO $-1
                GOTO $-5
            GOTO $-9
                MOVLW       26
            MOVWF       STACK_11
            MOVLW       255
                MOVWF       STACK_10
                DECFSZ      STACK_11, F
GOTO $+2
GOTO $+4
DECFSZ      STACK_10, F
GOTO $-1
GOTO $-5
MOVLW       66
MOVWF       STACK_10
DECFSZ      STACK_10, F
GOTO $-1
            PORTB.F3=1;
                BSF     PORTB, 3
            Delay_ms(1000);
            MOVLW       6
                MOVWF       STACK_12
            MOVLW       255
                MOVWF       STACK_11
            MOVLW       255
            MOVWF       STACK_10
                DECFSZ      STACK_12, F
            GOTO $+2
                GOTO $+8
```

```
                DECFSZ      STACK_11, F
            GOTO $+2
            GOTO $+4
                DECFSZ      STACK_10, F
            GOTO $-1
                GOTO $-5
                GOTO $-9
            MOVLW       26
                MOVWF       STACK_11
                MOVLW       255
            MOVWF       STACK_10
                DECFSZ      STACK_11, F
                GOTO $+2
            GOTO $+4
                DECFSZ      STACK_10, F
            GOTO $-1
                GOTO $-5
            MOVLW       66
                MOVWF       STACK_10
                DECFSZ      STACK_10, F
            GOTO $-1
            PORTB.F3=0;
            BCF    PORTB, 3
            while(1) {
        L_main_0:
;
                MOVLW       1
ANDWF       PORTB, 0
                MOVWF       STACK_1
            MOVF STACK_1, 0
```

```
                XORLW   1
                BTFSS   STATUS, Z
                GOTO L_main_2
        PORTB.F7=1;
    BSF     PORTB, 7
L_main_2:
                MOVLW   0
                BTFSC   PORTA, 1
        MOVLW   1
        MOVWF   STACK_1
        MOVF    STACK_1, 0
        XORLW   0
        BTFSS   STATUS, Z
                GOTO L_main_5
                MOVLW   1
    ANDWF   PORTB, 0
        MOVWF   STACK_1
        MOVF    STACK_1, 0
    XORLW   1
        BTFSS   STATUS, Z
                GOTO L_main_5
L_main_5:
PORTB.F3=0;
BCF     PORTB, 3
PORTA.F2=1;
    BSF     PORTA, 2
    PORTA.F3=1;
        BSF     PORTA, 3
    PORTB.F6=1;
        BSF     PORTB, 6
```

```
Delay_ms(40000);
        MOVLW       204
MOVWF       STACK_12
MOVLW       255
MOVWF       STACK_11
MOVLW       255
MOVWF       STACK_10
        DECFSZ      STACK_12, F
        GOTO $+2
GOTO $+8
        DECFSZ      STACK_11, F
GOTO $+2
GOTO $+4
        DECFSZ      STACK_10, F
GOTO $-1
GOTO $-5
        GOTO $-9
        MOVLW       249
        MOVWF       STACK_11
        MOVLW       255
        MOVWF       STACK_10
        DECFSZ      STACK_11, F
        GOTO $+2
        GOTO $+4
        DECFSZ      STACK_10, F
        GOTO $-1
        GOTO $-5
        MOVLW       212
        MOVWF       STACK_10
        DECFSZ      STACK_10, F
```

```
                GOTO $-1
                NOP
                NOP
        PORTA.F2=0;
                BCF     PORTA, 2
        PORTA.F3=0;
                BCF     PORTA, 3
        PORTB.F6=1;
                BSF     PORTB, 6

                MOVLW       51
MOVWF       STACK_12
                MOVLW       255
                MOVWF       STACK_11
        MOVLW       255
                MOVWF       STACK_10
                DECFSZ      STACK_12, F
                GOTO $+2
                GOTO $+8
                DECFSZ      STACK_11, F
                GOTO $+2
                GOTO $+4
                DECFSZ      STACK_10, F
                GOTO $-1
                GOTO $-5
                GOTO $-9
                MOVLW       253
                MOVWF       STACK_11
                MOVLW       255
                MOVWF       STACK_10
```

```
                DECFSZ      STACK_11, F
                GOTO $+2
                GOTO $+4
                DECFSZ      STACK_10, F
                GOTO $-1
                GOTO $-5
                MOVLW       181
                MOVWF       STACK_10
                DECFSZ      STACK_10, F
                GOTO $-1
                NOP
        PORTB.F6=0;
                BCF    PORTB, 6

L_main_5:

                MOVLW       0
                BTFSC       PORTA, 1
                MOVLW       1
                MOVWF       STACK_1
                MOVF STACK_1, 0
                XORLW       1
                BTFSSSTATUS, Z
GOTO L_main_8
                MOVLW       1
                ANDWF       PORTB, 0
MOVWF       STACK_1
                MOVF STACK_1, 0
        XORLW       0
        BTFSSSTATUS, Z
```

```
                GOTO L_main_8
_L_main_8:
        PORTB.F3=0;
        BCF     PORTB, 3
        PORTB.F7=0;
                BCF     PORTB, 7
        PORTA.F2=0;
                BCF     PORTA, 2
        PORTA.F3=0;
                BCF     PORTA, 3
        PORTB.F6=0;
    BCF     PORTB, 6

main_8:

        MOVLW   1
ANDWF   PORTA, 0
                MOVWF   STACK_1
                MOVF STACK_1, 0
        XORLW   0
        BTFSSSTATUS, Z
                GOTO L_main_11
                MOVLW   0
                BTFSC   PORTA, 1
    MOVLW   1
                MOVWF   STACK_1
MOVF STACK_1, 0
                XORLW   1
                BTFSSSTATUS, Z
                GOTO L_main_11
```

```
L_main_11:
        PORTB.F3=0;
                BCF    PORTB, 3

L_main_11:
                MOVLW      1
        ANDWF      PORTA, 0
                MOVWF      STACK_1
                MOVF STACK_1, 0
                XORLW      1
                BTFSSSTATUS, Z
                GOTO L_main_14
                MOVLW      1
                ANDWF      PORTB, 0
                MOVWF      STACK_1
                MOVF STACK_1, 0
                XORLW      1
                BTFSSSTATUS, Z
                GOTO L_main_14
                MOVLW      0
                BTFSC      PORTA, 1
                MOVLW      1
                MOVWF      STACK_1
                MOVF STACK_1, 0
        XORLW      0
        BTFSSSTATUS, Z
                GOTO L_main_14
L_main_14:
        PORTB.F3=0;
                BCF    PORTB, 3
```

```
L_main_14:

        MOVLW   1
        ANDWF   PORTA, 0
        MOVWF   STACK_1
        MOVF STACK_1, 0
        XORLW   0
        BTFSSSTATUS, Z
        GOTO L_main_17
        MOVLW   1
    ANDWF   PORTB, 0
        MOVWF   STACK_1
        MOVF STACK_1, 0
        XORLW   1
        BTFSSSTATUS, Z
        GOTO L_main_17
        MOVLW   0
        BTFSC   PORTA, 1
        MOVLW   1
        MOVWF   STACK_1
        MOVF STACK_1, 0
        XORLW   0
        BTFSSSTATUS, Z
        GOTO L_main_17
L_main_17:
        PORTB.F3=0;
    PORTB, 3
_main_17:
GOTO L_main_0
End
```

6.3 MATLAB CODES

```
% Data
conditions = {'Daylight', 'LED Indoor', 'Low-Light'};
accuracy = [99.4, 98.9, 98.3];

% Create a bar graph
% Test and Evaluate.
figure;
bar(accuracy);
set(gca, 'XTickLabel', conditions);
title('Accuracy of Detection under Different Lighting Conditions');
xlabel('Condition');
ylabel('Accuracy (%)');
ylim([0 100]);

% Display the accuracy values on top of the bars
% Demonstrate.
%%%%%%%%%%%%%%
for i = 1:length(accuracy)
    text(i, accuracy(i) + 0.5, sprintf('%.1f%%', accuracy(i)), 'HorizontalAlignment',
'center');
end
```

```
% Time parameters
total_time = 60; % Total simulation time in seconds
intrusion_time = 20; % Intrusion occurs at 20 seconds
lock_duration = 15; % Door remains locked for 15 seconds after intrusion

% Time vector
```

```
time = 0:1:total_time; % Time steps (1-second intervals)

% Door status indicator: 1 (Unlocked - Green), 0 (Locked - Red)
door_status = ones(size(time)); % Initially unlocked

% Lock the door after intrusion has been detected
lock_start = intrusion_time;
lock_end = intrusion_time + lock_duration;

for t = 1:length(time)
    if time(t) >= lock_start && time(t) < lock_end
        door_status(t) = 0; % Locked state
    end
end

% Plot the results
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
hold on;
plot(time, door_status, 'g', 'LineWidth', 2, 'DisplayName', 'Door Status');

% Mark intrusion point
xline(intrusion_time, '--r', 'Intrusion Detected', 'LabelVerticalAlignment', 'bottom',
'DisplayName', 'Intrusion Event');
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Point lock duration
xline(lock_end, '--b', 'Lock Released', 'LabelVerticalAlignment', 'bottom', 'DisplayName',
'Lock Released');

% Labels and formatting
```

```
xlabel('Time (seconds)');
ylabel('Door Status (1 = Unlocked, 0 = Locked)');
title('Access Door Status Over Time');
yticks([0 1]);
yticklabels({'Locked', 'Unlocked'});
legend('Location', 'best');
grid on;
hold off;
```

```
% Data
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
conditions = {'Daylight', 'LED Indoor', 'Low-Light'};
A-ccuracy = [99.4, 98.9, 98.3];

% Create a bar graph
% Design a bar
figure;
bar(A-ccuracy);
set(gca, 'XTickLabel', conditions);
title('Accuracy of Detection under Different Lighting Conditions');
xlabel('Condition');
ylabel('Accuracy (%)');
ylim([0 100]);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Display the accuracy values on top of the bars
for i = 1:length(A-ccuracy)
   text(i, A-ccuracy(i) + 0.5, sprintf('%.1f%%', A-ccuracy(i)), 'HorizontalAlignment',
'center');
end
```

```
% MATLAB script to visualize biometric fingerprint authentication accuracy
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%
% Random biometric fingerprint values (1 or below for recognized, >1 for rejected)
n = 100; % Number of authentication attempts
fingerprint_values = [rand(1, 98) * 1, rand(1, 2) * 2 + 1]; % 98% accuracy

% Create x-axis index for visualization
x = 1:n;

% Identify recognized and rejected fingerprints
recognized = fingerprint_values <= 1;
rejected = fingerprint_values > 1;

% %%%%%%%%%%%%%%%%%%%%%%Scatter plot
figure;
scatter(x(recognized), fingerprint_values(recognized), 'b', 'filled'); % Blue for recognized
hold on;
scatter(x(rejected), fingerprint_values(rejected), 'r', 'filled'); % Red for rejected
yline(1, 'k--', 'Threshold (Value = 1)');
hold off;

title('Biometric Fingerprint Authentication Accuracy');
xlabel('Authentication Attempt');
ylabel('Fingerprint Value');
grid on;
legend('Recognized Fingerprints', 'Rejected Fingerprints', 'Threshold');
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
% Simple Alarm Simulation in MATLAB
clc; clear; close all;

% Describe
threshold = 1; % 1 represents unauthorized access

% Simulating sensor input (0 = Safe, 1 = Intruder Detected)
sensor_input = randi([0, 1], 1, 10); % Random sequence of 10 values

% Display sensor input values
disp('Sensor Input Sequence:');
disp(sensor_input);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Sensor
figure;
stem(sensor_input, 'filled', 'r');
hold on;
plot(sensor_input, 'b');
grid on;
xlabel('Time Index');
ylabel('Sensor Input (0 = Safe, 1 = Intruder)');
title('Alarm System Sensor Input Over Time');
hold off;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Condition
for i = 1:length(sensor_input)
    if sensor_input(i) == threshold
        disp(['Alarm Triggered at index ', num2str(i)]);
        beep; % Sound alert
        pause(0.5); % Delay for alarm effect
```

```
    else
        disp(['No threat at index ', num2str(i)]);
    end
    pause(0.5); % Simulating real-time processing
end

disp('Alarm Simulation Complete.');
```

```
clc; clear; close all;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%5
% Delay Vector
t = 1:10; % Simulating 10 fingerprint scans
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
fingerprint_scans = [1 0 1 1 0 0 1 1 0 1];

stored_fingerprints = [1 1 1 1 1 1 1 1 1 1];
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Authentication results (1 = Access Granted, 0 = Access Denied)
auth_result = fingerprint_scans & stored_fingerprints;

% Plot Authentication Graph
figure;
stem(t, auth_result, 'r', 'LineWidth', 2);
hold on;
plot(t, fingerprint_scans, 'b--o', 'LineWidth', 1.5);
legend('Authentication Result', 'Fingerprint Scan Input');
xlabel('Scan Number');
ylabel('Authentication Status');
title('Fingerprint Authentication System Simulation');
```

```
ylim([-0.5, 1.5]);
grid on;
hold off;
```

```
% Generate synthetic data
numSamples = 1000;
contamination = rand(numSamples, 1) * 100; % Contamination (0 to 100)
success = rand(numSamples, 1) < (1 - contamination / 100); % Success (inverse
relationship with contamination)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Calculation
[r, p] = corr(contamination, success); % Calculate Pearson correlation
disp(['Pearson Correlation: ', num2str(r)]); % Display the result
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Regression (using contamination as predictor)
X = [ones(numSamples, 1), contamination]; % Add intercept term
y = success;
%B = mnrfit(X, y, 'binary', 'link', 'logit'); % Logistic regression
%yhat = mnrval(B, X); % Predicted probabilities
%accuracy = mean(yhat >= 0.5) * 100; % Accuracy calculation
%disp(['Logistic Regression Accuracy: ', num2str(accuracy), '%']); % Display accuracy

% Results
figure;
subplot(1, 2, 1);
scatter(contamination, success);
title('Contamination vs. Success');
xlabel('Contamination');
ylabel('Success');
```

```
subplot(1, 2, 2);
scatter(contamination, contamination / 100);
title('Contamination vs. Delay');
xlabel('Contamination');
ylabel('Authentication Delay');
```

```
%TF
num = [1];
den = [1 1];
sys = tf(num, den);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% TV
t = linspace(0, 5, 1000);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% SR
[y, t] = step(sys, t);

% PR
figure;
plot(t, y, 'b', 'LineWidth', 2);
hold on;
yline(1, 'r--', 'Steady-State Activation Level');
grid on;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Labelling
xlabel('Time (seconds)');
ylabel('Activation Level');
title('Biometric Activation Response Over Time');
legend('Biometric Activation Response', 'Steady-State Activation Level');
```

```
% GSD
% SF
numSamples = 1000; % Number of samples

% CL
contamination = rand(numSamples, 1) * 100;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% SD
success = rand(numSamples, 1) < (1 - contamination / 100);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%
% PC
[r, p] = corr(contamination, success);
fprintf('Pearson Correlation Coefficient: %.2f\n', r);
fprintf('p-value for correlation: %.4f\n', p);

% LRM
% C
X = [ones(numSamples, 1), contamination]; % Add intercept term
y = success;

% FL
B = mnrfit(X, y, 'model', 'binary', 'link', 'logit');

% PP
yhat = mnrval(B, X);
```

```
% Accuracy
predictions = yhat >= 0.5; % If probability >= 0.5, predict success
accuracy = sum(predictions == y) / numSamples * 100;
fprintf('Logistic Regression Predictive Accuracy: %.2f%%\n', accuracy);

% SA
auth_delay = contamination / 100; % Assume delays increase with contamination

% DisplDRay results in a plot
figure;

subplot(2,1,1);
scatter(contamination, success, 'b.');
xlabel('Fingerprint Surface Contamination (%)');
ylabel('Successful Identification (0 = Fail, 1 = Success)');
title('Relationship Between Contamination and Success');
grid on;

subplot(2,1,2);
scatter(contamination, auth_delay, 'r.');
xlabel('Fingerprint Surface Contamination (%)');
ylabel('Authentication Delay (Seconds)');
title('Authentication Delay vs. Contamination');
grid on;
```

```
% DTP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%5
predefined_period = 60; % Camera activation threshold (seconds)
```

```
counter = 10; % Counter increase step
leave_times = [30, 60]; % Different leave times to test cases

% TV
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
time = 0:1:100; % Simulating up to 100 seconds
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Int (1 = up, 0 = down)
camera_status = zeros(size(time));

% CC
for leave_time = leave_times
activation_time = leave_time + counter;
for t = 1:length(time)
if time(t) >= activation_time && activation_time > predefined_period
camera_status(t) = 1; % Camera ON
end
end
end

% Plot results
figure;
hold on;
plot(time, camera_status, 'g', 'LineWidth', 2, 'DisplayName', 'Camera Status');

% Mark predefined period threshold
yline(0.5, '--r', 'Predefined Threshold (60s)', 'LabelVerticalAlignment', 'bottom');

% Mark activation events
xline(40, '--b', 'Camera Off', 'DisplayName', 'Camera Remains Off');
```

```
xline(70, '--m', 'Camera On', 'DisplayName', 'Camera Activated');

% Labels and formatting
```

```
% SD
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
time = 0:1:24; % Time in hours (e.g., over a 24-hour period)
tampering_attempts = rand(1, 25) > 0.99; % Random tampering attempts (1 for tampering
detected)
user_presence = rand(1, 25) > 0.1; % Random user presence (1 for user present, 0 for
absent)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% F G
figure;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% PTA
subplot(2, 1, 1);
plot(time, tampering_attempts, 'r', 'LineWidth', 2);
title('Tampering Attempts Detected by the Smart Camera');
xlabel('Time (hours)');
ylabel('Tampering Detected');
ylim([-0.1, 1.1]);
grid on;
hold on;
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% HT
plot(time(tampering_attempts == 1), ones(1, sum(tampering_attempts == 1)), 'bo',
'MarkerFaceColor', 'b');
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% PUP
subplot(2, 1, 2);
plot(time, user_presence, 'g', 'LineWidth', 2);
title('User Presence Around the Mobile Device');
xlabel('Time (hours)');
ylabel('User Presence');
ylim([-0.1, 1.1]);
grid on;
hold on;

% HP
plot(time(user_presence == 0), ones(1, sum(user_presence == 0)), 'ko',
'MarkerFaceColor', 'k');

% DF
sgtitle('Smart Camera Monitoring Results');

% DAT
fprintf('Tampering Detection Accuracy: 99%%\n');
grid on;
hold on;
```

```
% DD
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
camera_delay = 30;   % Camera delay time after the user leaves
lock_delay = 10;     % Lock delay time after intrusion detection
buffer_time = 2;     % Buffer time to account for sensor errors or latency

% SU
leave_time = datetime('now');  % Record the time user leaves
camera_activation_time = leave_time + seconds(camera_delay + buffer_time);

% SI
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
intrusion_time = datetime('now') + seconds(5);  % Intrusion detected 5 seconds later
lock_activation_time = intrusion_time + seconds(lock_delay + buffer_time);

% PCAT
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
hold on;
plot([leave_time, leave_time], [0, 1], 'r', 'LineWidth', 2, 'DisplayName', 'User Leaves');
plot([camera_activation_time, camera_activation_time], [0, 1], 'g', 'LineWidth', 2,
'DisplayName', 'Camera Activated');
plot([leave_time, camera_activation_time], [0.5, 0.5], 'b--', 'LineWidth', 1, 'DisplayName',
'Camera Delay');
title('Camera Activation Timeline');
xlabel('Time');
ylabel('Event');
legend('Location', 'best');
grid on;
```

```
% PLAT
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
hold on;
plot([intrusion_time, intrusion_time], [0, 1], 'r', 'LineWidth', 2, 'DisplayName', 'Intrusion
Detected');
plot([lock_activation_time, lock_activation_time], [0, 1], 'g', 'LineWidth', 2,
'DisplayName', 'Lock Engaged');
plot([intrusion_time, lock_activation_time], [0.5, 0.5], 'b--', 'LineWidth', 1,
'DisplayName', 'Lock Delay');
title('Door Lock Activation Timeline');
xlabel('Time');
ylabel('Event');
legend('Location', 'best');
grid on;
```

```
% Sensor
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% Tests Number
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
n = 100;

% Generate random door status values (0 = closed, 1 = open)
door_status = randi([0 1], 1, n);

% G (0 = not activated, 1 = activated)
biometric_status = randi([0 1], 1, n);
```

```
% Determine buzzer status: buzzer turns on if the door is open and biometric is not
activated
buzzer_status = (door_status == 1) & (biometric_status == 0);

% Create x-axis index for visualization
x = 1:n;

% SP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
scatter(x(door_status == 1), door_status(door_status == 1), 'b', 'filled'); % Blue for door
open (1)
hold on;
scatter(x(door_status == 0), door_status(door_status == 0), 'c', 'filled'); % Cyan for door
closed (0)
scatter(x(buzzer_status == 1), buzzer_status(buzzer_status == 1), 'r', 'filled'); % Red for
buzzer on (1)
hold off;

title('Door Sensor and Buzzer Activation');
xlabel('Test Case');
ylabel('Status');
grid on;
legend('Door Open (Blue: 1)', 'Door Closed (Cyan: 0)', 'Buzzer On (Red: 1)');
```

```
% MATLAB Code

% PP
authorized_user_detected = 1; % 1 if authorized user is detected, 0 otherwise
```

```
unauthorized_intrusion_detected = 0; % 1 if intrusion is detected, 0 otherwise
response_time_threshold = 5; % seconds for alarm trigger time

% SS
time = 0:0.1:20; % Time vector for 20 seconds simulation
alarm_state = zeros(size(time)); % Initial alarm state (0 = off, 1 = on)

% SSR
for t = 1:length(time)
    if authorized_user_detected
        alarm_state(t) = 0; % No alarm if authorized user
    end
end

% SSR
for t = 1:length(time)
    if unauthorized_intrusion_detected
        alarm_state(t) = 1; % Alarm triggered if unauthorized user
    end
end

% PTR
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
plot(time, alarm_state, 'r', 'LineWidth', 2);
xlabel('Time (seconds)');
ylabel('Alarm State');
title('System Response to Authorized vs Unauthorized User');
legend('Alarm Triggered');
grid on;
```

```
% OF
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Observed_PMU = [13, 11, 6];
Observed_SecurityOffice = [14, 9, 7];

% EFFF
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Expected = [15, 10, 5];
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% PMU
chi_PMU = sum((Observed_PMU - Expected).^2 ./ Expected);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Security Office
chi_SecurityOffice = sum((Observed_SecurityOffice - Expected).^2 ./ Expected);

% DF = (categories - 1)
df = length(Expected) - 1;

% alpha = 0.05, df = 2
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
critical_val = chi2inv(0.95, df);

% DR
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
fprintf('PMU Chi-square = %.2f\n', chi_PMU);
fprintf('Security Office Chi-square = %.2f\n', chi_SecurityOffice);
fprintf('Critical Chi-square value (0.05, df=2) = %.2f\n', critical_val);
```

```
if chi_PMU < critical_val
    fprintf('PMU: No significant deviation. System performance is consistent with
expected.\n');
else
    fprintf('PMU: Significant deviation. System may need review.\n');
end

if chi_SecurityOffice < critical_val
    fprintf('Security Office: No significant deviation. System performance is consistent
with expected.\n');
else
    fprintf('Security Office: Significant deviation. System may need review.\n');
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Plotting the graph
categories = {'Category 1', 'Category 2', 'Category 3'};

% Create bar graph
figure;
hold on;

%
bar(1:3, [Observed_PMU; Observed_SecurityOffice]', 'grouped');
set(gca, 'XTickLabel', categories);
xlabel('Categories');
ylabel('Frequency');
title('Observed vs Expected Frequencies');
legend({'PMU Observed', 'Security Office Observed'}, 'Location', 'northeast');

%
```

```
plot(1:3, Expected, '-o', 'LineWidth', 2, 'MarkerSize', 8, 'MarkerEdgeColor', 'k', 'Color',
'r');

%
text(1, max(max(Observed_PMU, Observed_SecurityOffice)) + 1, sprintf('PMU Chi-
square: %.2f', chi_PMU), 'FontSize', 12, 'Color', 'b');
text(2, max(max(Observed_PMU, Observed_SecurityOffice)) + 1, sprintf('Security
Office Chi-square: %.2f', chi_SecurityOffice), 'FontSize', 12, 'Color', 'b');
text(3, max(max(Observed_PMU, Observed_SecurityOffice)) + 1, sprintf('Critical Chi-
square: %.2f', critical_val), 'FontSize', 12, 'Color', 'r');

hold off;
```

```
% PP

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
laptop_present = false;  % Initial state of the laptop (false = not present)
fingerprint_registered = true;  % Assuming the user is authorized (true = registered)
switch_status = 0;  % Limit switch status (0 = Low, 1 = High)
siren_status = 0;  % Siren status (0 = off, 1 = on)
lock_status = 0;  % Lock status (0 = unlocked, 1 = locked)
laptop_withdrawn = false;  % Flag to track if the laptop is withdrawn

% TP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
t = 0:0.1:10;  % Time vector from 0 to 10 seconds with 0.1 second interval
```

```
switch_status_vals = [];  % To store the status of the limit switch over time
siren_vals = [];  % To store siren status over time
lock_vals = [];  % To store lock status over time

for i = 1:length(t)

    if rand() > 0.01  % 99% accuracy for detection
        laptop_present = true;  % Laptop is detected
        switch_status = 1;  % Switch activates (High)
    else
        laptop_present = false;  % Laptop not detected
        switch_status = 0;  % Switch resets (Low)
    end

    % When the laptop is withdrawn
    if laptop_present == false && laptop_withdrawn == false
        % Check if security system is activated
        if fingerprint_registered
            siren_status = 0;  % No alarm for authorized user
            lock_status = 1;   % Lock the smart lock
        else
            siren_status = 1;  % Activate siren if unauthorized user
            lock_status = 1;   % Lock the smart lock
        end
        laptop_withdrawn = true;  % Mark the laptop as withdrawn
    elseif laptop_present == true && laptop_withdrawn == true
        % Reset system once the laptop is placed back
        siren_status = 0;  % Reset siren
        lock_status = 0;   % Unlock the smart lock
```

```
        laptop_withdrawn = false;  % Mark the laptop as placed back
    end

    switch_status_vals = [switch_status_vals, switch_status];
    siren_vals = [siren_vals, siren_status];
    lock_vals = [lock_vals, lock_status];
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

figure;
subplot(3,1,1);
plot(t, switch_status_vals, 'bo-', 'LineWidth', 2);
title('Limit Switch Status');
xlabel('Time (s)');
ylabel('Switch Status (0=Low, 1=High)');

subplot(3,1,2);
plot(t, siren_vals, 'ro-', 'LineWidth', 2);
title('Siren Status');
xlabel('Time (s)');
ylabel('Siren Status (0=Off, 1=On)');

subplot(3,1,3);
plot(t, lock_vals, 'go-', 'LineWidth', 2);
title('Lock Status');
xlabel('Time (s)');
ylabel('Lock Status (0=Unlocked, 1=Locked)')
```

```matlab
% DTP
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
T_Intrusion = [0, 1]; % Intrusion event at 0s and 1s
T_Period = 0; % Predefined time set in microcontroller

% Compute Relay Status
T_Relay_on = T_Intrusion + T_Period; % Relay turns ON when intrusion occurs
T_Relay_off = 0; % Relay OFF initially

% DTV
time = 0:1:5;

% Initialize relay status (1 = ON, 0 = OFF)
relay_status = zeros(size(time));

% Update relay status based on intrusion event
for t = 1:length(time)
   if time(t) >= T_Relay_on(2) % Relay turns on at T_Intrusion = 1
      relay_status(t) = 1; % Relay ON
   end
end

% PRVA
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
figure;
hold on;
plot(time, relay_status, 'g', 'LineWidth', 2, 'DisplayName', 'Relay Status');

% Mark the intrusion event
xline(1, '--r', 'Intrusion Occurred (1s)', 'LabelVerticalAlignment', 'bottom');
```

```
% Mark relay activation time
xline(T_Relay_on(2), '--b', 'Relay ON (1s)', 'DisplayName', 'Relay Activated');

% Labels and formatting
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
xlabel('Time (seconds)');
ylabel('Relay Status (1 = ON, 0 = OFF)');
title('Relay Activation Based on Intrusion Event');
yticks([0 1]);
yticklabels({'OFF', 'ON'});
legend('Location', 'best');
grid on;
hold off;
```

Central University of Technology, Free State

6.4 EDITING CERTIFICATE

NERESHNEE GOVENDER COMMUNICATIONS (PTY) LTD

REGISTRATION NUMBER: 2016/369223/07
DR NERESHNEE GOVENDER (PhD)
neresh@ngcommunications.co.za
0847022553
WRITING PRACTITIONER • EDITOR • COPYWRITER • TRAINER

PhD-Management Sciences: Marketing (gender and media); *PG DIP - Higher Education - Academic Developers (Cum laude;)* M-Tech Public Relations; B-Tech Public Relations *(Cum laude);* B-Tech Journalism *(Cum laude); N-Dip Journalism*

27/05/2025

Thabiso John Matsemela
Central University of Technology
Supervisor: Prof ED Markus

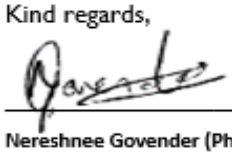
RE: EDITING CERTIFICATE

TITLE: A HYBRID EARLY WARNING SYSTEM FOR THE PREVENTION OF MOBILE ASSET THEFT: CASE OF LAPTOPS IN SOUTH AFRICAN GOVERNMENT BUILDINGS

Dissertation submitted in fulfilment of the requirements for the degree MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING in the Department of Electrical, Electronic and Computer Engineering Faculty of Engineering, Built Environment and Information Technology at the Central University of Technology, Free State, Bloemfontein.

This serves to confirm that this journal article has been edited for clarity, language and layout.

Kind regards,



Nereshnee Govender (PhD)