Smart IoT-Based Intrusion Detection System for Power & Telecommunications Infrastructure Using LoRa and Active Deterrents

Martha Tafadzwa Musendo[1], Silence Thomas Madondo[2], Sam Masunda[3]

Abstract

This paper presents the design and evaluation of a Smart IoT-based Intrusion Detection System (IDS) for critical power and telecommunications infrastructure. The system is based on a rule-based event-driven intrusion detection algorithm, where sensor-triggered events are processed using predefined thresholds and decision logic to classify intrusion states and activate appropriate deterrent responses. The IDS integrates motion sensors, floodlights, deterrent pumps, and LoRa radio modules with a secure web-based monitoring platform to provide real-time alerts and remote oversight. Prototype testing demonstrated an average alert delivery time of 2.6 seconds, a 95% intrusion detection accuracy, and a 70% reduction in false alarms compared to conventional alarm systems. The system further projects potential monthly savings of US$9,000 through reduced equipment loss and downtime. LoRa technology is employed for long-range, low-power communication, while a layered security framework combining detection, deterrence, and alerting is used to prevent intrusions before theft occurs. These findings indicate that the proposed IDS prototype effectively addresses key limitations of existing security measures, enhances operational efficiency, and, if implemented at scale, could significantly reduce financial losses in the telecommunications sector. This work represents a practical step toward safeguarding power and telecommunications infrastructure in Zimbabwe and improving service reliability.

Keywords: IoT; Intrusion Detection System; LoRa; Anti-vandalism Systems; Remote monitoring; Smart Surveillance

[1] *Electronics and Telecommunications University of Zimbabwe Harare, Zimbabwe*
[2] *Electronics and Telecommunications University of Zimbabwe Harare, Zimbabwe*
[3] *Electronics and Telecommunications University of Zimbabwe Harare, Zimbabwe*

1. INTRODUCTION

1.1 BACKGROUND

The rapid expansion of mobile telecommunications network services has transformed how we communicate and access information. Their security and reliability are paramount. In Zimbabwe, the mobile industry contributes over 50% to the country's economy (Chigwende and Govender, 2020). The government aims to raise mobile penetration from 94.2% to 100% by 2025 (Ndlovu, 2024). In that regard, base stations have a strategic importance because they form the backbone of telecommunications networks. However, these sites face escalating security threats, particularly theft and vandalism of fuel, batteries, generators, and copper cables.

Historical data indicates a trend of theft incidents in the Zimbabwean telecommunications sector. This includes a 2012 case involving the theft of 1,400 litres of fuel and a generator (Newsday, 2012), as well as numerous break-ins reported in 2021 (Safeguard, 2021). Between January and March 2022, ZESA experienced more than 500 incidents of vandalism and theft, nearly half of the 1,200 cases recorded in 2021 (Masarakufa, 2023). In the first quarter of the year 2024, US22,500 worth of electricity infrastructure was lost due to theft and vandalism in the Midlands province (Tshili and Chitumba, 2024). Losses have been significant, NetOne lost around US$30,000 in 2023 (NewsDay, 2023), TelOne approximately US$600,000 (P and Kwashirai, 2021). Nationally, vandalism costs Zimbabwe roughly US$5 million annually.

Despite implementing various security measures such as locked cabinets, perimeter fencing, and security personnel, these have proven inadequate. Security guards have proven effective in some situations; however, criminals often overpower guards, sometimes use weapons, and thefts frequently occur before any response can be mounted (Newsday, 2012). Alarm systems that trigger when cabinets are opened are widely used but suffer from limitations, including delayed response times, false alarms, and the inability to prevent theft proactively. These weaknesses result in costly service disruptions, financial losses, increased downtime, and higher maintenance and security costs.

The telecommunications and power sectors face persistent theft and vandalism at critical infrastructure sites, targeting valuable equipment, fuel, generators, lithium batteries, and transformers. These incidents cause frequent service disruptions, longer mean time to repair (MTTR), and rising maintenance costs, severely affecting network availability (a key performance indicator) and operational efficiency. Existing security measures, such as perimeter fencing, locked cabinets, and security personnel, have proven inadequate in deterring intrusions.

Given these challenges, implementing an effective IDS is essential for telecommunications and power companies. An effective IDS would continuously monitor for unauthorized activity, enable real-time alerts, and integrate deterrent mechanisms such as lights and alarms to prevent theft before it occurs. It continuously monitors the system for abnormal patterns or malicious behaviour, enables remote oversight, and acts as a deterrent by discouraging attempts at unauthorized access.

1.2 AIM OF STUDY

This study aims to develop an IoT-based monitoring and security system to detect unauthorized access, deter theft, and minimize financial losses, and ensure uninterrupted service delivery.

1.3 RESEARCH OBJECTIVES

i. To design a system that automatically detects and deter intrusions, and alert security personnel for a prompt response to potential threats.
ii. To evaluate the effectiveness of active deterrent mechanisms in reducing intrusion attempts.
iii. To assess the reliability and suitability of LoRa communication for remote infrastructure monitoring.
iv. To determine a cost-effective hardware configuration suitable for large-scale deployment.

2. LITERATURE REVIEW

2.1 PREVIOUS STUDIES

The growing dependence on telecommunications infrastructure has amplified the need for secure and efficient base station operations. Studies have developed systems to address vulnerabilities such as fuel theft, battery security, and access control. This literature review analyses the background and methodologies of these systems.

Antem and Ebong, (2018) developed an automated fuel monitoring system using a web interface and USSD technology to detect fuel discrepancies, reducing fraud but lacking intruder identification. Similarly, Sathish *et al.*, (2020) introduced a GSM-based battery protection system with real-time SMS alerts and audible alarms, effective even during power outages but limited by GSM connectivity.

Karawita, Dhammearatchi and De Silva, (2020) proposed a microcontroller-based access control system using Raspberry Pi cameras to verify visitors via SMS and image matching, triggering alarms and emailing images of unauthorized access. This proactive model improved monitoring but still depended solely on GSM networks.

IoT integration became more prominent in later work. Ranjith and Saibaba, (2022) designed a Raspberry Pi-based system combining cameras and sensors for temperature, smoke, and voltage monitoring, providing real-time video streaming and alerts via GSM. Although comprehensive, this solution was costly and power-dependent.

Denis Mbowoh and Eric Bewor, (2023) focused on generator fuel and battery level monitoring using microcontroller-based IoT solutions, issuing SMS alerts when thresholds were breached. Liu, (2023) advanced the field by introducing AI-driven wireless base station monitoring, offering real-time data processing and reporting but requiring stable internet connectivity.

Balakrishnan and Murugan, (2024) developed a smart anti-theft system using NodeMCU, ultrasonic sensors, and ESP32 cameras to capture intruder images, providing evidence for investigations. The methodology involved assessing security needs to identify vulnerabilities, which informed the design phase for selecting appropriate sensors and cameras, ensuring a comprehensive and effective monitoring strategy. While effective, it raised privacy concerns and relied heavily on internet access.

Across these studies, a clear pattern emerges, the integration of technology whether through GSM modules, IoT sensors, or microcontrollers serves as a fundamental solution to the vulnerabilities faced by telecommunications infrastructure. While each system presents unique methodologies tailored to specific challenges, the goal remains consistent, enhancing security, preventing theft, and ensuring operational efficiency in an increasingly technology-driven environment.

2.2 ANALYSIS OF PREVIOUS STUDIES

Table 1: Comparison of existing systems from literature

Author(s)	Technology/Method	Strengths	Weaknesses	Gap Addressed by New System
Ebong (2018)	Web + USSD fuel monitoring	Detects discrepancies in fuel usage	Cannot identify intruders; vulnerable to fuel contamination; no deterrents	New system integrates motion sensors + cameras + deterrent spray to both detect and prevent theft
Sathish et al. (2020)	GSM + Arduino battery protection	Real-time SMS alerts; works during power cuts	GSM dependency; fails during poor connectivity; no deterrence	New system uses LoRa + Twilio for reliable communication
Karawita et al. (2020)	Microcontroller + Raspberry Pi camera	Captures intruder images; access control	Relies solely on GSM; prone to network outages; no active prevention	New system integrates LoRa fallback and deterrents (lights + spray) for proactive intrusion response
Ranjith & Saibaba (2022)	Raspberry Pi + IP camera + sensors	Remote monitoring;	High setup costs; internet and power dependency	New system uses low-cost ESP32 + LoRa for

		multi-parameter detection		affordable scalability in Zimbabwe
Mbowoh & Bewor (2023)	IoT-based GSM fuel & battery monitoring	Real-time alerts for low levels	No surveillance capability; GSM only; cannot deter theft	New system integrates video surveillance, deterrents, and dual communication for stronger security
Liu (2023)	AI-based wireless monitoring system	Real-time AI analysis; centralized reporting	Requires stable internet; costly to implement at scale	New system offers cost-effective LoRa + cloud storage instead of expensive AI-only frameworks
Balakrishnan & Murugan (2024)	IoT (NodeMCU, ultrasonic, ESP32 camera)	Captures intruders; stores images	Internet dependency; raises privacy concerns; no active deterrents	New system integrates cloud storage + non-lethal deterrents for compliance

Existing systems demonstrate useful features but often fall short of providing a holistic, reliable solution. GSM-based systems fail during network disruptions, while fuel monitoring solutions cannot identify perpetrators. Camera-based access control systems offer real-time monitoring but lack deterrent mechanisms. High costs and dependence on power and internet connectivity limit the scalability of many solutions.

The proposed system builds upon these works by integrating advanced technologies such as motion sensors, surveillance cameras, LoRa communication, a cloud storage and a web application, the new system aims to overcome the limitations present in previous studies. This approach not only enhances the detection and response to intrusions but also ensures effective management of critical security data for ongoing assessments, ultimately providing a more secure and efficient solution for telecommunications base station monitoring. These findings are consistent with recent LPWAN performance reviews, which identify LoRaWAN as a cost-effective and energy-efficient technology capable of supporting long-range communication in infrastructure monitoring applications, particularly in environments with limited connectivity (Judvaitis *et al.*, 2025).

3. METHODOLOGY

This section outlines the design, components, and operational flow of the proposed IoT-based IDS. The methodology integrates hardware, software, and communication modules to achieve a robust, reliable, and cost-effective security solution.

3.1 HARDWARE AND SOFTWARE TOOLS

Table 2: Hardware tools used in the prototype

Component	Role in Prototype	Key Specifications / Notes
PIR Motion Sensors	Detect infrared radiation from moving bodies (humans/animals) to trigger intrusion alerts.	• Operating Voltage: 3–5V DC (some up to 12V) • Detection Range: 3–10 m • Detection Angle: ~100–140° • Adjustable sensitivity, low power consumption, environmental factors, potential false triggers
Surveillance Cameras	Cameras simulate real-time monitoring and intrusion documentation.	• Resolution: 720P • Supports Wi-Fi streaming
Alarm Systems (Buzzer)	Provides loud audible alerts to demonstrate intrusion detection.	• Sound level: ≥85 dB
Alarm Systems (Strobe Light)	Provides bright flashing visual alerts during an intrusion, useful at night or in noisy environments.	• High-intensity LED, ≥1 W power • Flash frequency: 1–2 Hz
Central Monitoring Unit	Processes signals from prototype sensors and cameras.	• ESP32-based hub

Power Supply	Converts electric current to the required voltage for prototype devices.	• 220V AC to 5V/12V DC regulated
ESP32 Microcontroller	Automates prototype operations and integrates communication modules.	• Dual-core 32-bit MCU • Wi-Fi + Bluetooth
LoRa Transmitter/Receiver	Provides simulated long-range communication between nodes.	• Range: up to 10 km

Table 3: Software tools used in the prototype

Software Tool	Role in Prototype	Details
Web Application	Demonstrates real-time monitoring, notifications, and remote system access.	Accessible via secure login
Twilio SMS API	Sends free SMS alerts to designated security personnel during tests.	Cloud-based SMS service, replacing the GSM module
Mobile Application (OTP Authentication)	Provides secure system access by requiring one-time password (OTP) verification.	Used by security personnel to enter OTPs received via SMS, ensuring only authorized users access the system.
Programming Languages	Used for developing and integrating prototype functions.	- C++: sensor + hardware programming - PHP: front-end & API communication - MySQL: manages logs & user data

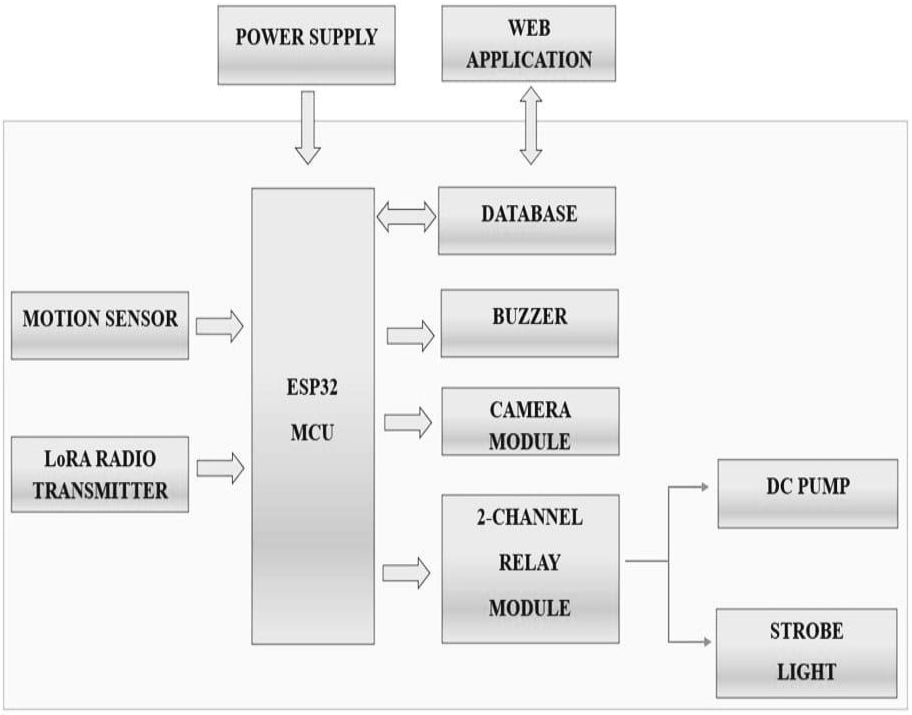

Figure 1: System Block diagram

3.2 SYSTEM DESIGN AND IMPLEMENTATION

Proteus System Circuit Design (Schematic)

After simulating the circuit diagram, the PCB layout was designed in Proteus software, which efficiently drew circuit tracks and marked connections. The software was easy to install and use, allowing quick modifications to component footprints and saving significant time compared to manual drawing.

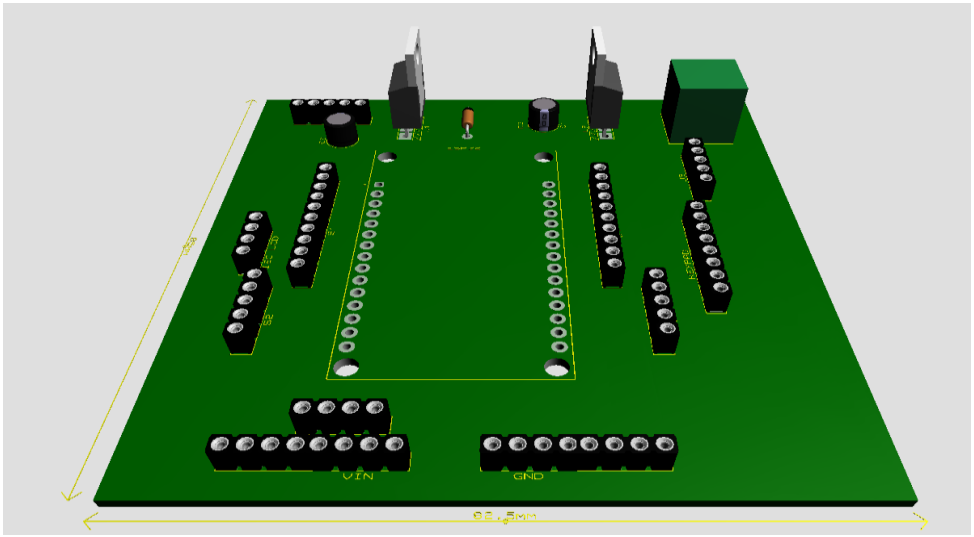

Figure 2: 3D view of PCB layout

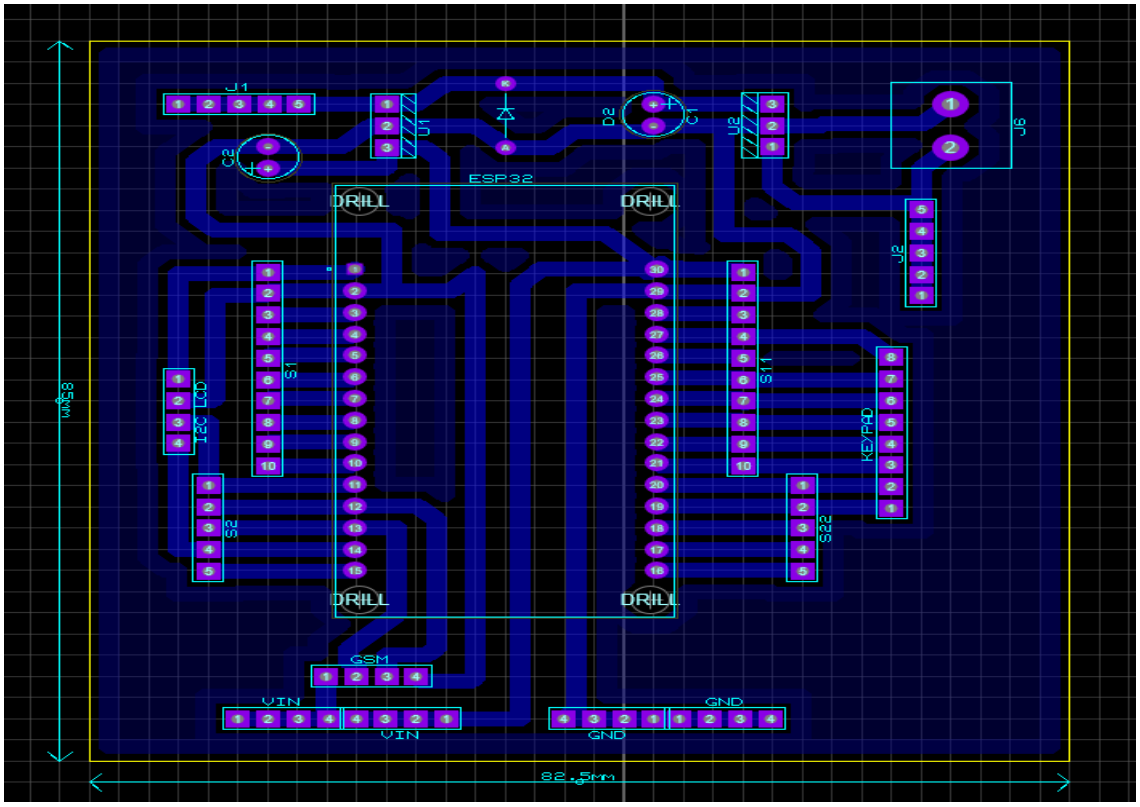

Figure 3: LoRA transmitter PCB layout

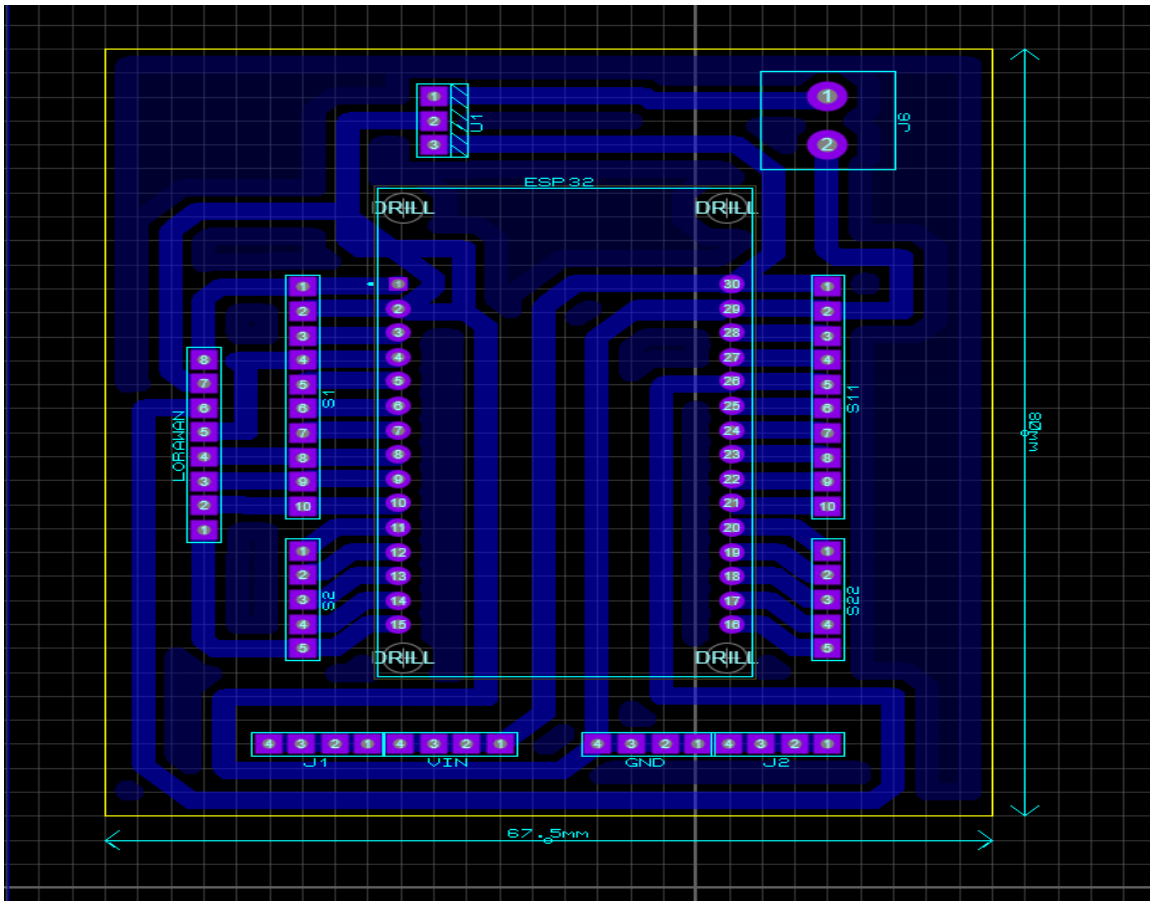

Figure 4: LoRA receiver PCB layout

Website programming

HTML was used to create a layout for live video streams, system status indicators, and alerts, utilizing tags and CSS Flexbox or Grid for responsiveness. HTML forms enabled user interactions like arming alarms and adjusting camera angles, while multimedia elements like <video> and <canvas> displayed live data. Media queries ensured the application is accessible on various devices. Although HTML does not handle data security, the application implements HTTPS to encrypt data and uses secure login forms for user authentication, protecting sensitive information and ensuring authorized access.

Surveillance system

The webcam monitored activities, detected motion, and provided remote access to live feeds, enabling rapid response to threats. It captured images and recorded video continuously, on a schedule, or upon motion detection, with footage uploaded for storage. The monitored area was divided into three virtual zones: a strobe light was activated in the outermost zone, a buzzer in the intermediate zone, and pepper spray in the innermost zone closest to the protected equipment.

Face Recognition

Face recognition detected and prevented unauthorized entry by capturing images of individuals attempting to access the secure base station area and comparing them with a database of authorized personnel. Alerts were alerted when an unauthorized individual was detected.

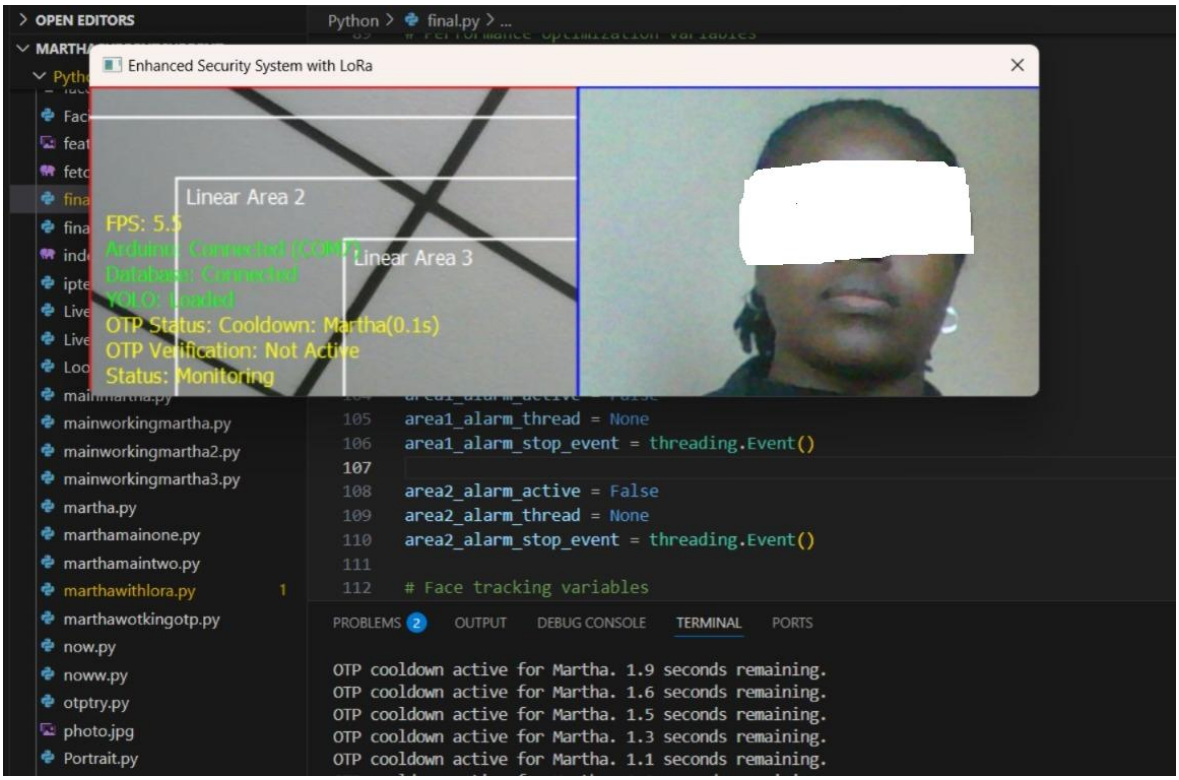

Figure 5: Facial recognition identifies Martha

3.3 SYSTEM OPERATION

The system flow chart is as shown below:

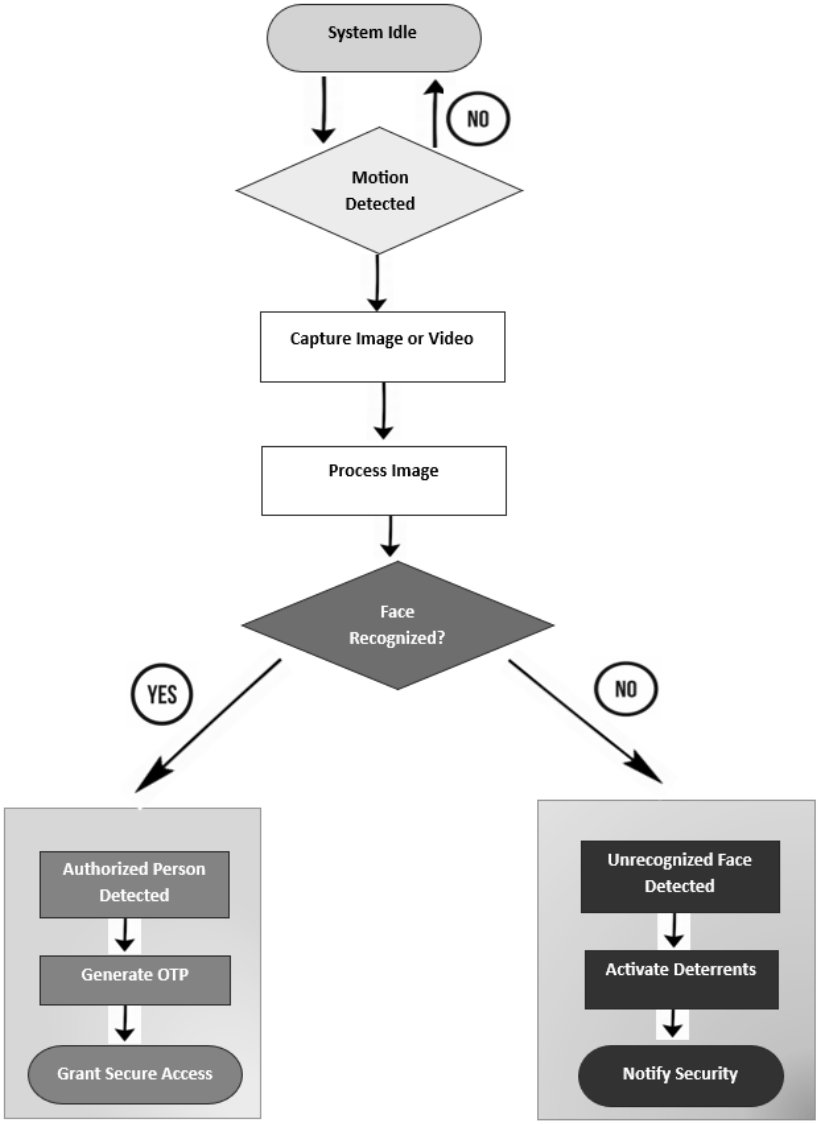

Figure 6: System flow chart

The system operation begins with authorized access, where users are verified through facial recognition. If a user is authorized, the system generates a one-time password (OTP) for further authentication. Users must enter this OTP to complete the access process. Once authentication is successful, the system deactivates the sensors and deterrents and logs user activity for future reference.

When an intruder is detected, the system responds based on proximity. Initially, strobe lights are activated to deter the intruder, followed by a buzzer that alerts security personnel. If the intruder gets very close, pepper spray is deployed for immediate deterrence. This multi-layered response aims to prevent unauthorized access effectively.

In terms of data handling, video footage of any intrusion is regularly saved to the storage device for evidence collection and analysis. The system is equipped with effective security features, including two-factor authentication, which secures remote access through the use of OTPs, ensuring that only authorized users can access the system.

Additionally, the system sends immediate alerts to security personnel if unauthorized access is attempted, enabling a quick response to potential threats. This operation flow enhances monitoring and response capabilities, significantly improving overall security.

4. FINDINGS AND RESULTS

This section presents the simulation and testing methods used to evaluate the design's viability, functionality, and performance. It includes an analysis of results to determine how effectively the design meets project objectives and addresses the identified gaps in earlier systems.

4.1 SOFTWARE EVALUATION

The evaluation of the web-based application involved assessing user experience, functionality, security, scalability, and maintainability. Regular assessments throughout the development process identified areas of improvement, ensuring the application remained aligned to the desired goals.

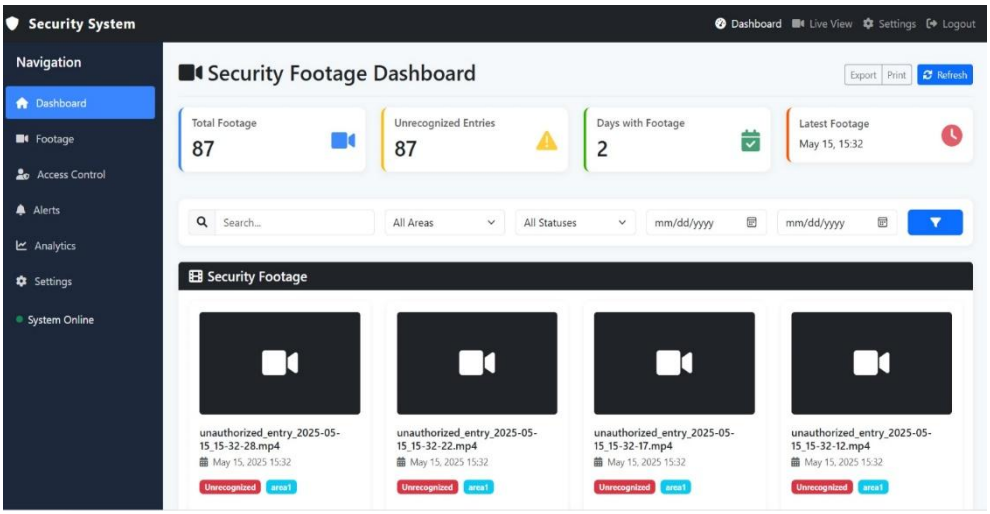

Figure 7: Website frontend

The web application serves as the central monitoring interface for control room operators. It was evaluated for overall user experience, responsiveness, visual consistency, and security. Its interface proved intuitive and easy to navigate, enabling operators to access camera feeds, alerts, and logs with minimal clicks, thereby reducing response times during incidents. The layout maintained consistent functionality and clarity across desktop, tablet, and mobile devices, while colour schemes, typography, and icons were visually coherent, allowing quick interpretation of system status. Additionally, secure login mechanisms, including role-based access control and encrypted session management, were successfully implemented to prevent unauthorized system manipulation.

The mobile application successfully generated and entered a One-Time Pin (OTP) following the completion of the facial recognition process. Upon successful face authentication, the OTP was sent to the authorized user's mobile device to complete the authentication process. Additional functionalities, such as a backup OTP request option and a user activity logging section, were also successfully implemented.

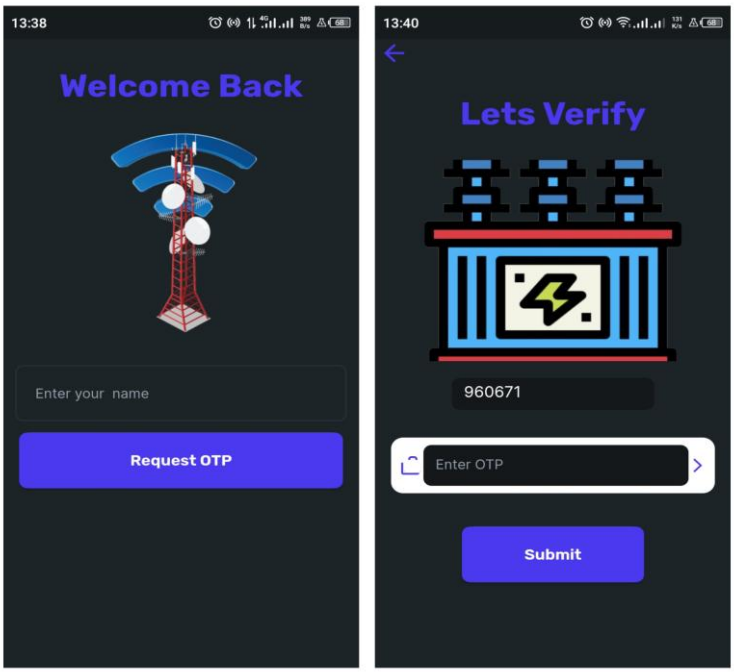

Figure 8: Mobile Application screenshots

4.2 HARDWARE EVALUATION

The motion sensor prototype was evaluated at varying distances to determine its effective detection range. Table 4 provides a breakdown of each intrusion attempt, including estimated distances, detection outcomes, and false positives. Within the nominal 5 m range, the sensor reliably detected intrusions, with only one missed detection occurring at the maximum distance of 5 m. Beyond 5 m, detection performance declined, with several intrusions missed between 5.5 m and 7.5 m, indicating reduced sensitivity at longer distances. Overall, the sensor achieved a 90% detection rate within 5 m and a 60% detection rate beyond 5 m. Considering a 95% confidence interval for these binomial proportions, the results demonstrate that the sensor performs reliably at close range, but placement is critical to maintain coverage in larger areas.

Table 4: Motion sensor prototype test results

Attempt	Distance (meters)	Intrusion Detected?	False Positive?
1	1.5	Yes	No
2	2.5	Yes	No
3	3.2	Yes	No
4	3.5	Yes	No
5	4.0	Yes	No
6	4.2	Yes	No
7	4.5	Yes	No
8	4.8	Yes	No
9	5.0	Yes	No
10	5.0	No	Yes
11	5.2	Yes	No
12	5.5	No	Yes
13	5.8	Yes	No
14	6.0	No	Yes
15	6.3	No	No
16	6.5	Yes	No
17	6.7	No	Yes
18	7.0	Yes	No
19	7.2	No	No
20	7.5	Yes	No

Floodlights provided enhanced visibility and deterrence upon motion detection. The system successfully integrated a relay to activate the strobe light, which was chosen for its high brightness and durability in harsh conditions.

The DC pump served as an actuator to deter intruders. Upon receiving a signal from the motion sensor, the microcontroller activated the pump to spray a deterrent fluid, effectively discouraging unauthorized access.

LoRa communication was evaluated with 10 transmission attempts across line-of-sight (LOS) and non-line-of-sight (NLOS) conditions. Table 5 details each attempt, including distance, packet success, and observed issues. In LOS conditions, packets were reliably transmitted up to 1800m, with minor delays near the maximum distance. In NLOS conditions, with obstructions such as walls or equipment, the most reliable range dropped to approximately 800m, with occasional packet loss. These results demonstrate that LoRa provides low-power, reliable data transmission in a field environment, with performance affected by distance and line-of-sight obstructions. Similar findings were reported by Chapungo and Nelson José, (2025) who demonstrated that LoRa WAN maintains high packet delivery reliability in rural field deployments, with terrain and physical obstructions being the primary factors influencing communication range.

Table 5: Lora module field test results

Attempt	Test Condition	Distance (meters)	Packet Received?	Notes
1	Line-of-Sight	800	Yes	Stable signal
2	Line-of-Sight	1000	Yes	Stable signal
3	Line-of-Sight	1200	Yes	Stable signal
4	Line-of-Sight	1500	Yes	Minor delay
5	Line-of-Sight	1800	Yes	Maximum reliable distance
6	Non-Line-of-Sight, obstructed	800	Yes	Minor signal attenuation
7	Non-Line-of-Sight, obstructed	1000	Yes	Minor packet delay
8	Non-Line-of-Sight, obstructed	1200	Yes	Occasional packet loss
9	Non-Line-of-Sight, obstructed	1300	No	Maximum reliable NLOS distance
10	Non-Line-of-Sight, obstructed	1500	Yes	Packet loss due to obstruction

The alert delivery system was evaluated by measuring the time required for notifications to reach security personnel. Ten tests were conducted, five using the Twilio Short Message Service and five using the LoRa channel. Table 6 presents the delivery time for each attempt. Twilio alerts were received within 2.6 to 3.1 seconds, with an average of 2.9 seconds, while LoRa alerts were received within 1.5 to 2.2 seconds, averaging 1.9 seconds. The results indicate that both channels deliver alerts effectively, with LoRa providing faster notification.

Table 6: Alerts delivery performance comparison

Attempt	Communication Channel	Time to Deliver Alert (seconds)	Notes
1	Twilio (Short Message Service)	2.6	Minimum observed time
2	Twilio (Short Message Service)	2.7	
3	Twilio (Short Message Service)	2.8	
4	Twilio (Short Message Service)	3.0	
5	Twilio (Short Message Service)	3.1	Maximum observed time
6	LoRa	1.5	Minimum observed time
7	LoRa	1.7	
8	LoRa	1.8	
9	LoRa	2.0	
10	LoRa	2.2	Maximum observed time

5. DISCUSSION

The results presented in this section reflect prototype-level testing under controlled conditions. While the findings validate the feasibility of the design, industrial deployment would require the use of higher-grade hardware and extended field testing to ensure performance under real-world operational conditions.

The study demonstrates that the designed security system effectively enhances security through a robust integration of hardware and software for real-time surveillance. The motion sensor reliably detects intruders while filtering out false alarms, reducing alarm fatigue for security personnel. The web-based application provides user-friendly access to surveillance data across various devices, and security features such as OTP for remote access protect against unauthorized manipulation.

Additionally, LoRa technology enables long-range communication with low power consumption, ensuring accurate updates on motion status and GPS location even in areas with poor connectivity. Deterrent measures, such as floodlights and a DC pump for spraying a deterrent fluid, further enhance security by preventing potential incidents. Overall, the findings indicate that this system effectively addresses current challenges and represents a significant advancement in base station security solutions.

Table7: Prototype performance summary across hardware and software components

Component	Test Conditions	Prototype Performance Results	Notes / Limitations
PIR Motion Sensor	• 5 m range • 120° field of view	• 90% detection rate • 10% false positives	Reliable at close range; occasional environmental triggers
Strobe Light	Day vs Night conditions	• Visible up to 20 m at night, 10 m in daylight • Flash frequency: 1–2 Hz	Effective visual deterrent but limited daytime visibility
Buzzer	Indoor/outdoor environment	Loud alert at ≥85 dB	Suitable for short-range alerting only
DC Pump	Spraying deterrent liquid	• Achieved 2–3 m spray radius • Flow adequate for short bursts	Limited coverage; suitable only for close-range deterrence
Camera module	Day, night, and cloudy conditions	• Daytime: Clear images up to 7m • Cloudy: Moderate degradation • Night: Poor clarity without extra lighting	Prototype suitable for testing, but lacks night vision
LoRa Radio Module	Semi-urban field tests	Line-of-sight: Stable up to 1.8 km (95% packet delivery) Non-line-of-sight: Reliable up to 800 m (85%)	Range limited by obstructions; results consistent with LoRa technical specifications
Web App + Twilio SMS	Internet-connected environment	Real-time monitoring worked; SMS alerts delivered successfully to test numbers	Dependent on internet access for Twilio service

6. CONCLUSION AND RECOMMENDATIONS

6.1 CONCLUSION

The development of an effective IDS is crucial as it minimize financial losses associated with replacing stolen equipment for telecommunications and power companies. The proposed IoT-based IDS successfully detects, deters, and reports intrusion attempts in real-time. By integrating LoRa communication, deterrent devices, and a secure monitoring platform, it significantly improves

infrastructure security and operational reliability. This solution has strong potential for large-scale deployment by telecom operators seeking to minimize losses and downtime.

6.2 RECOMMENDATIONS

In order to enhance the effectiveness of this Intrusion Detection system the following improvements can be considered:

- Use of more sensors to detect motion

To improve the effectiveness of the Intrusion Detection system more sensors can be incorporated to detect motion. These sensors include infrared sensors that detect infrared radiation emitted by moving objects such as humans and microwave sensors that emit microwave signals and detects changes in the reflected signal.

- Use of fibre optic perimeter sensors

Fiber optic cables can be laid along the perimeter fence of the base station. This will provide uninterrupted and consistent monitoring of the base station area. Any attempted intrusion will be detected regardless of their location around the facility. Another advantage of fibre optic perimeter sensors is that they are not affected by environmental factors and electromagnetic interference.

- Use of Industrial-Grade Hardware

Upgrading to industrial-grade components capable of withstanding extreme weather conditions and prolonged outdoor operation would ensure system durability and reliability during real-world deployment.

- Machine Learning Integration

Incorporating machine learning algorithms for pattern recognition and predictive analysis will enable the system to intelligently classify motion types, learn from past intrusion data, and minimize false alarms.

- Alternate Power Source

Introducing solar-powered modules for off-grid or remote areas where electricity supply is unreliable will make the system energy-efficient and sustainable.

- LoRa Mesh Expansion

The communication network can be extended using LoRa mesh topology to improve coverage, fault tolerance, and multi-node coordination across wider geographical areas.

ACKNOWLEDGEMENT

The authors sincerely thank all individuals and institutions whose support, guidance, and encouragement contributed to the successful completion of this research. Above all, we give glory and honour to the Lord Almighty, whose divine wisdom, provision, and grace sustained us and made this work possible.

REFERENCES

Antem, E. and Ebong, Y. (2018) 'Automated System for Monitoring Fueling Operations on Telecommunication Tower Sites', (December).

Chapungo, N.J. (2025) 'Experimental Evaluation of LoRaWAN Connectivity Reliability in Remote Rural Areas of Mozambique'.

Chigwende, S. and Govender, K. (2020) 'Corporate brand image and switching behavior: Case of mobile telecommunications customers in Zimbabwe', *Innovative Marketing*, 16(2), pp. 80–90. Available at: https://doi.org/10.21511/IM.16(2).2020.07.

Denis Mbowoh, K. and Eric Bewor, V. (2023) 'Generator's Fuel and Battery Levels Monitoring in Base Station Cell Sites Using IoT-Based Technology with SMS Alerts: A NEXTTEL Cameroon Perspective', 11, p. 3.

Judvaitis, J. *et al.* (2025) 'LPWAN Technologies for IoT: Real-World Deployment Performance and Practical Comparison', pp. 1–20. Available at: https://www.preprints.org/manuscript/202511.0316.

Karawita, W.S.R.M.C., Dhammearatchi, D. and De Silva, R. (2020) 'Access Control & Security Alarm System for BTS Management with Microcontroller', *CINEC Academic Journal*, 4(1), p. 1. Available at: https://doi.org/10.4038/caj.v4i1.88.
Liu, X. (2023) 'Design of Wireless Communication Base Station Monitoring System Based on Artificial Intelligence and Network Security', *Procedia Computer Science*, 228, pp. 1254–1261. Available at: https://doi.org/10.1016/j.procs.2023.11.097.

Masarakufa, C. (2023) *Vandalism Seriously Affecting Telecommunications Companies In Zimbabwe - StartupBiz Zimbabwe*. Available at: https://startupbiz.co.zw/vandalism-seriously-affecting-telecommunications-companies-in-zimbabwe/ (Accessed: 3 September 2025).

Ndlovu, B. (2024) 'Di g ita l r ig h ts a nd i nclus i on i n a f r i ca r e port 20 23'.
Newsday (2012) *'Gang gets 20 years for raiding Econet Base Stations'*.

NewsDay (2023) *Telcos battle rising cases of vandalis - Zimbabwe Situation*, *NewsDay Zimbabwe*. Available at: https://www.zimbabwesituation.com/news/telcos-battle-rising-cases-of-vandalis/ (Accessed: 3 September 2025).

P, C.M. and Kwashirai, Z. (2021) 'Infrastructure Vandalism and Protection in a Vulnerable Zimbabwean Environment : Review of the Structural Materialism Theory', 3878(3), pp. 10–16. Available at: https://doi.org/10.35940/ijrte.C6355.0910321.

Ph.D., B.B. and V, A.M. (2024) 'Smart Anti-Theft Security Sytem Using Iot', *Iarjset*, 11(6), pp. 138–143. Available at: https://doi.org/10.17148/iarjset.2024.11618.

Ranjith, K. and Saibaba, J. (2022) 'Cell Phone Tower Base Station Safety And Security System 1Prathyusha Muthukur,2Shaik Misbah NuISSN NO : 0377-9254 Page No : 628 Vol 13 , Issue 03 , MARCH / 2022 ISSN NO : 0377-9254 Page No : 629', *Journal Of Engineering Sciences*, 13(03), pp. 628–637.

Safeguard (2021) 'SAFEGUARD CRIME REPORT – FEBRUARY 2021 HIGH-RISK AREAS SAFEGUARD CRIME REPORT – FEBRUARY 2021 MODUS OPERANDI', (February), pp. 1–9.

Sathish, A. *et al.* (2020) 'Antitheft System For Battery', pp. 218–224.

Tshili, N. and Chitumba, P. (2024) *Crack unit to deal with vandalism, theft - herald*, *The Herald*. Available at: https://www.heraldonline.co.zw/crack-unit-to-deal-with-vandalism-theft/ (Accessed: 3 September 2025).