KWARA STATE UNIVERSITY, MALETE

FACULTY OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

DESIGN AND CONSTRUCTION OF AN IOT BASED INTRUSION DETECTION SYSTEM FOR A TRANSFORER AGAINST VANDALIZATION

(A Case Study of KWASU Library 500KVA Transformer)

Submitted by

AYOMIPOSI PRAISE ADEMAKINWA
20D/67EC/01055

Submitted to

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

In partial fulfillment for the Award of Bachelor of Engineering Degree in Electrical and Computer Engineering.

January 2024

ABSTRACT

The escalating trend of transformer vandalism poses a significant financial burden on electricity distribution companies, compelling frequent replacements of pilfered components and also causes lot of inconvenience to consumers due to resulting power failure. This has greater need for the protection of the transformers globally. In response, an innovative system is in the works, integrating a micro-controller, camera, radar sensor for motion detection, and GSM module to detect potential vandals. Emphasizing factors such as cost-effectiveness and mobility, this surveillance and anti-vandalism solution aims to safeguard transformers effectively.

Contents

1 CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

Transformers are vital components of the electricity grid, and their vulnerability to vandalism poses a significant threat. In Nigeria, with its rapidly growing electricity demand and infrastructure investment, transformers endure an alarming wave of vandalism which plunge communities into darkness and inflict financial burdens, particularly in Kwara State.

In Kwara State, an alarming rate of power outages echoes through communities ravaged by rampant transformer vandalism. KEDC reports paint a grim picture: thousands plunged into darkness, vital businesses crippled, and millions lost to theft and damage. NECR data amplifies the chorus, highlighting the alarming frequency of these attacks across the state. Existing security measures, largely physical barriers, often prove ineffective due to false alarms, delayed response times, and limited coverage (Adegboye et al., 2022).

This dire situation demands a new solution - an IoT-based intrusion detection system poised to revolutionize transformer security. These systems utilize sensors (motion, temperature) to monitor transformers in real-time, triggering alerts upon suspicious activity (Abiodun et al., 2023. Implementing such a system in Kwara State, while requiring careful consideration of infrastructure and costs, can significantly mitigate the detrimental effects of transformer vandalism and ensure reliable power supply (Olajide et al., 2022).

1.2 MOTIVATION

Visualize Kwara State illuminated by a perpetual glow, with businesses flourishing and communities abuzz with activity as the persistent menace of power outages becomes a relic of the

past. This vision isn't merely a figment of imagination. It's the tangible outcome achievable through our concerted efforts to combat rampant transformer vandalism. Envision students immersed in uninterrupted study sessions, hospitals operating at full capacity, and countless lives and livelihoods safeguarded from the grip of darkness. This isn't merely an engineering challenge; it's a mission to illuminate Kwara State. By designing and implementing an IoT-based intrusion detection system and rewriting its narrative from blackout to brilliance, Kwara State can be safeguarded against the threat of vandalism.

1.3 PROBLEM STATEMENT

In Kwara State, transformers stand in silent vigil, vulnerable to the shadows of vandalism. Each attack plunges communities into darkness, cripples businesses, and siphons millions from the state's economic bloodstream. Current security measures, like bumbling watchmen, stumble with false alarms and sluggish responses, leaving these critical assets exposed. A sentinel with sharper senses, quicker reflexes, and unwavering vigilance is needed.

1.4 AIM AND OBJECTIVES

The aim of the project is to design and implement an efficient and cost-effective IoT-based intrusion detection system (IDS) for transformers in Kwara State, Nigeria, to significantly reduce the incidence of vandalism and ensure reliable power supply. Using the KWASU 500KVA library transformer as a case study.

The objectives of the project include:

i. Conduct a comprehensive study of existing transformer security measures in Kwara State and their limitations.

ii. Design an IoT-based IDS architecture suitable for deployment on 500KVA transformers in Kwara State University Malete, considering cost, power availability, and communication infrastructure.

iii. Implement the designed IDS on a pilot basis at selected transformers in Kwara State.

iv. Evaluate the effectiveness of the IDS in reducing transformer vandalism.

v. To document the entire process of designing, constructing, and testing the anti-vandalism system, and provide comprehensive guidelines for deploying and maintaining the system within the power industry

vi. Present the project findings and recommendations.

1.5 SCOPE OF STUDY

Imagine a guardian, not of mere stone, but of intelligent sensors and watchful optics, standing sentinel over Kwara State University's vital 500kVA transformer. By combining the watchful gaze of cameras with the sensitive whispers of temperature and vibration sensors, a multi-layered shield against vandalism will be created. Temperature shifts and vibrations are detected by sensors, instantly triggering an SMS alert and a live camera feed to the administrator's phone. No time is wasted, no shadows creep in. This pilot project on the university transformer isn't just illuminating the library; it's lighting the path towards a safer future for Kwara State's power grid, one transformer at a time.

1.6 PROJECT LAYOUT

The organizational structure outlined below is adhered to in the project report:

Chapter 1: Introduction

In this chapter, an overview of the research project is presented. It encompasses an introduction to the project, a delineation of the problems under scrutiny, the study's goals, aim and objectives, the research's importance, the study's scope, and the layout of the project.

Chapter 2: Literature Review

This chapter Reviews existing research for transformers, focusing on direct sensor-based approaches and analyzing previous research utilizing AI algorithms for transformer failure prediction and identify gaps in knowledge.

Chapter 3: Methodology

This chapter describes the watchful gaze of cameras with the sensitive whispers of temperature and vibration sensors, the creation of a multi-layered shield against vandalism explaining the preprocessing techniques used to ensure that the sensors whisper of temperature shifts and vibrate and how it instantly triggers an SMS alert and a live camera feed.

Chapter 4: Result and Analysis

In this chapter, a comparative analysis of PIR Sensor [For Motion] is performed, highlighting their strengths and weaknesses in predicting transformer failures based on grid stability data.

Chapter 5: Conclusion and Recommendation

This chapter summarizes the key findings of the project, emphasizing the feasibility and advantages of using an IOT Based Intrision System f or a transformer against vandalism. Also to draw conclusions about the effectiveness

REFERENCES

Include a comprehensive list of all cited sources according to the preferred style guide.

2 CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL BACKGROUND

2.1 INTRODUCTION

The purpose of this chapter is to review existing literature both the past and the present. Research began by reviewing journals, magazines, books, and internet sites in the field of transformers, focusing on direct sensor-based approaches and analyzing previous research utilizing AI algorithms for transformer failure prediction and identify gaps in knowledge. In this chapter, the background theory of our topic is discussed and several terms associated with it will also be discussed and reviewed.

2.2 THEORETICAL BACKGROUND

2.2.1 VANDALISM OF DISTRIBUTION TRANSFORMER

Vandalism of distribution transformers constitutes a severe threat, involving deliberate damage to critical electrical infrastructure within the power grid. This malicious act disrupts the flow of electricity to homes, businesses, and essential services, resulting in power outages that not only inconvenience individuals but also jeopardize public safety and essential operations, such as medical facilities. Beyond the immediate inconvenience, the financial toll of repairing or replacing damaged transformers is substantial, placing strains on utility providers and potentially leading to increased consumer costs. Furthermore, environmental concerns arise from the leakage of transformer oil, which can contaminate ecosystems and pose risks to public health, necessitating costly cleanup efforts.

Various factors contribute to the prevalence of transformer vandalism, including physical damage driven by the theft of valuable materials, exploitation of software vulnerabilities, and systemic

inefficiencies within the distribution system. To address this multifaceted challenge, comprehensive strategies are needed, encompassing enhanced security measures, community engagement, and technological innovations. By implementing proactive measures to protect critical infrastructure, raising awareness about the consequences of vandalism, and leveraging advanced technologies for surveillance and detection, stakeholders can collaborate to mitigate the socio-economic and environmental impacts of transformer vandalism and safeguard the reliability of the power grid for all.

2.2.2 INTRUSION DETECTION SYSTEM

An Intrusion Detection System (IDS) is a vital part of a security infrastructure, designed to detect and respond to unauthorized access attempts or security breaches within a network or a physical environment. The primary function of an IDS is to monitor network traffic, system activities, or physical spaces for suspicious behavior or patterns that indicate a security threat. Two main types of intrusion detection systems exist: Network-based IDS (NIDS) and Host-based IDS (HIDS).

A. **NIDS** operates by analyzing network traffic in real-time, looking for signs of suspicious activity such as unauthorized access attempts, malware infections, or unusual communication patterns. It examines packets of data passing through network segments, searching for known attack signatures or anomalous behavior. NIDS sensors are strategically placed at key points within the network to monitor traffic flow effectively. When suspicious activity is detected, alerts are generated to notify security personnel, allowing them to investigate and mitigate the threat promptly.

B. On the other hand, **HIDS** focuses on monitoring individual host systems such as servers, workstations, or endpoints. HIDS agents are deployed on these systems to collect and

analyze logs, system events, and file integrity data. By monitoring system calls, file accesses, and other activities, HIDS can detect unauthorized changes to system configurations, file tampering, or the presence of malicious software. HIDS provides granular visibility into the security posture of individual hosts, complementing network-based detection mechanisms.

Intrusion detection systems employ a variety of detection techniques, including signature-based detection, anomaly-based detection, and behavior-based detection. Signature-based detection relies on predefined signatures or patterns of known attacks to identify malicious activity. Anomaly-based detection compares observed behavior against baseline profiles or statistical models to detect deviations from normal activity. Behavior-based detection analyzes user and system behavior over time to identify patterns indicative of malicious intent.

Intrusion detection systems play a crucial role in enhancing security measures for critical infrastructure, specifically transformers. By integrating intrusion detection sensors and systems, a robust security framework capable of detecting and responding to potential threats in real-time can be established.

2.2.3 INTERNET OF THINGS (IoT)

The Internet of Things (IoT) refers to a vast network of interconnected devices, objects, and machines that are equipped with sensors, software, and other technologies. These devices, which range from everyday household items like refrigerators and thermostats to sophisticated industrial machinery and wearables, collect, exchange, and analyze data over the internet. The IoT process involves data collection by sensors embedded in the devices, data transmission to a central hub or cloud platform via various communication technologies, data analysis and processing on the

platform often using AI and machine learning algorithms, and action and response based on the analysis. The variety of IoT devices is constantly expanding and includes smart home devices, wearables, Industrial IoT (IIoT) devices, and connected cars.

The benefits of IoT are numerous. It can increase efficiency and productivity by automating tasks, optimizing processes, and improving resource management across various industries. These systems can also monitor restricted areas around power lines or substations, detecting intrusions and potentially deterring vandals. However, IoT also presents challenges such as security and privacy concerns, interoperability and standardization issues, and ethical considerations. Despite these challenges, the future of IoT is brimming with potential, with advancements in technologies like artificial intelligence, edge computing, and 5G networks expected to further unlock its capabilities. We can expect to see even more widespread adoption of IoT across various sectors, leading to smarter cities, safer power grids, personalized healthcare, and a more connected and efficient world.

2.2.4 SENSORS

A sensor is a device that detects and responds to changes in its physical environment. It acts as a bridge between the physical world and the electronic world, converting physical phenomena into measurable signals. They make it possible to create an ecosystem for collecting and processing data about a specific environment so it can be monitored, managed and controlled more easily and efficiently. They emerge as pivotal instruments ensuring robust surveillance and real-time threat detection. The intricate network of sensors strategically placed in and around the transformer serves as a vigilant frontline defense mechanism, meticulously monitoring various facets of the transformer's environment to preclude unauthorized access and tampering.

2.2.4.1 TYPES OF SENSORS

In the context of transformer vandalization, some sensors used include:

A. **Proximity Sensors**: Proximity sensors are versatile devices used across various industries for detecting the presence or absence of nearby objects or individuals without physical contact. They work by emitting an electromagnetic field or beam and then detecting changes in that field caused by the presence of an object. This technology finds applications in automatic doors, mobile devices, industrial machinery, and security systems. Capacitive, inductive, ultrasonic, and infrared are common types of proximity sensors.

B. **Vibration Sensors**: Vibration sensors senses vibrations across a wide frequency range and are commonly used in various fields such as structural health monitoring, predictive maintenance, automotive systems, and security applications. Vibration sensors can be piezoelectric, capacitive, or based on other sensing principles, and they are capable of detecting subtle vibrations that may indicate mechanical faults, tampering, or unauthorized access, making them essential for ensuring the integrity and safety of critical infrastructure and equipment.

C. **Sound Sensors**: Sound sensors, also referred to as microphones or acoustic sensors, are devices that detect sound waves in the environment. They are widely used in applications such as speech recognition, environmental monitoring, home automation, and security systems. In security applications, sound sensors play a crucial role in detecting unusual noises or events that may indicate unauthorized access, intrusion, or

other security breaches, enabling prompt responses to mitigate risks and ensure the safety and security of assets and facilities.

D. Infrared Sensors: Infrared sensors detect infrared radiation emitted by objects based on their temperature. They are commonly used for motion detection, temperature measurement, proximity sensing, and object detection in various applications ranging from consumer electronics to industrial automation and security systems. In security applications, infrared sensors are utilized to detect heat signatures of objects or individuals in their vicinity.

2.2.4.2 CONSIDERATIONS WHEN CHOOSING A SENSOR

When choosing a sensor, things to put into consideration include:

A. **Project Requirements:** The first step in choosing a sensor is understanding what you need the sensor to do. What kind of data do you need to collect? How will this data be used? The answers to these questions will help identify the type of sensor that can provide this data.

B. **Compatibility:** The sensors you choose need to be compatible with your IoT platform or network infrastructure. This means that the sensor should be able to communicate effectively with the rest of your system. It's important to check whether the sensor supports the same communication protocols as your system.

C. **Cost-Effectiveness:** The cost of sensors can vary widely, so it's important to consider both the upfront purchase cost and the ongoing maintenance cost. Your budget and the scale of your project will determine how much you can spend per sensor. However, it's also important to consider the long-term value that the sensor will provide.

D. **Environment:** The environment in which the sensor will be used can greatly affect its performance. Some sensors may not work well in certain conditions, such as extreme temperatures or high humidity. Therefore, it's important to choose a sensor that is suitable for the environment in which it will be used.

E. **Quality of the Sensor**: The quality of the sensor is another important factor. High-precision, high-accuracy sensors are desirable, but they may also be more expensive. On the other hand, a low-accuracy sensor may yield data that is not very useful. Therefore, it's important to find a balance between cost and quality.

F. **Sensor Security:** Security is a major concern in IoT applications. IoT devices, including sensors, can have significant security vulnerabilities that may put an organization's entire network at risk. Therefore, it's important to choose sensors that have robust security features.

2.2.5 ALARM SYSTEMS

An alarm system is a crucial component of security infrastructure designed to detect and alert users to potential threats or breaches in a monitored area. These systems utilize a combination of sensors, detectors, and signaling devices to detect unauthorized access, intrusion, fire, or other emergencies, and promptly notify relevant personnel or authorities to take appropriate action. Here are key components and features typically found in alarm systems.

A. **Sensors and Detectors:** Alarm systems rely on various sensors and detectors to monitor different types of threats or events. Common types include motion sensors, door/window contacts, glass break detectors, smoke detectors, heat detectors, and gas

detectors. These sensors are strategically placed to cover vulnerable entry points or detect specific hazards within the protected area.

B. **Control Panel:** The control panel serves as the central processing unit of the alarm system, responsible for receiving signals from sensors, processing data, and triggering appropriate responses. It also provides user interface options for arming/disarming the system, programming settings, and displaying status indicators and alerts.

C. **Communication Devices:** Alarm systems often incorporate communication devices to transmit alerts to designated recipients or monitoring centers. These devices may include landline phone connections, cellular networks, internet-based communication, or radio frequency transmitters. Backup communication methods are essential to ensure reliable transmission of alerts, especially in cases of network outages or tampering.

D. **Alarm Notification Devices:** Upon detecting a threat or triggering an alarm condition, the system activates notification devices to alert occupants, security personnel, or emergency responders. Common notification devices include sirens, strobe lights, voice/speech annunciators, and text/email alerts sent to designated contacts or monitoring centers.

E. **User Interface:** Alarm systems provide user-friendly interfaces for configuring settings, arming/disarming the system, and accessing status information. This interface may include keypad controllers, touchscreen panels, remote key fobs, or mobile applications for remote monitoring and control.

F. **Monitoring Services**: Many alarm systems offer optional monitoring services provided by professional security companies. These services involve 24/7 surveillance

of the alarm system's signals by trained operators who can verify alarms, dispatch emergency responders, or notify designated contacts as needed.

G. **Integration with Other Systems:** Alarm systems can be integrated with other security systems such as CCTV cameras, access control systems, and automation devices for enhanced functionality and centralized management. Integration allows for coordinated responses to security events and provides a comprehensive security solution.

H. **Backup Power Supply:** To ensure continuous operation during power outages, alarm systems are equipped with backup power supplies such as batteries or generators. These backup sources power critical components, including sensors, control panels, and communication devices, to maintain functionality and security even when the primary power source is unavailable.

2.2.5.1 TYPES OF ALARM SYSTEMS

There are various types of alarm system which include:

A. **Security Alarm Systems**: These are the most common, designed to prevent and detect unauthorized entry into a building or area. They use sensors like door and window contacts, motion detectors, and glass break detectors to trigger alarms, often accompanied by loud sirens and flashing lights. Some systems can also connect to monitoring centers for further response.

B. **Fire Alarm Systems**: These detect smoke, heat, or carbon monoxide and sound alarms to warn occupants of a fire and trigger evacuation procedures. They can be interconnected with security systems for comprehensive protection.

C. **Medical Alarm Systems**: These are often used by elderly or disabled individuals to call for help in case of a medical emergency. They may have panic buttons, fall detectors, or sensors that monitor vital signs.

D. **Personal Alarm Systems:** These portable devices are activated by individuals facing an immediate threat and emit loud sounds to attract attention and deter attackers.

2.2.5.2 CONSIDERATIONS WHEN CHOOSING ALARM SYSTEMS.

When choosing an alarm system, things to put into consideration include:

A. **Type of Installation:** Alarm systems can be either professionally installed or DIY (Do-It-Yourself). Professional installation is typically performed by experienced security experts, but it may come with an installation cost. DIY installation, on the other hand, is usually more straightforward and doesn't require professional help.

B. **Monitoring Service:** Some alarm systems offer professional monitoring services. These services monitor your system 24/7 and can contact the appropriate authorities in case of an emergency. However, these services usually come with a monthly fee.

C. **System Features:** Consider the features that you want in your alarm system. This could include home automation capabilities, remote control via mobile app, integration with other smart devices, etc.

D. **Cost:** The cost of alarm systems can vary widely. It's important to consider both the upfront costs (purchase of equipment, installation) and the ongoing costs (maintenance, monitoring service).

E. **User-Friendliness:** The alarm system should be easy to use. This includes a straightforward installation process, an intuitive control panel, and easy-to-understand alerts and notifications.

F. **Reliability:** The reliability of the system is crucial. This includes the battery life of wireless components, the range of sensors, and the system's resistance to tampering.

G. **Scalability:** Consider whether the system can be easily expanded or upgraded in the future as your needs change.

H. **Customer Support**: Good customer support can be very helpful for troubleshooting issues, understanding how to use the system, and getting assistance during emergencies.

2.2.5.3 EMBEDDED SYSTEMS

Embedded systems are specialized computer systems designed to perform a specific task within a larger mechanical or electronic system. They are essentially miniaturized computers that are embedded, inside devices, often invisible to the end user. Unlike general-purpose computers designed for various tasks, embedded systems are programmed for a single function, such as controlling the traffic lights in a city or monitoring the temperature within a building. In 2009, it was estimated that ninety-eight percent of all microprocessors manufactured were used in embedded systems

These systems typically consist of a microprocessor or microcontroller, memory, and input/output (I/O) devices. The software, known as firmware, is specifically written for the embedded system's designated task and stored in read-only memory. The complexity of embedded systems can vary greatly, ranging from simple devices with minimal user interface to intricate systems with complex

functionalities. They play a vital role in modern technology, silently operating behind the scenes in countless everyday devices, from smartphones and cars to power grids and industrial machinery.

2.2.6 MICRO CONTROLLER

A microcontroller (sometimes referred to as an MCU or Microcontroller Unit) is a compact integrated circuit (IC) designed for controlling specific tasks within electronic systems. The concept of microcontrollers emerged in the early 1970s. At that time, the Intel 4004 made its debut as the world's first single-chip microprocessor. These versatile devices combine a microprocessor unit (MPU), memory, and various peripherals on a single chip. Their primary purpose is to execute embedded applications that require both processing functionality and agile interaction with digital, analog, or electromechanical components. Microcontrollers find applications in a wide range of fields, from low-cost wearables and medical equipment to high-end consumer electronics and rugged industrial devices. They are user-friendly, cost-effective, and adaptable, making them an essential component in modern electronic products. These components are not only used by experienced electrical engineers but also by hobbyists, students, and professionals from various disciplines.

2.2.6.1 ARCHITECTURE OF A MICROCONTROLLER

A. CPU: Microcontrollers typically feature a compact CPU core, optimized for low power consumption and real-time processing. Common CPU architectures include ARM, AVR, PIC, and 8051, each offering different performance levels and instruction sets.

B. Memory: Microcontrollers integrate various types of memory, including Flash memory for program storage, RAM for data storage and temporary workspace, and EEPROM for non-volatile data storage.

C. **Peripherals:** Microcontrollers include a range of on-chip peripherals such as timers/counters, analog-to-digital converters (ADCs), digital-to-analog converters (DACs), UART, SPI, I2C interfaces, GPIO pins, PWM controllers, and more. These peripherals enable interaction with external devices and facilitate diverse functionality.

2.2.7 Types Of A Micro Controller

Microcontrollers come in a vast array of types, each suited for different tasks and applications. Here's a breakdown of some key categories to help you navigate the diverse world of microcontrollers:

A. **Based on Data Bus Width:**

- **8-bit Microcontrollers:** These microcontrollers have an 8-bit data bus width, making them suitable for applications with modest computational requirements and where cost and power consumption are critical factors. They are commonly used in simple control systems, household appliances, and low-cost embedded devices.

- **16-bit Microcontrollers:** With a wider 16-bit data bus, these microcontrollers offer improved performance and are suitable for applications requiring more computational power, such as motor control, instrumentation, and industrial automation. They provide better processing capabilities compared to 8-bit microcontrollers while remaining cost-effective.

- **32-bit Microcontrollers:** Featuring a 32-bit data bus width, these microcontrollers offer even higher performance and computational capabilities. They are ideal for applications requiring advanced processing, real-time operation, connectivity, and multimedia capabilities, such as automotive systems, medical devices, and consumer electronics.

B. Based on Architecture:

- **ARM-based Microcontrollers:** Microcontrollers based on the ARM architecture are widely used due to their energy efficiency, scalability, and extensive ecosystem of development tools and software libraries. ARM-based microcontrollers come in various configurations, ranging from low-power devices for IoT applications to high-performance devices for automotive, industrial, and consumer electronics applications.

- **Traditional Microcontrollers (PIC, AVR, 8051):** These microcontrollers are based on proprietary architectures and have been popular choices for many embedded applications. Examples include the Microchip PIC series, Atmel AVR series, and Intel 8051 series. They offer a wide range of features, peripherals, and development tools, making them suitable for diverse applications ranging from simple control tasks to more complex embedded systems.

C. Based on Specialization:

- **Digital Signal Controllers (DSCs):** These microcontrollers are optimized for digital signal processing (DSP) tasks and feature enhanced DSP instructions, hardware acceleration, and specialized peripherals. They are used in applications such as audio processing, motor control, digital power management, and telecommunications.

- **Application-Specific Microcontrollers**: Some microcontrollers are designed for specific applications or industries, incorporating specialized features and peripherals to meet unique requirements. Examples include automotive microcontrollers with built-in CAN interfaces, medical microcontrollers with safety features, and industrial microcontrollers with support for industrial communication protocols.

2.3 LITERATURE REVIEW

In a study conducted by (Wang et al, 2023), a novel machine learning-based Network Intrusion Detection System (NIDS) was proposed. This system combines network traffic-based and telemetry data-based NIDS. A self-attention mechanism is utilized to learn contextual embeddings for input network features, which aids in classifying network flow behavior as benign or malicious. This approach could be adapted for transformer protection by training the model on network traffic patterns associated with normal operation and various types of vandalism. The proposed method utilizes a self-attention mechanism to learn contextual embeddings for input network features. Based on the contextual embeddings, their method can solve the feature set challenge, including both continuous and categorical features. Their method is the first to utilize both network traffic data and IoT sensors' telemetry data at the same time for intrusion detection. Experiments reveal the effectiveness of their method on a realistic network traffic intrusion detection dataset named ToN_IoT, with an accuracy of 97.95% for binary classification and 95.78% for multiple classifications on pure network data (Wang et al, 2023).

(Elrawy et al, 2018) provided a comprehensive survey of the latest IDSs designed for the IoT model. The corresponding methods, features, and mechanisms used in these systems were discussed. The authors highlighted the need for IDSs designed specifically for IoT environments to mitigate IoT-related security attacks. This is relevant to transformer protection as transformers can be considered as part of an IoT environment. They also provide deep insight into the IoT architecture, emerging security vulnerabilities, and their relation to the layers of the IoT architecture. This work demonstrates that despite previous studies regarding the design and implementation of IDSs for the IoT paradigm, developing efficient, reliable and robust IDSs for IoT-based smart environments is still a crucial task (Elrawy et al, 2018)

In this study conducted by (Long et al, 2024), a novel Network Intrusion Detection System (NIDS) was proposed, which is anchored in the Transformer model and finely tailored for cloud environments. The authors melded the fundamental aspects of network intrusion detection with the sophisticated attention mechanism inherent to the Transformer model. This facilitated a more insightful examination of the relationships between input features and diverse intrusion types, thereby bolstering detection accuracy. The authors provided a detailed design of their approach and conducted a thorough comparative evaluation. Their experimental results demonstrated that the accuracy of their model is over 93%, which is comparable to that of the CNN-LSTM model, underscoring the effectiveness and viability of their Transformer-based intrusion detection algorithm in bolstering cloud security.

In this study by (Hazman et al, 2023), a revolutionary intrusion detection methodology for IoT-based smart environments was described. The approach presented an optimum anomaly detection model which is based on AdaBoost and the Boruta feature selection technique based on the Xgboost algorithm. The suggested model metrics were evaluated utilizing the NSL-KDD and BoT-IoT datasets. When compared to existing IDS, the results demonstrated that the proposed method produces excellent performance metrics in high accuracy (ACC), recall, and F1-score. It gives 99.9% on record detection and computation time.

(Khraisat et al, 2021) presented a comprehensive review of contemporary IoT IDS and an overview of techniques, deployment Strategy, validation strategy and datasets that are commonly applied for building IDS. They also reviewed how existing IoT IDS detect intrusive attacks and secure communications on the IoT. It also presents the classification of IoT attacks and discusses future research challenges to counter such IoT attacks to make IoT more secure (Khraisat et al, 2021).

3 CHAPTER THREE

METHODOLOGY

3.1 INTRODUCTION

This chapter begins with the selection of appropriate IoT devices and sensors that are capable of detecting potential vandalism activities. It then proceeds to the design of the network architecture that allows these devices to communicate effectively. The core of this chapter is the development of the intrusion detection algorithm, which is based on machine learning techniques to accurately identify potential intrusions. The construction of the system involves the physical installation of the IoT devices and sensors, as well as the setup of the network infrastructure. By the end of this chapter, a fully functional prototype of the intrusion detection system will be ready for testing and evaluation.

3.1.1 IoT DEVICES AND SENSORS