# ABSTRACT

In the modern digital landscape, cyber threats have become increasingly sophisticated, posing significant risks to organizations and individuals. As networks grow in complexity, traditional security measures often fall short in effectively detecting and mitigating evolving threats. This research focuses on the design and implementation of a comprehensive approach to monitor malicious activities and provide robust network protection. The proposed system integrates multiple security mechanisms, including real-time threat detection, anomaly-based monitoring, and automated incident response. By leveraging advanced machine learning algorithms and signature-based Intrusion Detection Systems (IDS), the proposed new approach ensures accurate identification of suspicious activities such as unauthorized access attempts, malware propagation, and data exfiltration. Additionally, behavioral analysis techniques are employed to detect deviations from normal network activity, allowing for proactive threat mitigation. The effectiveness of the proposed approach is evaluated through extensive simulations and real-world testing in controlled network environments. Experimental results demonstrate its capability to detect various forms of cyber threats with high accuracy while maintaining minimal false positives. Moreover, the system proves to be scalable, adaptable, and efficient in protecting networks from both known and emerging threats. In conclusion, this research presents a holistic approach to network security by combining real-time monitoring, threat intelligence, and automated mitigation strategies. The findings contribute to the advancement of cybersecurity frameworks, offering a viable solution for organizations seeking to enhance their network protection against increasingly sophisticated cyber threats.

# CHAPTER I: GENERAL INTRODUCTION

# INTRODUCTION

This study provides a comprehensive introduction to the study, laying the foundation for the exploration of **network protection** and **malicious activity monitoring. It also** highlights the **problem statement**, emphasizing the limitations of existing detection technologies and the need for advanced **intrusion detection systems (IDS)** that can address these shortcomings. The **objectives** of the study are outlined, including the design of a **threat monitoring system**, the integration of **IDS mechanisms.** also presents **research questions** and **hypotheses** to guide the study, investigating the efficacy of various detection and mitigation techniques. The **significance** of the study is emphasized, particularly in terms of improving cybersecurity practices, reducing response times to cyber threats. Finally, the chapter outlines the **scope** of the study, focusing on **real-time network monitoring** and **intrusion detection.**

# Background of the study

The Internet communication technology brings great convenience to our society. At the same time, a variety of viruses and malicious codes increasingly spread on the network seriously, it brings growing threats to the network. Among the various forms of malicious software, the Trojan and spyware are most popular in internet. These malwares are always used or programmed by attackers to gain access to private computer systems or gather sensitive information. Trojan and spyware distinguish themselves from other forms of malware, by that, they have to establish a command and control channel to translate command and data. Most of the current malware detection technology runs on one machine and cannot monitor the network layer effectively. (Jiang, 2010)

So such kind of malware detection is not beneficial for detecting the whole local area network (LAN). Some intrusion detection system (IDS)-based network malware detecting methods, such as Snort , is based on the communication ports and some other known characteristics. These methods do not identify or detect the communication behavior. Thus, these methods are sometimes ineffective with the malicious software that changes the ports dynamically and disguise themselves with protocols. They are also not effective for some unknown malicious software newly created. (Wrightson, 2012)

Modern malware detection requires a more comprehensive approach that extends beyond signature-based methods. Advanced detection techniques, such as **anomaly detection** and **machine learning**, offer the potential to identify previously unknown threats by analyzing network behavior, traffic patterns, and system activity in real-time. The integration of **behavioral analysis** can further enhance detection by identifying deviations from normal user or system behavior that may indicate the presence of malicious activity. (Xiang, 2015)

Additionally, there is a growing need for **automated threat mitigation** to address the speed and scale of cyberattacks. Manual responses to cyber incidents are often too slow and ineffective, leading to significant damage before a threat can be neutralized. By implementing **automated response mechanisms**, organizations can quickly isolate compromised devices, block malicious IP addresses, and contain attacks before they can spread further. (Xiang, 2015)

## 1.2 Problem Statement

In today's digital era, organizations face persistent cyber threats such as malware, phishing, Distributed Denial-of-Service (DDoS) attacks, and unauthorized access. Traditional security measures often fail to detect sophisticated attacks, leading to data breaches, financial losses, and reputational damage. To address these challenges, a comprehensive **Network Protection and Malicious Activity Monitoring System** is required to continuously monitor, detect, and respond to cyber threats in real-time. The proposed system will leverage advanced security techniques, threat intelligence, and automated response mechanisms to enhance organizational cybersecurity.

## 1.3 Objectives of the Study

### 1.3.1 General Objective

The general objective of the study is to design and implement an approach to monitor Malicious activities and provide network protection

### 1.3.2 Specific Objectives

1. To **Design a Threat Monitoring System** – Develop a framework for continuous monitoring of network traffic to detect malicious activities in real-time.
2. To **Implement Intrusion Detection Mechanisms** – Integrate both signature-based and anomaly-based intrusion detection systems (IDS) for threat identification.
3. To **Utilize Machine Learning for Threat Analysis** – Apply machine learning techniques to analyze patterns and detect previously unknown cyber threats.
4. To **Develop Automated Response Mechanisms** – Implement automated threat mitigation strategies such as blocking malicious IPs and isolating compromised devices.
5. To **Enhance Network Security Policies** – Design and enforce dynamic firewall rules and access control policies to prevent unauthorized access.
6. To **Integrate Behavioral Analysis Techniques** – Monitor user and network behavior to detect anomalies that may indicate cyber threats.
7. To **Implement a Security Information and Event Management (SIEM) System** – Collect, analyze, and correlate security logs for centralized threat intelligence and reporting.



**1.4 Research Questions**

1. What are the key challenges in monitoring and detecting malicious activities in a network environment?
2. How can machine learning techniques improve the accuracy of threat detection in network security?
3. What are the advantages and limitations of integrating signature-based and anomaly-based intrusion detection methods?
4. How effective is automated threat mitigation in reducing the impact of cyberattacks?
5. What role does behavioral analysis play in identifying network anomalies and potential security threats?
6. How can a Security Information and Event Management (SIEM) system improve real-time threat intelligence and response?
7. What are the performance benchmarks for evaluating the effectiveness of a network protection system?

## 1.5. Research hypothesis

* 1. **H₀ (Null Hypothesis):** The integration of machine learning techniques does not significantly enhance the detection of malicious activities in network security.  
     **H₁ (Alternative Hypothesis):** The integration of machine learning techniques significantly enhances the detection of malicious activities in network security.
  2. **H₀:** Signature-based and anomaly-based intrusion detection systems (IDS) do not complement each other in improving network threat detection.  
     **H₁:** The combination of signature-based and anomaly-based IDS enhances network threat detection by providing more comprehensive coverage.
  3. **H₀:** Automated threat mitigation mechanisms do not significantly reduce the impact of cyberattacks compared to manual response methods.  
     **H₁:** Automated threat mitigation mechanisms significantly reduce the impact of cyberattacks by providing faster and more effective responses.
  4. **H₀:** Implementing behavioral analysis techniques does not improve the detection of network anomalies and potential security threats.  
     **H₁:** Implementing behavioral analysis techniques improves the detection of network anomalies and potential security threats.
  5. **H₀:** A SIEM system does not enhance real-time threat intelligence and incident response in network security.  
     **H₁:** A Security Information and Event Management (SIEM) system enhances real-time threat intelligence and incident response in network security.
  6. **H₀:** The proposed network protection system does not offer significant improvements in scalability and adaptability to emerging cyber threats.  
     **H₁:** The proposed network protection system significantly improves scalability and adaptability to emerging cyber threats.
  7. **H₀:** Dynamic firewall rules and access control policies do not contribute to enhanced network security and threat prevention.  
     **H₁:** Dynamic firewall rules and access control policies significantly enhance network security and threat prevention.

## 1.6 significance of the study

This study is significant as it enhances cybersecurity by designing and implementing an advanced approach to monitor malicious activities and provide robust network protection. By integrating real-time threat detection, machine learning, and automated mitigation mechanisms, the study improves the accuracy of identifying cyber threats and reduces response time. It benefits organizations by securing sensitive data, ensuring compliance with cybersecurity regulations, and minimizing the impact of cyberattacks. Additionally, the study contributes to research in network security by offering scalable and adaptable solutions to emerging threats, ultimately protecting businesses, institutions, and individual users from potential cyber risks.

## 1.7 Scopes

The **Network Protection and Malicious Activity Monitoring System** will focus on the following key areas:

* **Real-time monitoring of network traffic to identify and mitigate potential threats.**
* **Deployment of intrusion detection and prevention systems (IDPS) to detect suspicious activities.**
* **Integration of threat intelligence feeds to stay updated with the latest cyber threats.**

## 1.****8. Study Delimitations****

While the proposed **Network Protection and Malicious Activity Monitoring System** aims to provide comprehensive cybersecurity solutions, it has certain limitations:

**Limited Scope to Network Security:** This study focuses solely on network protection and does not cover endpoint security, physical security, or insider threats extensively.

**Dependency on Threat Intelligence Feeds:** The effectiveness of real-time threat detection is dependent on the quality and accuracy of external threat intelligence feeds.

**AI/ML Limitations:** While AI/ML enhances anomaly detection, it may produce false positives and require continuous retraining to adapt to evolving threats.

**Infrastructure and Resource Requirements:** The implementation of real-time monitoring and automated response mechanisms requires significant computing resources and may not be feasible for small-scale organizations with limited budgets.

**Exclusion of Social Engineering Attacks:** The system primarily focuses on network-based threats and does not directly address phishing, impersonation, or other social engineering tactics.

**Legal and Compliance Challenges:** Deploying monitoring and detection mechanisms must comply with data privacy regulations, which may vary across different regions and industries.

**The** case study was conducted at UNIVERSITY OF KIGALI Musanze campus in Musanze District. This study was conducted there in order to analyze common malicious attacks that frequently targets the network system of that campus and propose an updated security system that will monitor all these threats and provide protection to that network system.

## 1.9 Research methodology

## 1.9.1. Q/Q or both….. (reference)

Several methods were taken in this study to integrate qualitative and quantitative methods. qualitative methods that will be used in this study are the following: Research Design, Data Collection Methods such as interviews, documentation, Semi-structural questionnaires and observation, Sampling Strategy and Data Analysis While quantitative techniques, like surveys and data analysis, will be used to gather numerical data on variables such as waiting times and passenger satisfaction, qualitative techniques such as focus groups, interviews, and observations will be utilized to understand the viewpoints of stakeholders. Convenience and stratified sampling will be employed for selecting bus stands and survey participants, respectively. Ethical considerations will ensure informed consent and confidentiality. Acknowledgment of limitations and delimitations will define the study's boundaries and scope, allowing for systematic data collection and analysis to evaluate the effectiveness of smart monitoring systems. The preferred research methodology to be used on this study is agile methodology. (Johnson, 2007)

## 1.9.2. Agile Software Process Method

## In my study I chose agile as a software process method. The ****Agile Software Process**** is a collection of software development methodologies that emphasize flexibility, collaboration, rapid delivery, and continuous improvement. Agile promotes iterative cycles with constant feedback from users and stakeholders. (Rasmusson, 2001)

## 1.9.3. Questionnaires

## In ****research methodology****, ****questionnaires**** are a widely used tool for collecting data, especially in ****quantitative research****, though they can also be used in ****qualitative research****. They are a structured form of data collection that involves asking participants a series of predefined questions to obtain information about a specific topic, behavior, or attitude. (Saunders, 2019)

## 1.10. Expected Results

**Improved Detection of Malicious Activities**

**Accurate Identification of Threats:**

The system should be able to correctly identify malicious activities (e.g., malware, DDoS attacks, unauthorized access attempts, phishing attacks) with high **accuracy** and **low false positive rates**.

**Effective Network Protection**

**Automated Mitigation of Malicious Activities:**

Upon detecting malicious activities, the system could automatically take actions such as **quarantining affected devices**, **isolating compromised network segments**, or **blocking harmful IP addresses** to prevent further damage.

**Enhanced Visibility and Monitoring**

**Centralized Dashboard for Monitoring:**The approach would likely feature a **centralized monitoring dashboard** where security analysts can visualize network traffic, identify potential threats, and analyze ongoing incidents. This dashboard would provide real-time insights into network health, threat status, and system vulnerabilities.

**Low Overhead and Minimal Impact on Network Performance**

**Scalable Performance:** The monitoring system should be **scalable** to handle varying amounts of network traffic, from small local networks to large enterprise networks, without introducing significant latency or resource overhead.

## 1.11 Organization of study

This research project paper was organized into five chapters:

**Chapter one** is the General Introduction and it includes the background of the study, problem statement, research obje ctives, research questions, research hypothesis, choice of the study, the significance of the study, limitations of the study, research methodology, and organization of the study.

**Chapter two** is Literature Review which will present theoretical concepts and fundamental definitions used in the research paper. The main objective is to provide useful information and explain the technology required to develop the research project.

**Chapter three** is Research Methodology and will describe the details of the developed project application analysis and its design. This chapter presents the study area and techniques used in the research project development.

**Chapter four** is Analysis, Design, and Implementation which will present and discuss the results. In this chapter, all findings during research will be displayed here. It will show the results in the form of tables, figures, and data.

**chapter five** is the Conclusion and Recommendations formulated with respect to the research objectives. There will also be references used in the project research.

# CHAPTER 2: LITERATURE REVIEW

**2.1** **Introduction**

This chapter includes the definition of the key concepts used in this study and explores related work in the field. It examines previous research and technology in IoT applications, particularly for systems designed to monitor the bus stand operation.

## 2.2 RELATED WORKS

**Kabiri & Ghorbani (2020)** analyzed signature-based intrusion detection systems (IDS) and found them highly effective for detecting known attacks but ineffective against zero-day exploits.**Snort and Suricata**, popular open-source IDS, use this approach but require frequent signature updates to remain effective. (Ghorbani, 2020)

**J. Zhang et al. (2021)** explored deep learning-based IDS, demonstrating that autoencoders and long short-term memory (LSTM) networks enhance anomaly detection accuracy. A challenge in anomaly detection is the high false-positive rate, leading to increased alert fatigue among security analysts. (Zhang, 2021)

**R. Brown (2020)** achieved 94% accuracy in detecting malicious traffic using CNN-based intrusion detection.The computational complexity of deep learning models limits their deployment in resource-constrained environments. (Brown, 2020)

**K. Patel et al. (2021)** deployed lightweight honeypots to collect botnet attack signatures. These honeypots are effective for basic threat intelligence but cannot capture sophisticated attack behaviors. (Patel, 2021)

**M. Ali (2021)** explored flow-based DDoS detection, highlighting that NetFlow analytics accurately detect volumetric attacks. However, flow-based monitoring struggles to detect stealthy, low-volume attacks. (Ali, 2021)

## 2.5 Research gap

Existing network security solutions, such as firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) systems, often work in isolation, leading to gaps in real-time threat detection and response. Additionally, many traditional security systems rely on signature-based detection, which fails to identify new and unknown (zero-day) attacks.

Another critical gap lies in the lack of integrated, automated response mechanisms that can proactively mitigate threats without human intervention. Current solutions often detect threats but require manual intervention to neutralize them, which delays response time and increases the risk of successful cyberattacks.

This research aims to address these gaps by designing and implementing a comprehensive network security approach that integrates real-time monitoring, AI-driven anomaly detection, and automated response mechanisms. By bridging the disconnect between threat detection and mitigation, the study seeks to enhance network protection against both known and evolving cyber threats.

## 2.3 Definition of the key concepts

### 2.3.1 System Approach

A **system approach** is a way of solving problems or managing tasks by **looking at the entire system as a whole**, rather than in isolated parts. It focuses on understanding **how all the components interact** with each other to achieve a common goal

**Network security system approach**: A structured, integrated method to address network security as a whole.

### ****2.3.2Threat detection in networking****

**Threat detection in networking** is the process of **identifying potential malicious activities or security threats** within a computer network. The goal is to **spot cyberattacks early**, before they can do damage—like stealing data, corrupting files, or taking down systems.

### 2.3.3 ****Network protection mechanisms****

**Network protection mechanisms** are the **tools, techniques, and strategies** used to **defend a network** from unauthorized access, misuse, and cyber threats. They're the **security layers** that keep your data, devices, and users safe.

**2.3.4** Incident Response

Incident Response is real-time and immediate – it focuses on stopping the threat and minimizing damage.

Digital Forensics is **after-the-fact** – it dives deep into logs, files, and systems to reconstruct the timeline and gather evidence.

### 2.3.5 Computer network

### A computer network is a set of [computers](https://en.wikipedia.org/wiki/Computer) sharing resources located on or provided by [network nodes](https://en.wikipedia.org/wiki/Node_(networking)). Computers use common [communication protocols](https://en.wikipedia.org/wiki/Communication_protocol) over [digital](https://en.wikipedia.org/wiki/Digital_signal) [interconnections](https://en.wikipedia.org/wiki/Interconnection) to communicate with each other. These interconnections are made up of [telecommunications network](https://en.wikipedia.org/wiki/Telecommunications_network) technologies based on physically wired, [optical](https://en.wikipedia.org/wiki/Optical_fiber), and wireless [radio-frequency](https://en.wikipedia.org/wiki/Radio_frequency) methods that may be arranged in a variety of [network topologies](https://en.wikipedia.org/wiki/Network_topology).

### 2.3.6 Malicious activities in a network

Malicious activities in a network" refers to any intentional actions taken by a cybercriminal to exploit vulnerabilities within a computer network, aiming to gain unauthorized access, steal data, disrupt operations, or cause damage, including activities like malware infections, phishing attacks, denial-of-service attacks, unauthorized access attempts, and data breaches.

### 2.3.7 Network threats

A network threat refers to any potential activity or event that could harm or interrupt the systems, applications and services operating on a network. These threats can compromise the security of the network by attacking its infrastructure with the primary target usually being information theft or service disruption.

### 2.3.8 Cyber security

Cyber security is how individuals and organizations reduce the risk of cyber attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

### 2.3.6 Network integrity

Network Integrity gives you insight into whether users are connecting to an evil twin or suspicious network. Attackers set up evil twin hotspots, which are Wi-Fi access points that an attacker sets up. The fake hotspot imitates a legitimate hotspot, including the primary network name of a nearby business, such as a coffee shop that provides free Wi-Fi access to its customers.

### 2.3.7 Virus

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software

### 2.3.8 Spyware

### Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent.

## 2.4 Some network tools that can be used in network monitoring

1. **Intrusion Detection System (IDS)** – Monitors network traffic for suspicious activities and generates alerts when potential threats are detected. Examples: **Snort, Suricata**.
2. **Intrusion Prevention System (IPS)** – Similar to IDS, but with the capability to actively block or mitigate detected threats in real-time. Examples: **Zeek (formerly Bro), Cisco Firepower**.
3. **Firewall** – A security system that filters incoming and outgoing network traffic based on predefined rules, preventing unauthorized access. Examples: **pfSense, iptables, Cisco ASA**.
4. **Security Information and Event Management (SIEM) System** – Collects, analyzes, and correlates security event logs from various sources to provide real-time threat intelligence and incident response. Examples: **Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), IBM QRadar**.
5. **Packet Sniffers and Network Analyzers** – Capture and analyze network traffic to detect anomalies and security vulnerabilities. Examples: **Wireshark, tcpdump**.
6. **Vulnerability Scanners** – Identify security weaknesses in systems and networks by scanning for known vulnerabilities. Examples: **Nessus, OpenVAS, Qualys**.
7. **Endpoint Detection and Response (EDR) Tools** – Monitor endpoint devices (computers, servers, mobile devices) for malicious activities and provide incident response capabilities. Examples: **CrowdStrike Falcon, Microsoft Defender for Endpoint**.
8. **Honeypots** – Decoy systems designed to attract and analyze attackers' behavior without putting real systems at risk. Examples: **Cowrie, Dionaea**.

## 2.5 Hardware and software tools that will be used in development of this system

## 2.5.1 hardware requirements

* Multi-core processors (Intel i7/i9, AMD Ryzen 7/9, or higher)
* Minimum 16GB RAM (32GB recommended for deep learning-based detection)
* SSD with at least 500GB storage for logs and historical data
* High-speed network adapters (1Gbps or higher)

## 2.5.2 Software requirements

* Windows 10 operating system
* IDS/IPS tools (Snort, Suricata, Zeek)
* Database management systems (PostgreSQL, Elasticsearch, MongoDB)

## 2.5.3 Network and Security Requirements

* TLS/SSL encryption for secure communication
* Role-Based Access Control (RBAC)

Real-time log collection with SIEM integration

# CHAPTER 3: METHODOLOGY AND MATERIALS

## 3.1 Introduction

The specific steps or methods used to find, pick, process, and evaluate data on a subject are known as research methodology. The methods for gathering data and the materials and tools needed to carry out and examine this project are the next topics covered in this chapter. A proper definition of methodology would be the theoretical examination of procedures appropriate for a given field of study or the collection of principles and practices specific to a particular field of knowledge.

## 3.2 Case study

The purpose of the project is to develop a system approach to monitor Malicious activities and provide network protection. . This case study was conducted at UNIVERSITY OF KIGALI Musanze campus in Musanze District. This study was conducted there in order to analyze common malicious attacks that frequently targets the network system of that campus and propose an updated security system that will monitor all these threats and provide protection to that network system

## 3.3 Data collection

## Design and implementation of an approach to monitor Malcious activities and provide network protection uses a range of data collection strategies that are adapted to the goals of the study. To acquire information on present operations and stakeholder views, these methods include surveys, observations, and interviews. For an extensive review, additional sensor data from integrated IoT devices and documentation evaluation support main data gathering activities

### 3.3.1 Techniques used to collect data

### 3.3.1.1 Documentation

One way to get data from written sources, such as journals, the internet library, and many other sources, is through documentation of the writers' ideas of smart bus stands used for public transportation, they have researched a variety of published materials.

### 3.3.1.2 Observation

The system involves systematically monitoring bus stand activities to collect real-time data on traffic flow, arrivals, and passenger behavior, providing insights into the operational dynamics and effectiveness of the smart bus stand monitoring system.

### 3.3.1.3 Interview

Engage with key stakeholders like bus drivers, stand managers, and passengers to gather qualitative information on operational challenges, user preferences, and monitoring system performance.

### 3.3.1.4 Sampling

Selecting representative buses or time intervals for data collection ensures accuracy and reliability, efficiently gathering data while minimizing resources and time required.

## 3.4 Data analysis

The acquired data will be processed all over the data analysis phase of the smart bus stand monitoring system project to ensure accuracy. While correlation and regression studies will look into factors influencing bus stand operations, qualitative and geographic analysis will be used to highlight patterns and physical interactions.

### 3.4.1 System requirement

**System Requirements** section outlining the necessary hardware, software, and network security specifications for implementing a network protection system.

### 3.4.2 Functional Requirements

To effectively monitor malicious activities and provide network protection, the following functional requirements should be met:

**Real-time Threat Detection:**

Detect and log suspicious network activities instantly.

Identify known and unknown cyber threats using anomaly-based detection.

**Intrusion Prevention System (IPS):**

Block malicious traffic automatically.

Implement dynamic security policies to respond to evolving threats.

**Machine Learning-Based Analysis:**

Train models to classify network traffic.

Continuously update learning algorithms to adapt to new threats.

**Log Management and Reporting:**

Store logs for auditing and forensic analysis.

Generate real-time dashboards and alerts for administrators.

**User Access Control and Authentication:**

Implement multi-factor authentication (MFA) for administrators.

* + Enforce role-based access control (RBAC) to prevent unauthorized modifications.

### 3.5.3Non-Functional Requirements

**Performance**

Ensure low-latency threat detection and response.

Support high network throughput without performance degradation.

**Scalability**

Handle increasing network traffic and threats as the organization grows.

Support distributed deployment across multiple locations.

**Reliability**

Ensure 99.9% system uptime with fault-tolerant mechanisms.

Implement failover strategies to maintain availability.

**Security**

Adhere to industry security standards (ISO 27001, NIST, GDPR).

Encrypt all sensitive data and logs.

**Usability**

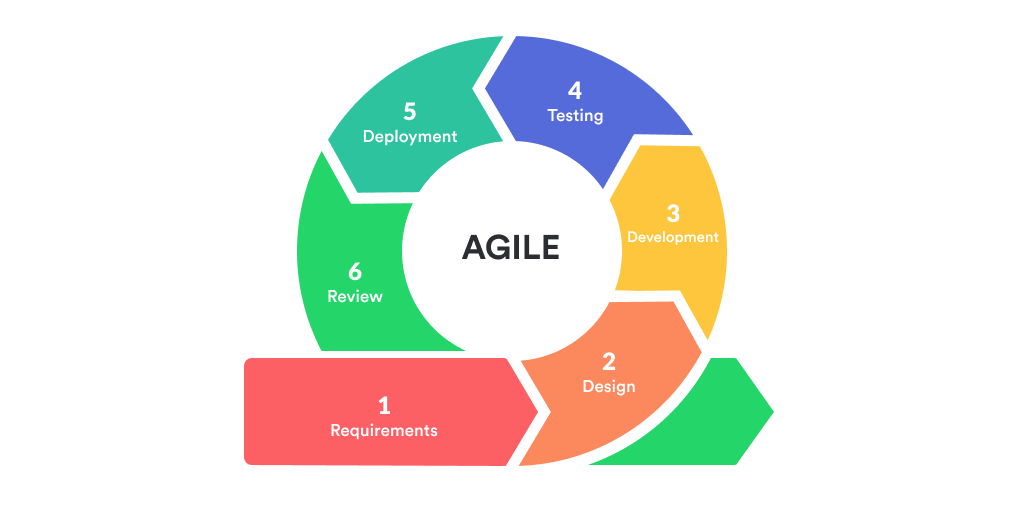
Provide an intuitive dashboard for administrators.

Ensure automated alerting and reporting for security teams.

## 3.6 System development methodology

### 3.6.1 Agile model

Agile model is a combination of iterative and incremental process models with a focus on process adaptability and customer satisfaction by rapid delivery of working software products. Agile Methods break the product into small incremental builds. Each iteration typically lasts from about one to three weeks. The iterative approach is taken and the working software build is delivered after each iteration.



**Figure 12:** Model Agile

### 3.8.2 Planning Phase

Planning is a technique for project planning that uses self-contained work units called revisions or stages to estimate work. This stage establishes a repeatable procedure and specifies the tasks completed in each stages, assisting developers in determining how much work is required.

### 3.6.3 Requirements Analysis Stage

The objective of the IoT-based smart bus stand monitoring system project's requirement analysis phase is to monitors and detect the functionalities of the system. This involves gathering possible system requirements using a variety of methods, such as use case diagrams and flowcharts. This phase's main goals are to identify the problem that the system is meant to solve and to understand the needs of the stakeholders.

### 3.6.4 System Design Phase

Design documents are created to correspond with the requirement specification document during the system design stage of the IoT-based smart bus stand monitoring system project. System design include determining the general system architecture as well as the hardware and system requirements. The goal of this phase is to design a plan for the monitoring system's implementation, making sure that every part is correctly connected and in alignment with the project's goals.

### 3.6.5 Implementation Phase

The goal of the Internet of Things-based smart bus stand monitoring system project is to use communication modules, sensors, and microcontrollers to turn a design into a working system. Software development makes ensuring that integration and operation go smoothly, readying the system for testing and implementation in real situations.

### 3.6.6 Testing Phase

Whenever the project completes, the IoT-based smart bus stand monitoring system will be tested in a testing environment. After confirming system stability, alignment with stakeholders, and functionality, the team repeats until the system is prepared for implementation at a bus stand in reality.

### 3.6.7 Maintenance phase

After all, the previously mentioned phase is over. The next step is to maintain system updates so that users are satisfied, handle faults, and fix any issues that may arise. Updates and changes are important considerations during this maintenance phase.

### 3.6.8 System Phase

The process of defining and arranging a system's modules, components, and interconnections in order to satisfy certain needs and realize planned functionalities is known as system design. It involves drawing up a design or plan for how the system will be put together and how its various components will function.

# Bibliography

Ali, M. (2021). *DDoS detection using NetFlow analytics.* chicago: NYC publisher.

Brown, R. (2020). A Convolutional Neural Network Intrusion Detection Method Based on Data Imbalance. *CNN*, 30-38.

Ghorbani, A. A. (2020). *Network Intrusion Detection and Prevention:.* brunswick: Canadian Institute for Cybersecurity.

Jiang, X. (2010). *Malware Analysis and Detection Engineering.* shangai: network adventures work press.

Patel, K. (2021). *Honeypot-Aware Advanced Botnet Construction and Maintenance.* texas: IET research.

Wrightson, C. E. (2012). *Malware Analysis and Detection Engineering.* chicago: network adventure works press.

Xiang, J. (2015). *Detecting and Understanding Malware Using Machine Learning and Data Analytics.* shangai: shangai book publishers.

Zhang, J. (2021). *Anomaly Detection in Surveillance Scenes Using Autoencoders.* london: Springer Nature portfolio.