INTRUSION PREVENTION SYSTEM USING BANK OF INDUSTRY, LAGOS NIGERIA AS A CASE STUDY

BY

AGU, CHISOM VENORA

16010301030

BEING A PROJECT SUBMITTED IN THE DEPARTMENT OF COMPUTER SCIENCE AND MATHEMATICS, COLLEGE OF BASIC AND APPLIED SCIENCES, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF BACHELOR OF SCIENCE

MOLUNTAIN TOP UNIVERSITY

IBAFO, OGUN STATE

NIGERIA

November, 2020

CERTIFICATION

This Project titled, **INTRUSION PREVENTION SYSTEM USING BANK OF INDUSTRY, LAGOS NIGERIA AS A CASE STUDY,** prepared and submitted by **AGU, CHISOM VENORA** in partial fulfilment of the requirements for the degree of **BACHELOR OF SCIENCE (Computer Science),** is hereby accepted

_____ (Signature and Date)

Supervisor's name and initials

Supervisor

Accepted as partial fulfilment of the requirements for the degree of BACHELOR OF SCIENCE (Computer Science)

_____ **(Signature and Date)**

Dr. Akinyemi, I. O.

Head of Department, Department of Computer Science and Mathematics

_____ **(Signature and Date)**

Prof. Akinwande, A. I.

Dean, College of Basic and Applied Sciences

DEDICATION

This Project is dedicated to God Almighty

ACKNOWLEDGEMENTS

The success and outcome of this project goes to the Almighty God for wisdom, understanding and divine help to me from the beginning to the completion of this work. I specially appreciate my major supervisor Dr.Kasali F. A. who took keen interest in my project work and guided me all along, and taking the pains out of no time to attend to me. My gratitude goes to Dean, College of Basic and Applied Sciences Prof. Akinwade A. I. for his teachings, guidance, counsel and fatherly support in ensuring the successful completion of this research God bless you Sir. My heart-felt gratitude goes to the Head of Department Computer Science and Mathematics Dr. Akinyemi I. O. for his fatherly role, and owe deep gratitude for the efforts, constant encouragement, guidance and support of all staff members of the department of Computer Science and Mathematics: Dr. Oyetunji M. O., Dr. Adamu O. B, Dr. Alaba O. B., Dr. Mathew O. A., Dr. (Mrs.) Olaniyan O. O., Dr. Peter A. I., Dr. Okunoye O. B., Dr. Ojesanmi O. A., Dr. (Mrs.) Florence A. O., Mr. Taiwo A and other members of staff.

I acknowledge the constant support of my mentor who had contributed to my academic achievement. Who is no other but Mr Sarumi. I pray God would continue to increase your knowledge. I will forever be grateful to my parents Mr. and Mrs. Agu. who sacrificed wealth and enjoyable moments of their lives for the sake of my success; and my siblings – Lotanna, Kossi, and Triumph for their prayers. I would not forget to remember all the students in the Department of Computer Science and Mathematics, and Mountain Top University colleague and friends for their prayers, support, and help in one way or the other for making my stay a worthwhile one, I say God bless you all richly. God bless them all greatly.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The file server offers users convenience. It overcomes the traditional and tedious way of storing and searching for files. This system therefore increases the speed and standardization of the staff. It offers a better platform for sharing files. The file server has only one person (super admin) who is fully authorized to modify or update files to prevent intrusion. The super admin can monitor the login activities of the users, also block and unblock users, upload and delete files. This system allows the admin to create staff accounts using the company mail to enable them access to files pertaining their respective departments. Confidential and sensitive information are secure, due to the fact that only the super admin has access to the central archive to upload files on the file server An id and password are provided for each user. Therefore, it provides a sense of security for the users.

The structured methodologies have been chosen to develop the File Server. The structured design methodology adopts a formal step-by-step approach to the System Development Life Cycle that moves logically from one phase to the next. The methodology used involved system analysis, system design, system development, and system testing. The system design will be achieved using HTML, CSS AND JavaScript for the frontend and PHP and SQLite for backend design.

It was concluded that the File server system improves the process of sharing files, thus reducing the time wasted as well as the errors that are involved in the manual process. The File Server system is indeed a very promising solution for the handling of confidential information and should be undoubtedly patronized.

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

IPS is a modern technology that provides security for computer systems with new features that are effective in facing threats. Intrusion prevention system (IPS) is considered as the next step in the evolution of intrusion detection system (IDS). IPS is a software or hardware that has the ability to detect attacks whether known or unknown, and prevent the attacks. IPS can also be described as a network security device that monitors network and/or system operations for unwanted activity and can interact to prevent those activities. (Abdelkarim & Nasereddin, 2011)

IDSs are passive techniques. They typically notify the systems administrator to investigate further and take the appropriate action. The intrusion prevention system (IPS) seeks to combine the traditional monitoring and analysis functions of an IDS with more active automated responses, such as automatic reconfiguration of firewalls to block an attack. An IPS aims for a quicker response than humans can achieve, but its precision relies on the same techniques as the traditional IDS. (Vacca, 2014)

Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) also analyzes packets, but can also stop the packet from being delivered depending on what kind of attacks it detects, helping stop the attack. The biggest difference between them is that IPS is a control system, while IDS is a monitoring system. IPS prevents the packet from being transmitted depending on the contents

of the packet, much like how a firewall prevents traffic by IP address, whereas IDS doesn't stop the network packets in any way. (Petters, 2020)

An Intrusion Prevention System (IPS) is a framework that screens a network for malicious activities, for example, security dangers or policy compliance.

Typically, vulnerability exploits come in the form of malicious inputs to an objective application or resources that the attacker uses to block and pick up control of an application or System. Intrusion prevention systems are considered increment, since they both screen system activities for malicious activity and the network traffic.

The fundamental contrasts are, dissimilar to an Intrusion detection system, Intrusion prevention systems are set in-line and can effectively anticipate or impede intrusions that are recognized. (Gurubaran, 2019)

1.2 Statement of the Problem

The following problems were identified in the existing system that necessitated the development of the intrusion prevention system: Absence of an intrusion prevention system for files, Insecurity of sensitive organization information, Low level of file security.

1.3 Aim and Objectives of Study

The aim of this project is to develop a System that will implement Intrusion Prevention with the following objectives:

(1) To design a system that will encrypt information pertaining to customers' and staff to prevent intrusion.

(2) To develop a system that will give full access to admin to prevent intrusion.

(3) To implement a system that will prevent disclosure of customers' and staff data to fraudsters by utilizing cipher text.

1.4 Significance of the study

This study is significant in the following ways:

a. It will help deter unauthorized people (intruders) from gaining access to customers' financial details.
b. It will help to tighten the degree of protection of the company.
c. The study will show how encryption can be implemented to avoid access to customer information from intruders.

d. For other researchers pursuing relevant information, the analysis will serve as a valuable reference material.

1.5 Scope of the Study

This study covers Intrusion Prevention System using **B**ank of industry, Lagos Nigeria as a case study. It is limited to the use of encryption of cipher text to prevent intruders from gaining access to clients' vital information.

1.6 Organization of the Research

This research work is organized into five chapters, chapter one deals with the implementation of the research study and presents the preliminary, theoretical context, and statement of the study's issue, intent and goals, importance of the study, scope of the study, and research organization, limitation of the study, and definition of words.

Chapter two focuses on the literature review; contribution of other scholars on the subject matter is discussed.

Chapter three contains the system analysis and the design, it presents the research methodology used in development of the system, it analyses the present system to identify the problems and provide information on the merit of the proposed system. The system design is also presented in this chapter.

Chapter four present the system implementation, the choice of programming language used, and system requirement for implementation

Chapter five, this chapter focuses on the summary, conclusion and recommendation are also contained in this chapter based on the study carried out.

1.7 Definition of Terms

Detection is the extraction of particular information from a larger stream of information without specific cooperation from or synchronization with the sender.

Intrusion: It is an unconstitutional act to take ownership of the property of another person.

Password: A special code that the user uses to gain access to a database or analysis.

Security: protection, freedom danger.

Files: The set of documents that are logically linked.

Prevention: Maintenance performed to stop fault occurring or developing into major detects.

Codes: To write a computer program by putting one system of number, words, symbols into another system.

System: A group of interdependent items that interact regularly to perform task

Packets: The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The chapter presents an overview of computer threats and some of the techniques employed against intrusion. IPS types and approaches are also discussed.

2.1 Overview of IPS

A network intrusion is any unauthorized activity on a computer network. Detecting an intrusion depends on the defenders having an understanding of how attacks work.

An intrusion prevention system (IPS) is a form of network security that strives to detect and prevent identified threats. Intrusion prevention systems incessantly monitor the network, looking for possible malicious incidents and capturing information about them. The IPS reports these incidents to system administrators and takes provocative measures, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to detect issues with corporate security policies, deterring staff and network visitors from violating the rules these policies contain.

An intrusion prevention system is typically configured to use a number of different approaches to protect the network from unauthorized access. These include:

1. Signature-Based - The signature-based approach uses predefined signatures of well-known network threats. The system takes necessary action, when an attack is initiated that matches one of these signatures or patterns

2. Anomaly-Based - The anomaly-based approach monitors for any irregular or unexpected behavior on the network. If an anomaly is found, the system blocks access to the target host instantly.

3. Policy-Based - This method requires administrators to configure security policies according to organizational security policies and the network infrastructure. When an incident occurs that violates a security policy, an alert is triggered and delivered to the system administrators.

2.1.1 Principles of Intrusion Detection and prevention system

Intrusion detection and prevention is a software application that monitors network or system activities for malicious activities or policy violations and reports to a management station. Intrusion detection is the process of monitoring the events occurring in a computer system or network (NIDS) network intrusion detection system would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic. However, doing so might create a bottleneck that

would impair the overall speed of the network. OPNET and Netsim are commonly used tools for simulation network intrusion detection systems (Anderson & Ross,2001). (IDPS) intrusion detection and prevention system are network security appliances that monitor network or system activities for malicious activity. The functions of intrusion prevention systems are to identify malicious activity. Log information about this activity report it and attempt to block or stop it. NIST-guide to intrusion, detection and prevention system (IDPS) February 2007.

2.2 Overview of Computer Threats

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself (CNSS, 2010). The attacks could come in the form of viruses, Denial of Service (DoS), Distributed Denial of Service (DDoS), various types exploitations, worms or even physical attack on the computer hardware.

2.2.1 Types of threats

1. Computer virus

Computer viruses are pieces of software that are designed to be spread from one computer to another. They're often sent as email attachments or downloaded from specific websites with the intent to infect the computer and other computers on the contact list by using systems on the network. Viruses are known to send spam, disable the security settings, corrupt and steal data from the computer including personal information such as passwords, even going as far as to delete everything on the hard drive.

2. Phishing

Phishing is a method of a social engineering with the goal of getting sensitive data such as passwords, usernames, credit card numbers. The attacks often come in the form of instant messages or phishing emails designed to look legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient's computer. It can also attain personal information by sending an email that appears to be sent from a bank, asking to verify the identity by giving away the private information.

3. DoS/DDoS attacks

Attackers launch an attack on enterprise network server by flooding it with a large number of connection requests which appear authentic to the server. If the number of such connection requests exceed the server request rate, it would prevent the genuine users from accessing the server. This is called a Denial of Service (DoS) attack. In a Distributed Denial of Service attack, attackers place malicious code on lot of individual computers and use them to simultaneously launch DoS attacks from various locations.

4. Man-in-the-middle attacks

Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to eavesdrop on communication between two targets. It can listen to a communication which should, in normal settings, be private. As an example, a man-in-the-middle attack happens when the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attacker's public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferred back to person A, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets. Here are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking

5. Computer worm

Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer's contacts, then immediately to the contacts of the other computers. A worm spreads from an infected computer by sending itself to all of the computer's contacts then immediately to the contacts of the other computers. Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities. (SECURITYTRAILS, 2018)

6. IP Fragmentation

Programs like Flag route intercepts modifies and rewrites egress traffic destined for a specific host thereby perpetuating an attack.

7. Port Scanning

This is an attempt by the attackers to find out which ports are open on a specific host or multiple hosts on the network by scanning different ports. Once this information is obtained, attacks for known vulnerabilities for these services are tried.

2.3 Necessity of Intrusion Prevention Systems

Network intrusion prevention systems are security controls designed to monitor and analyze network traffic for malicious activity or for other actions that violate an organization's security policies. Unlike an intrusion detection system, network intrusion prevention systems are capable of dropping or blocking network connections that are determined too risky for the organization.

IPS capabilities provided through hardware or virtual appliances tend to be used by larger organizations. Compared to other network intrusion prevention systems, appliance-based IPS tends to be more expensive in terms of product acquisition and deployment, but there are often strong justifications for these higher costs. For example, a large organization may need to distribute the IPS workload across many devices for performance reasons, such as to avoid overloading one network security device with enormous volumes of traffic. Smaller organizations are more likely to use integrated IPS (such as enabling IPS features in a next-generation firewall) or cloud-based IPS over hardware or virtual IPS appliances because of cost and convenience. (Scarfone, 2015)

IPS technologies provide several benefits to organizations. This are three of the most significant benefits:

- Detects and stops attacks that other security controls cannot;
- Supports customization of detection capabilities to stop activity that is only of concern to a single organization; and
- Reduces the amount of network traffic reaching other security controls, which both lowers the workload for those controls and protects those controls from direct attacks.

2.3.1 Unique capabilities for detecting and stopping attacks

The main benefit provided by network intrusion prevention systems is the ability to detect and stop a variety of attacks that cannot be automatically identified by firewalls, antivirus technologies and other enterprise security controls. IPS technologies use a combination of several methodologies for detecting attacks. Each methodology has its own strengths and weaknesses, so by leveraging the strongest capabilities of each methodology, an IPS can detect an incredibly wide range of attacks.

This is particularly important when it comes to attacks that have never been seen before. Such attacks cannot be detected using signature-based detection methodologies, which are the basis for many other network security controls. IPS technologies can establish baselines of normal activity based on continuous monitoring over time; subsequent deviations from these baselines can indicate attacks. This is especially helpful at identifying distributed denial-of-service attacks, but it can also recognize malware infections within the organization by the anomalous patterns of network activity they can cause, for example.

Another distinguishing feature of network intrusion prevention systems, is they usually have a thorough understanding of applications. Most network security controls can parse and analyze Web and email activity to some extent, but they lack knowledge of the individual applications carried within Web traffic, as well as application communications carried via non-Web traffic. This greatly limits their efficacy in the detection of application-borne attacks. An IPS product usually has knowledge of hundreds, if not thousands, of applications, and this provides unique attack detection capabilities involving applications.

In addition to all of these detection capabilities, some IPS products offer support for detecting and stopping even more forms of attacks. For example, an IPS may offer a feature similar to application whitelisting, which limits which executables can be run. Similarly, an IPS may receive threat intelligence feeds or reputation information, enabling the IPS to block IP addresses, websites, URLs or other entities based on their behavior in the recent past. Some network intrusion prevention systems can also perform advanced, comprehensive analysis of files being transmitted via network communications to identify anomalous behavior associated with using or executing these files. This is useful for stopping both known and unknown forms of attack.

2.3.2 Organization-specific detection capabilities

Another significant advantage of network intrusion prevention systems, is they can readily be customized by the organization in order to detect attacks and other activity that is specifically of interest to the organization only. An instance is the use of a particular application that violates the organization's policies. Another example is the identification of a phishing attack that is specific to the organization. Because a network intrusion prevention system can support detection of attacks within so many applications, it provides a single point for security administrators to define a broad range of attacks, misuse and other undesirable activity.

This is especially effective because of the numerous detection methodologies a network intrusion prevention system supports. A security administrator who is searching for a known attack, such as a unique phishing email, can easily write a simple signature for the IPS to identify any instances of this email. If a more sophisticated attack is to be stopped, the security administrator could configure the IPS to alert when complex patterns of application activity are observed. The degree to which an IPS supports such customization varies from product to product, but nearly every IPS offers at least some customization for its attack detection features.

2.3.3 Protection of other enterprise security controls

Intrusion prevention systems can provide protection for the availability and integrity of other enterprise security controls. For instance, an IPS deployed in front of another enterprise security control can analyze the incoming network traffic and block suspicious activity from reaching that security control. In certain situations, this can protect the security control from being directly attacked by detecting and stopping the attack, preventing it from ever reaching its target. In other cases, this can prevent an attacker from circumventing the security control by specially crafting their activity at the application layer, network layer or elsewhere to avoid detection by other security controls.

More frequently, network intrusion prevention systems protect other security controls by assisting them in their workload. By strategically deploying IPS sensors in front of other security controls, an organization can reduce the amount of traffic reaching those controls. This, in essence, decreases the risk that they will be overwhelmed by high volumes of traffic, causing

traffic to be slowed or even dropped altogether because of a lack of processing or network resources.

2.4 Types of Intrusion Prevention System

2.4.1 Host-based IPS

Host-based intrusion prevention systems are used to secure both servers and workstations through software that runs between the system's applications and OS kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HIPS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HIPS monitors activities such as application or data requests, network connection attempts, and read or write attempts to name a few.

Historically HIPS and firewalls are closely related. Where a firewall regulates the traffic to and from the computer based on a rule set, HIPS do more or less the same, but for the major changes made on the computer.

HIPS solutions protect the computer against known and unknown malicious attacks. In case of attempted major changes by a hacker or malware, HIPS blocks the action and alerts the user so an appropriate decision about what to do can be made. What does the HIPS consider major changes? Take control of other programs. For example, sending a mail using the default mail client or sending the browser to a certain site to download more malware.

- Trying to change important registry keys, so that the program starts at certain events.
- Ending other programs. For example, the virus scanner.
- Installing devices or drivers, so that they get started before other programs
- Inter process memory access, so it can inject malicious code into a trusted program. (Arntz, 2013)

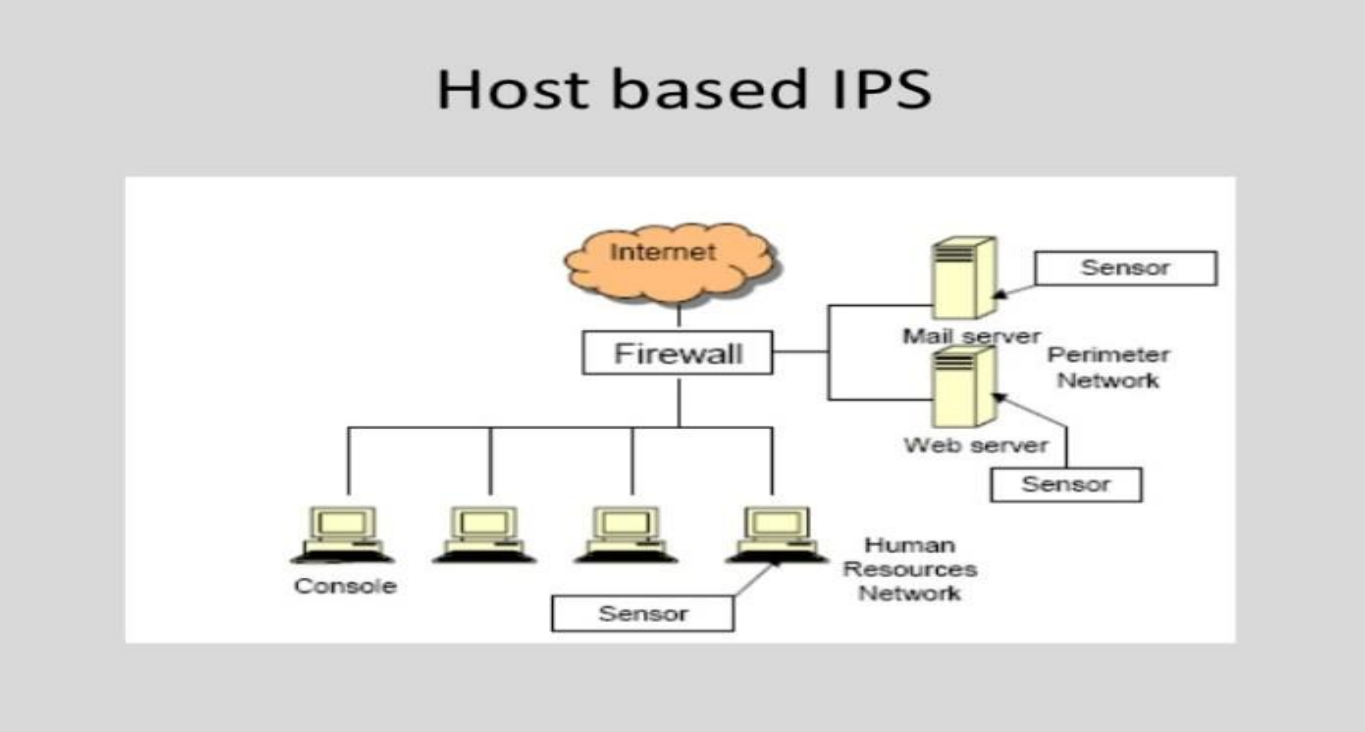

Figure 2.1: Host-based IPS (Gurubaran, 2019)

2.4.2 Network Based Intrusion Prevention System

A solution for network-based protection is network-based intrusion prevention systems (often called inline prevention systems). NIPS can intercept all network traffic and monitor it for suspicious behavior and incidents, should it be considered legitimate traffic, either blocking the requests or moving it along. Network-based IPSs operate in several ways. Usually, package- or software-specific features decide how a particular NIPS solution operates, but usually, it is expected that intrusion signatures should be checked for, protocol irregularities should be looked for, also identify commands that are not commonly executed on the network, and more. (Beal, 2005)

A network-based intrusion prevention system (NIPS) is a system used to monitor a network as well as protect the confidentiality, integrity, and availability of a network. Its main functions

include protecting the network from threats, such as denial of service (DoS) and unauthorized usage.

The NIPS monitors the network for malicious activity or suspicious traffic by analyzing the protocol activity. Once the NIPS is installed in a network, it is used to create physical security zones. This, in turn, makes the network intelligent and quickly discerns good traffic from bad traffic. In other words, the NIPS becomes like a prison for hostile traffic such as Trojans, worms, viruses, and polymorphic threats.

An intrusion prevention system (IPS) sits in-line on the network and monitors the traffic. When a suspicious event occurs, it takes action based on certain prescribed rules. An IPS is an active and real-time device unlike an intrusion detection system, which is not inline and is a passive device. IPSs are considered to be the evolution of the intrusion detection system. (Techopedia, 2020)

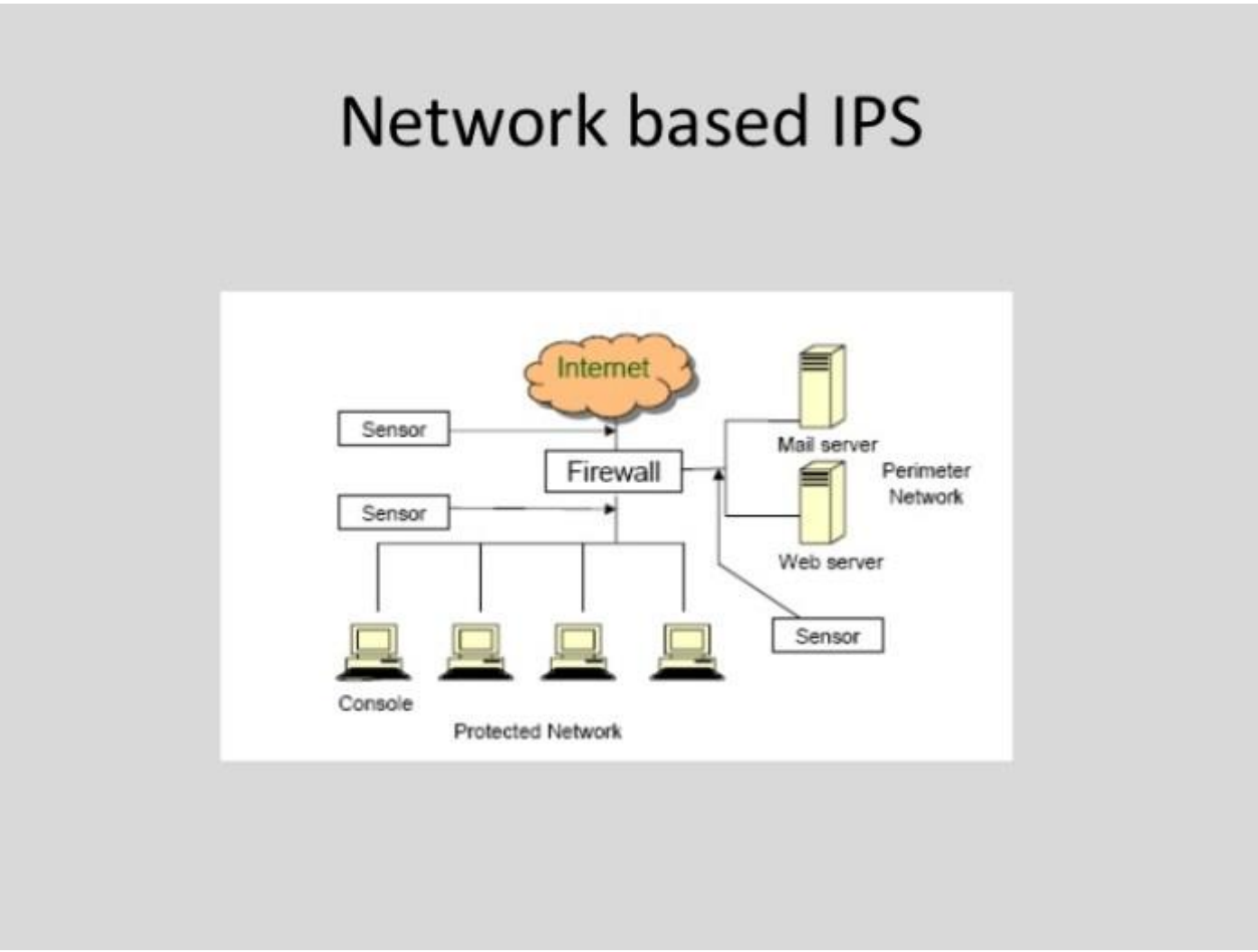

Figure 2.2: Network based IPS (Gurubaran, 2019)

2.5 Issues that every IPS should address

An intrusion prevention system (IPS) includes all the features of an intrusion detection system but also has the ability to act upon malicious traffic. As the IPS normally sits in line with network traffic, attacks can be shut down, typically by blocking access from the attacker or blocking access to the target. In some cases, the IPS can talk to the firewall to block an attack. (Lerner, 2012)

1) IDS, IPS and hybrid modes: The IPS should be multifunctional so that it can be deployed depending on the exact need. In the IDS mode, the device is passively monitoring network traffic. In the IPS mode, the device is configured in the traffic path. By submitting resets or demanding a firewall or inline IPS to separate the segment from other networks using blacklisting, IDS and IPS should both be able to limit traffic. The IPS mode is also effective in blocking attacks if you can identify a clear threat path -- for example, traffic from the Internet to a DMZ segment. In the hybrid mode, the same device is configured to function in both modes and using the same device in both modes is an efficient and cost-effective solution for smaller implementations.

2) AET protection: Advanced evasion techniques (AETs) are true and are presently used by NSS Labs and other organizations to test security vendor products. In its latest report, Verizon said that in 31% of attacks against large organizations, an attack vector remained unknown. Analyzing AETs requires inspecting and normalizing all data streams, but 95% of organizations are not doing that. Most current security devices cannot flag or log AETs separately. At best, they may report irregularities or suspicious traffic.

It's crucial not to confuse an exploit with the method. Stuxnet becomes visible when it reaches the target; it stays there and is easy to investigate once the code is isolated and recognized. AETs can be analyzed if the IPS records all traffic, not just what is logged by the security devices. Ask the IPS vendor what its strategy is for dealing with AETs.

3) Event correlation: Event correlation helps to minimize false positive events and provide accurate protection for network services and intranet users. Event correlation looks at log data from one or more sensor engines, looking for malicious event sequences, preferably in real-time. Event compression cleans repetitive log events and minimizes the bandwidth requirements from remote offices back to the data center. A good event correlation engine can alert the IPS to isolate an attacker or network worm on all firewall and IPS engines simultaneously, mitigating the damage to network services and clients.

4) Web filtering: A great enhancement for the IPS is Web filtering, which provides multiple advantages such as enhanced security by preventing access to known malware and phishing sites, as well as improved work efficiency and bandwidth utilization by blocking access to unwanted websites. Advanced Web filtering systems can offer plenty of options, such as blacklists and whitelists where there are set rules for the whole network. Reports of Web browsing habits and activities can also be produced.

5) SSL inspection: SSL inspection is important in ensuring that no attacks, viruses or other unwanted content can enter or exit the organization's network by disguising itself within the encrypted HTTPS channel. SSL inspection gives administrators the ability to monitor traffic inside the TLS/SSL encryption and detect and react to any unauthorized content. The IPS should have a controlled way to open the encryption in the network and to submit the encrypted traffic for the same inspection as the clear-text HTTP data, eliminating this

6) Denial-of-service protection: IPS should provide protection against illicit input and traffic flood DoS (denial of service) attacks without affecting legitimate network traffic. Connection flood or Web service starvation attacks are typical examples of distributed DoS (DDoS) attacks. TCP SYN flood attacks are stopped by blocking the incoming connection attempts from spoofed address sources under an attack and preventing them from reaching the target system. The IPS must quickly detect the spoofed connection sources and block them, while allowing valid user connections to pass through. UDP flood DoS attacks are controlled by rate limiting the incoming UDP datagrams against the protected Web service.

7) Central management capabilities: Central management is important for IPS security because it allows the manipulating of systems without having to manually touch every single remote location to make a change. Central management usually allows the monitoring and

managing of appliances and components with options that may include alerts, security content updates, appliance updates, firewall and intrusion prevention settings. As a result, there is less administrative time devoted to network security, incident and log management operations and the integration with other security components to enforce immediate threat mitigation policies or software updates.

8) Performance: IPS could affect the network if it is not implemented properly or if the IPS product is poorly architected. Look for the ability to use clustering to share processing connections, thus improving performance and decreasing downtime. The deployment of the components of the IPS could also minimize the risk of the performance deteriorating. The IPS should capture and analyze traffic, so it is best to separate the analysis component onto a dedicated system. Ask the IPS vendor how to best deploy the IPS with the least impact on the network performance. Also, ask about how signatures and other context information are analyzed to see if performance is an issue.

9) IPv6 ready: Major operating systems and core networking components offer IPv6 support. For instance, Windows Vista uses IPv6 addresses by default, which may be a potential security threat without properly implemented access control and deep inspection. In addition, malicious traffic may be hidden inside IPv6 and IP-in-IP tunnels, which many security solutions still fail to protect.

Make sure the IPS provides stateful access control and full deep inspection capabilities for IPv6 network traffic, including IPv6 encapsulation, IP-in-IP and GRE tunneling protocols.

10) Integration with the firewall: The essence of a next-generation firewall is the ability to interact with an intrusion prevention system. The integration of these capabilities can either be within a single system or separate, but be aware of issues that can occur around reporting, throughput and management.

CHAPTER THREE

RESEARCH METHODOLOGY, DESIGN AND ANALYSIS

3.0 Introduction

This chapter focused on the research methodology the methodology used in the development of the proposed system is the spiral model methodology, system analysis and design being used, the system analysis which include system design, system architecture, input layout, output format, analysis of the existing system, problem of the existing system, analysis of the proposed system, advantages and disadvantages of the proposed system and functional and non-functional requirements.

3.1 Research Methodology

The methodology employed for the development of the system is the spiral model. A software development methodology or system development methodology is a framework that is used to structure, plan and control the process of developing an information system. The spiral development model comprises the elements of both design and prototyping. The model has four stages namely: Planning, Analysis, Evaluation and Development. Also, the data used for the development of the research was gotten from the internet, textbooks, and articles. The contributions of other experts on the subject were examined to gather relevant information. The case study also provided useful information for the development of the system.

3.2 System Analysis

The term system analysis entails examining a system in order to understand its step by step operation so as to identify its benefits and areas of limitation that required improvement.

3.2.1 Analysis of the Existing System

The present system for intrusion prevention in the Bank of industry is reliable but restricts file sharing manually e.g through USB, flash drive e.t.c. Therefore, resorts to file sharing and storing the old-fashioned way.

3.2.2 Problem faced by the Existing System

The following are the problems associated with the existing system:

1. Due to the old-fashioned way of storing files it is exposed to physical damage
2. It is tedious to find files
3. The physical storage of files is very ambiguous.

3.2.3 Analysis of the Proposed System

The proposed system is a file server that prevents intrusion in the sense that only the admin has full control of the system and is able to make changes.

3.2.4 The Advantages of the Proposed System

- **i.** It will help to save time compared to the existing system.
- **ii.** It will help to reduce intrusion to users' data.
- **iii.** It will create convenience and user friendliness to the users.

3.2.5 The Disadvantages of the Proposed System

i. The system gives access to modify or make updates to only one person (super admin)

The system has been developed on the following requirements:

3.2.6 Functional Requirements

The following requirements were captured for the intended use of the system.

1. **Staff account:** The added staff can see files addressed to their department.
2. **Creation of new customer account:** When there is a new customer he should fill the form containing field like Name, Address, and Phone No.., and also Email address and Password.
3. **Creation of new staff account:** A company email is created for a new staff, which is used by the admin to create an account for the staff.
4. **Monitoring and conducting routine checks on staff activities:** The admin can monitor login activities of the staff and customers, also the admin has the site role/permission to block and unblock the users.
5. **Uploading of files:** The admin can upload specific departmental files from central archive which is cloud based.

3.2.7 Non-Functional Requirements

The application was designed to fulfil the following non-functional requirements.

1. **Performance Requirements:** Performance of the system is dependent on the bandwidth of the internet and also the hardware itself.

2. **Security Requirements:** There is only one authorized person who can see the confidential Information. The information of the staff is only available for the administrator.

3. **Software Quality Attributes:** The system is user friendly, interoperable and flexible

3.2.8 System Implementation

This included assembling or building different components of a framework for instance SQLite for database Xampp Server for facilitating the site pages. This is the phase wherein the genuine framework was perceived. The specialized engineering characterized in the structure stage was the gauge for building up the framework. The interface product structured utilizing HTML, CSS, JavaScript and Bootstrap content languages. This is on the grounds that these languages gave gigantic agreeable UIs; that is anything but difficult to learn and reasonable. The database was planned in SQLite basing on Xampp Server programming. SQLite gives a typical state of security to the database, that is, confirmation which can either be amid the signing in to the database or on DML directions, for example, erase, include or even alter, it additionally diminishes repetition.

3.3 System Design

The system design is the step that is followed in breaking down of how the new system functions or how it is being operated. System design includes the following:

a) Input Design
b) Database Structure
c) Activity Diagram
d) Use Case Diagram
e) System Architecture

3.3.1 Input Design

This was the input acknowledgment of input structure. Tables, structures and reports were made and connections characterized among these tables and security compels set. Amid the physical plan the scientist made an interpretation of the schemas into genuine database structures and as of now, he needed to outline:

- Entities to tables.
- Relationship to foreign key constraints.
- Attribute to column primary unique identifiers to primary key constraints.
- Unique identifier to unique key constraint.
- Attributes to columns.

3.3.2 Database Structure and Design

Column Name	*Data Type*	*Nullable*	*Size*
Admin_id	Int	No	12
Name	Varchar	Yes	100
Username	Varchar	Yes	60
Password	Varchar	Yes	60
Email	Varchar	Yes	100
Last_login	Datetime	Yes	60
Role	Varchar	Yes	60

Status	Tinyint	Yes	1

Table 3.1: ADMIN TABLE

Column Name	*Data Type*	*Nullable*	*Size*
Customer_id	Int	No	1
Name	Varchar	Yes	100
Address	Varchar	Yes	100
Email	Varchar	Yes	60
Phone no.	Varchar	Yes	60
Password	Varchar	Yes	60

Table 3.2: CUSTOMER TABLE

Column Name	*Data Type*	*Nullable*	*Size*
Staff_id	Int	No	1
Name	Varchar	Yes	100
Address	Varchar	Yes	100
Email	Varchar	Yes	60
Phone no.	Varchar	Yes	60
Password	Varchar	Yes	60

Table 3.3: STAFF TABLE

Database design

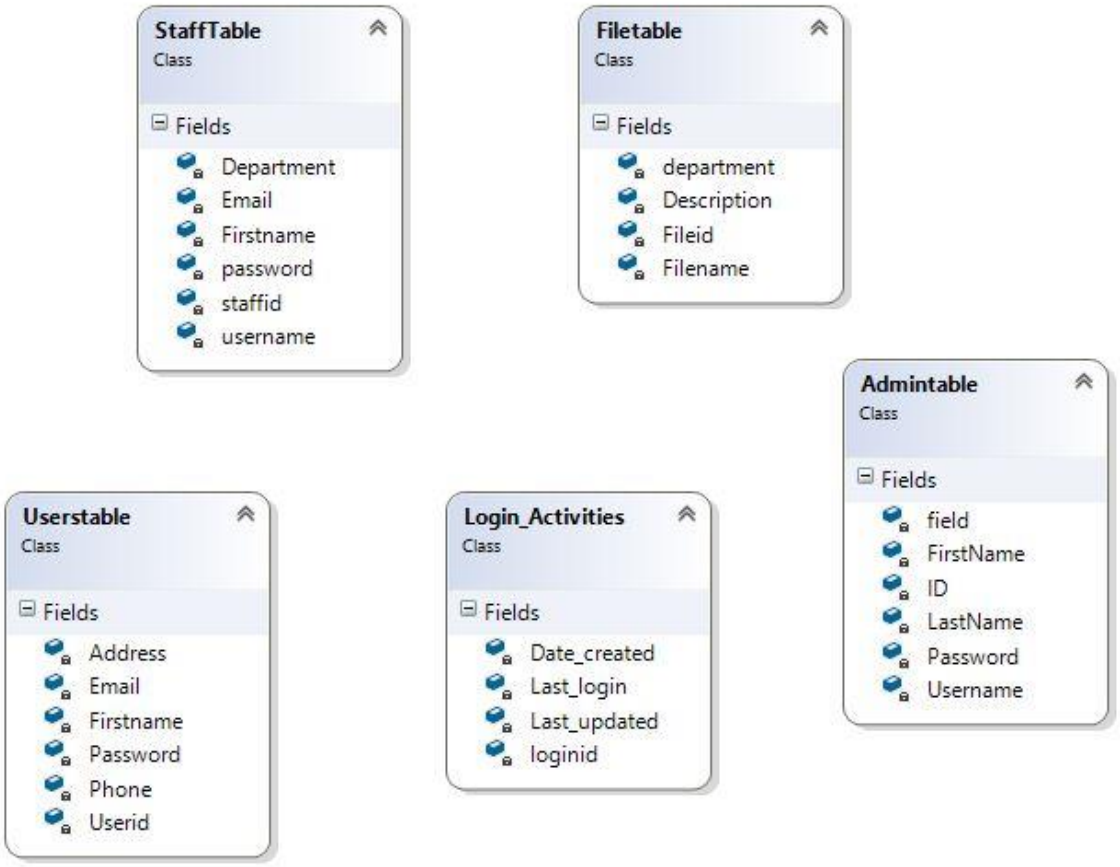

Figure 3.1: Database Design

3.3.3 Activity Diagram

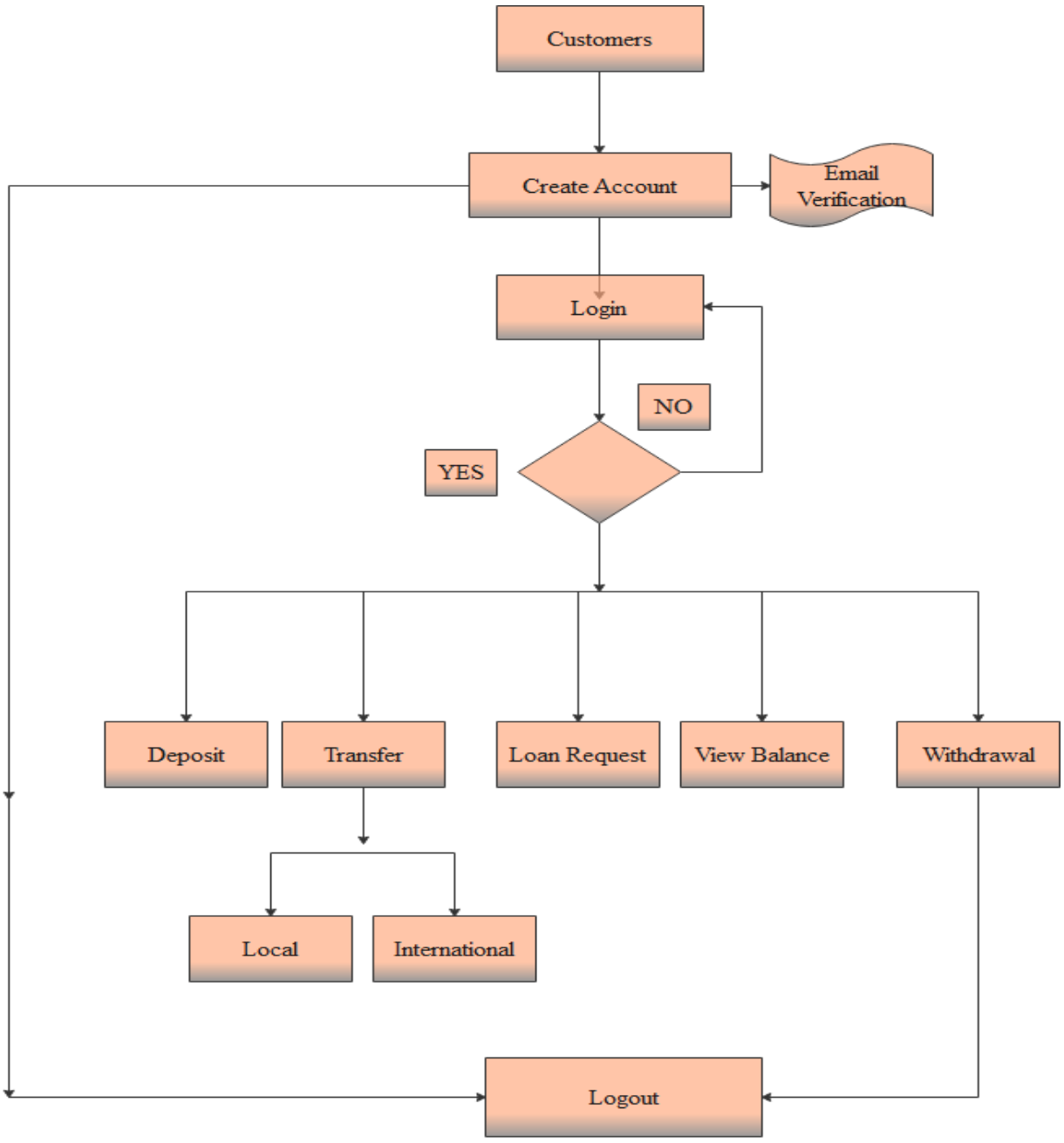

Figure 3.2: Customer Activity diagram

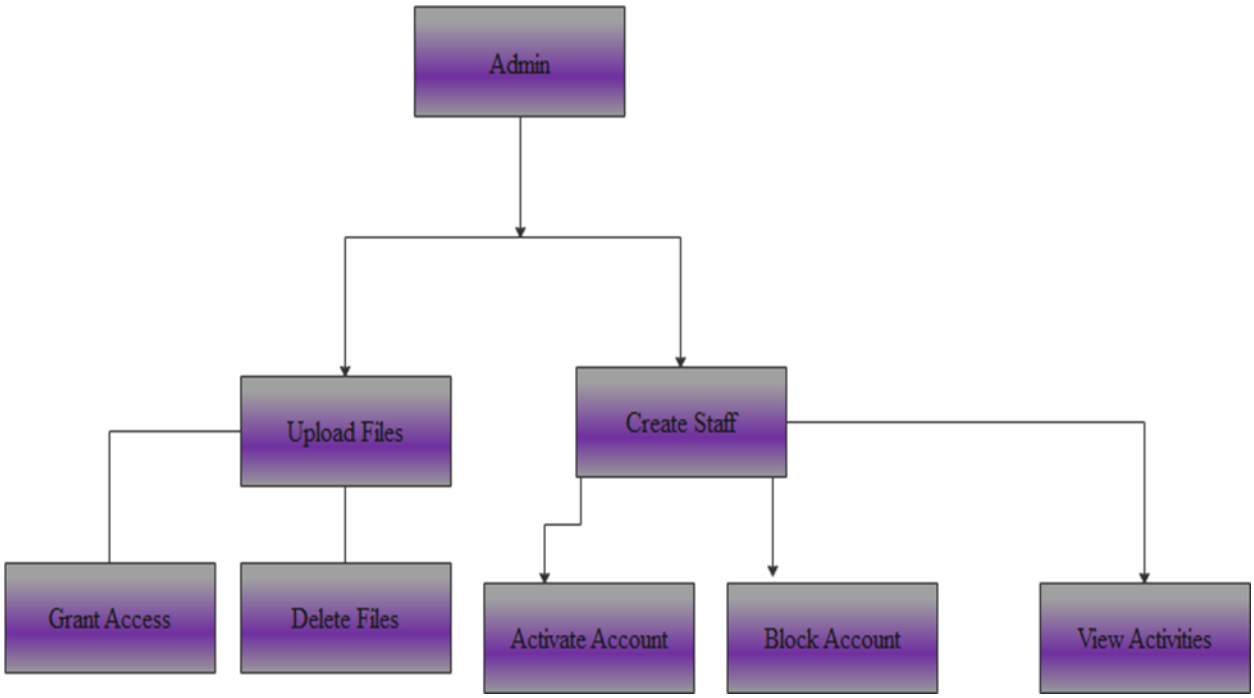

Figure 3.3: Administrator Activity diagram

3.3.4 Use case diagram

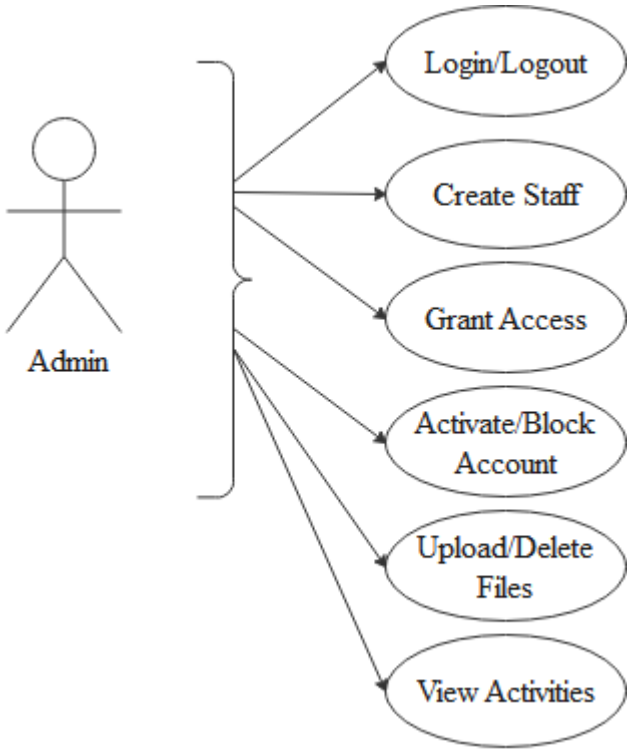

Figure 3.4: Administrator Use Case Diagram

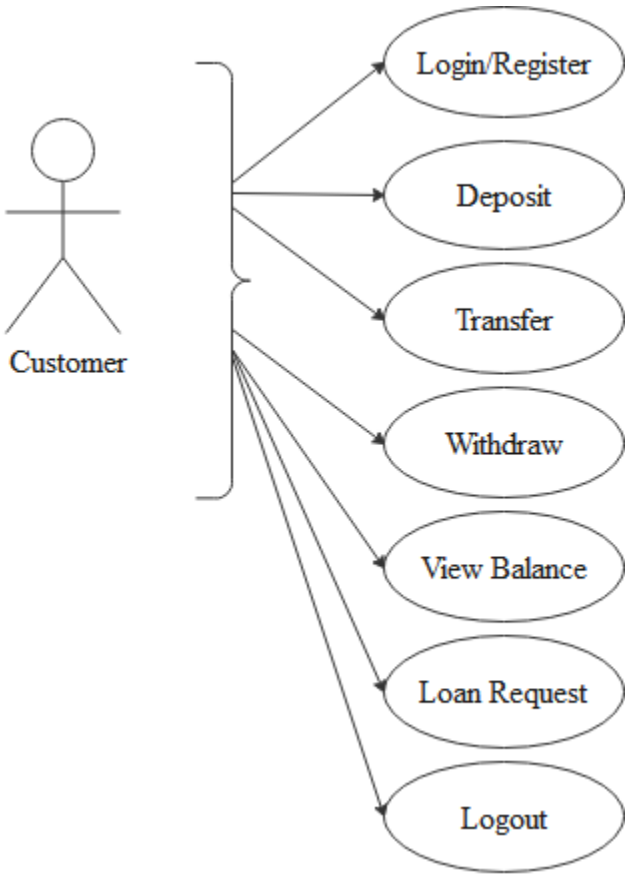

Figure 3.5: Customer Use Case Diagram

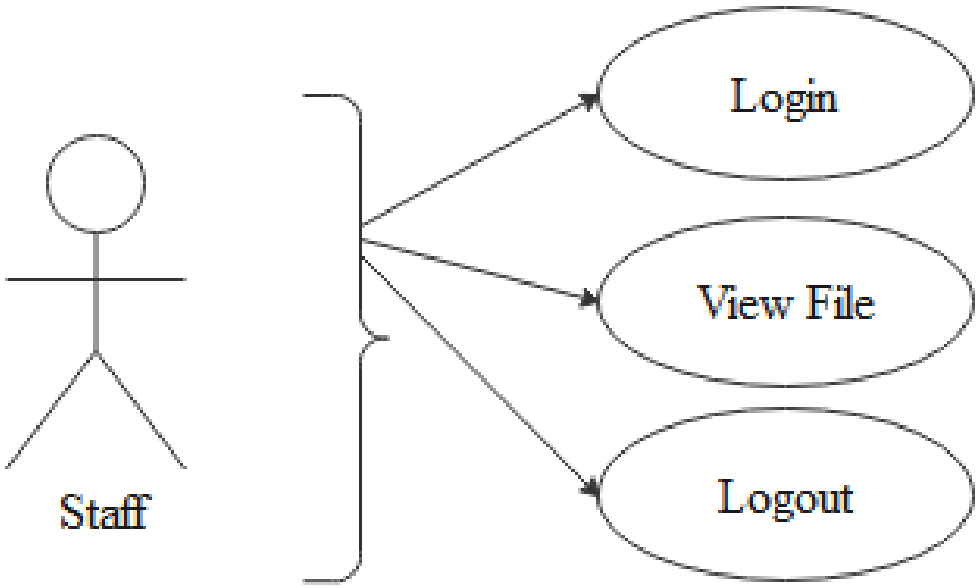

Figure 3.6: Staff Use Case Diagram

3.3.5 System Architecture

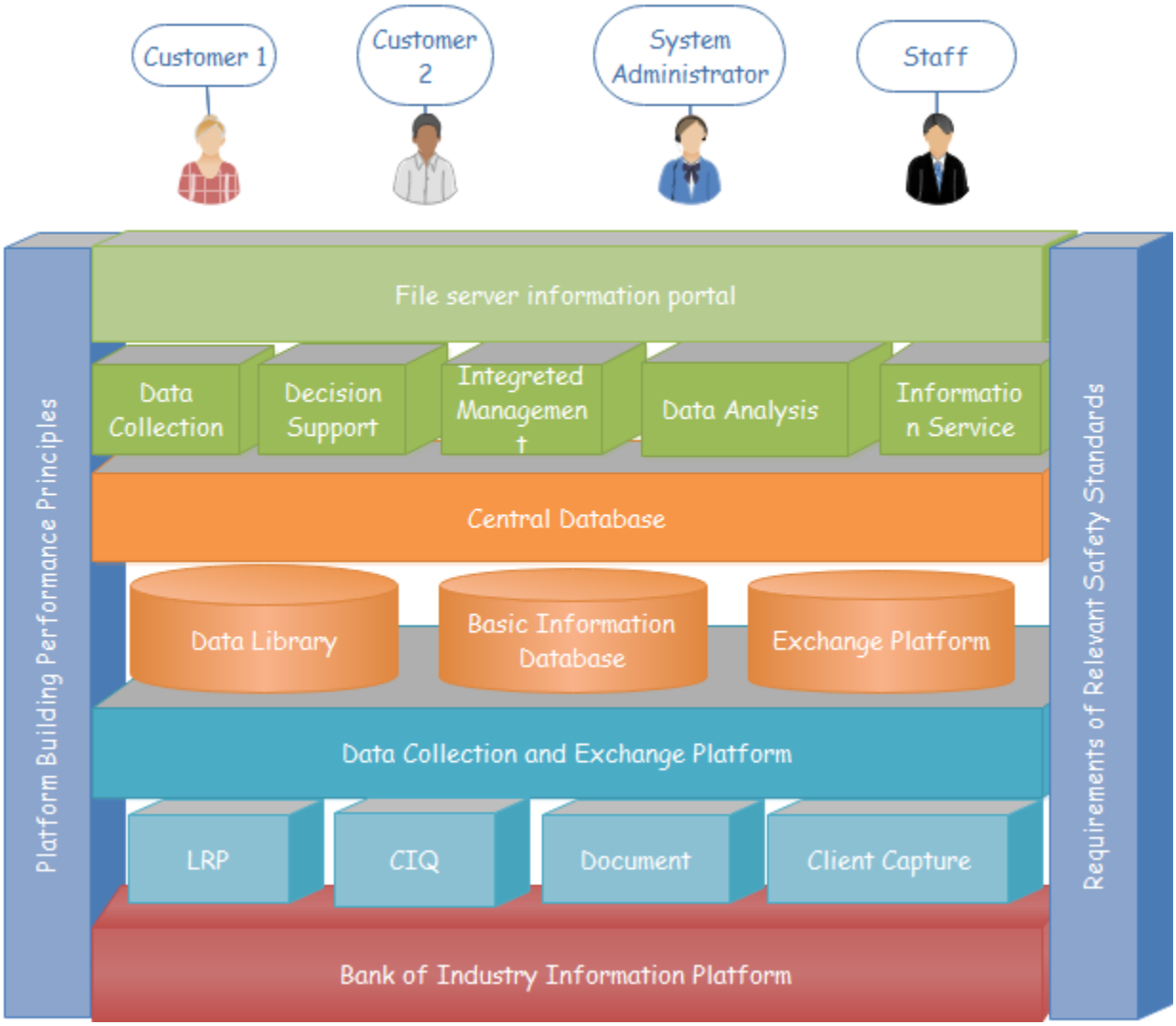

Figure 3.7: System Architecture

3.4 Analysis of Modules

Opening Account: This module is where the registration of customer opens of account.

Loan Request: This module enables the customer to apply for loan.

Create Staff: This module enables the admin to create accounts for the staff.

Grant Access: This module grants access to any file uploaded on the file server.

View Activities: This module enables the admin to view every activity on the fileserver.

Others services: These modules involve the rest of the services pertaining to the customers.

Logout: This module logs the current user out.

CHAPTER FOUR

SYSTEM IMPLEMENTATION AND DOCUMENTATION

4.0 Introduction

This chapter presents the choice of programming language, programming environment and system implementation.

4.1 Choice of the Programming Language

The programming language used for implementing this research work is Visual Basic edition. This programming language helps to develop program that runs in all platform with a user-friendly interface.

4.2 Programming Environment

Several computer hardware and software resources were used in completing this research work and are specifically mentioned below.

4.2.1 Hardware Requirement

The hardware requirement includes

(i) Processor speed of at least 700 Magahertz

(ii) At least 40 gigabyte of hard disk

(iii) A functional keyboard

(iv) At least 500MB of RAM and

(v) UPS

4.2.2 Software Requirement

The software requirement includes

(i) php 7.4,

(ii) Laravel Framework,

(iii) CSS6,HTML 5,

(iv) SQLite,

(v) Javascript,

(vi) Bootstrap 3

(vii) An effective antivirus

4.3 System Implementation

The File server provides the following types of easy-to-use, interactive, and intuitive graphical and telephonic interfaces.

i. The File server provides an easy-to-use, intuitive Graphical User Interface (GUI) as part of the Administrator's working desktop environment.

ii. The File server also provide an interactive Graphical User Interface, for the general users.

4.3.1 System testing

This is the system testing phase of the system development life cycle which includes the installation of the system and the initial use of the complete system.

For any system to output result, the user must be able to use the system effectively. This is user friendly, flexible and interactive. Thereby, offering users the ease of learning and training staff on the use of computer-based system. Once the training is completed, the system is implemented and the manual system has to be replaced. The following changes over procedure are available in this study:

1. **The Pilot Approach**

In this approach the changeover being with the selection of all the departments involved in using this application. This system is first tested within these departments so that, if the users' specification is in line with that of the program specification of the new system then all other sections of the organization will be converted. If there is any amendment to be done, it is done easily and the specification is met, the new system takes over automatically.

2. **Phased Approach**

The conversion type is useful in this study, since it is done in a step by step fashion, starting with single section of the firm at a time, until the entire conversion of the other sections is completed and the old system is absolutely search out.

3. **Parallel Approach**

This change over approach is also useful in this study, because it allows both data processing operations to occur simultaneously on both the old and the new system. The result from both systems are compared, which if identical then the new system takes over fully from the old system, despite the fact that this approach places strains on the resources of the organization.

4. **Direct change over**

In this system, the old system is no longer available and everything must run on the new system. Problem with the new system can cause problems for the business, only suitable for non-critical system.

The system working scenario is as follows:

i. The customer should register himself/herself in order to see the services concerning them.

ii. The admin will need to create the account for the staff, to enable them view files.

iii. The admin can now add files for the staff and their respective, monitor the login activities of the users.

4.3.2 SYSTEM USERS ADMINISTRATOR

This is the person charged with responsibility of updating System Content

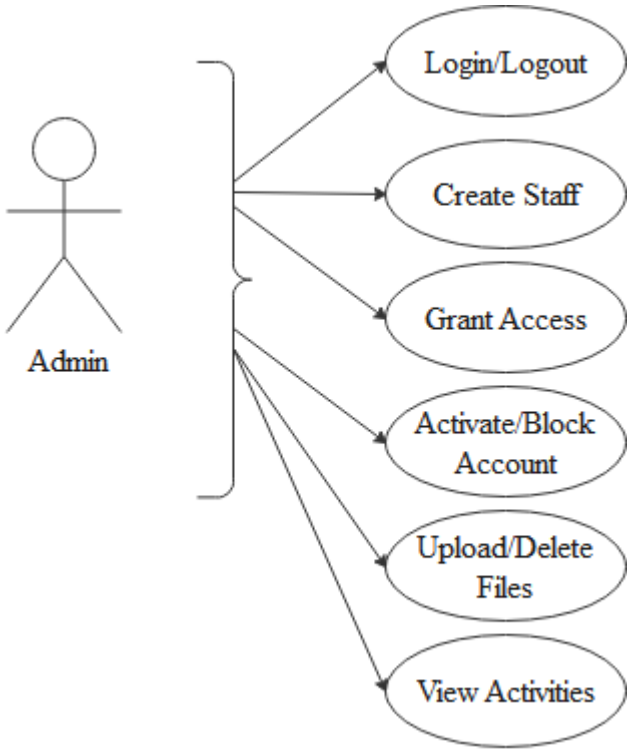

Figure 4.1: Administrator Use Case Diagram

Customer

The person who accesses the system from the customer point of view

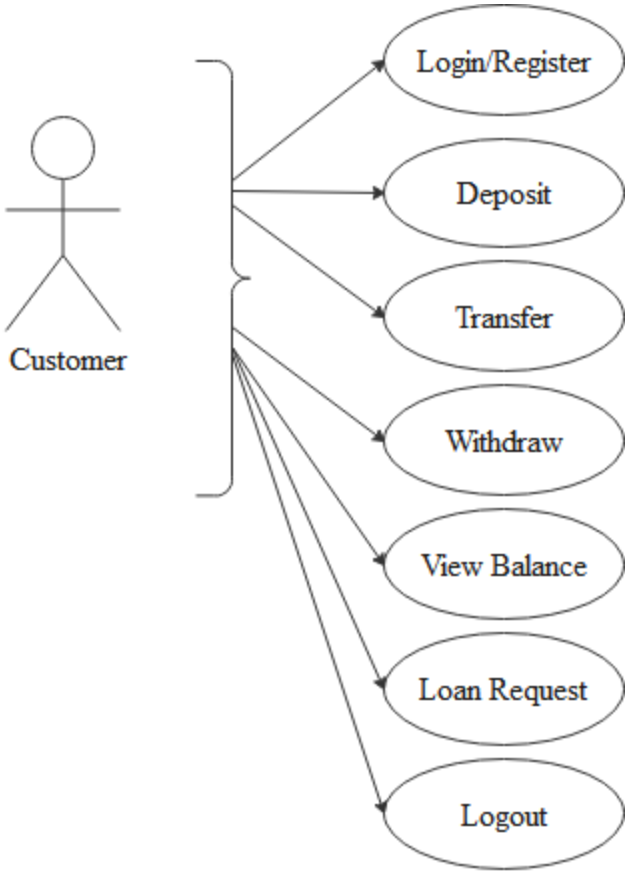

Figure 4.2: Customer Use Case Diagram

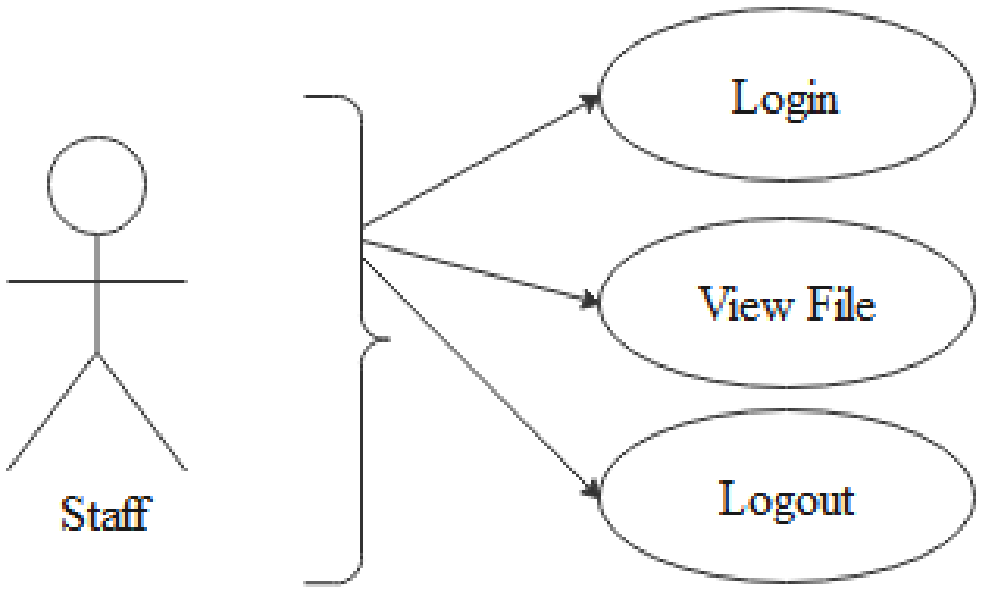

Figure 4.3: Staff Use Case Diagram

4.4 User's Environment

a) Welcome Page

This appears when the URL of the file server is typed in any browser.

Figure 4.4: Welcome Page

b) Login Page

This page customers are required to register or login.

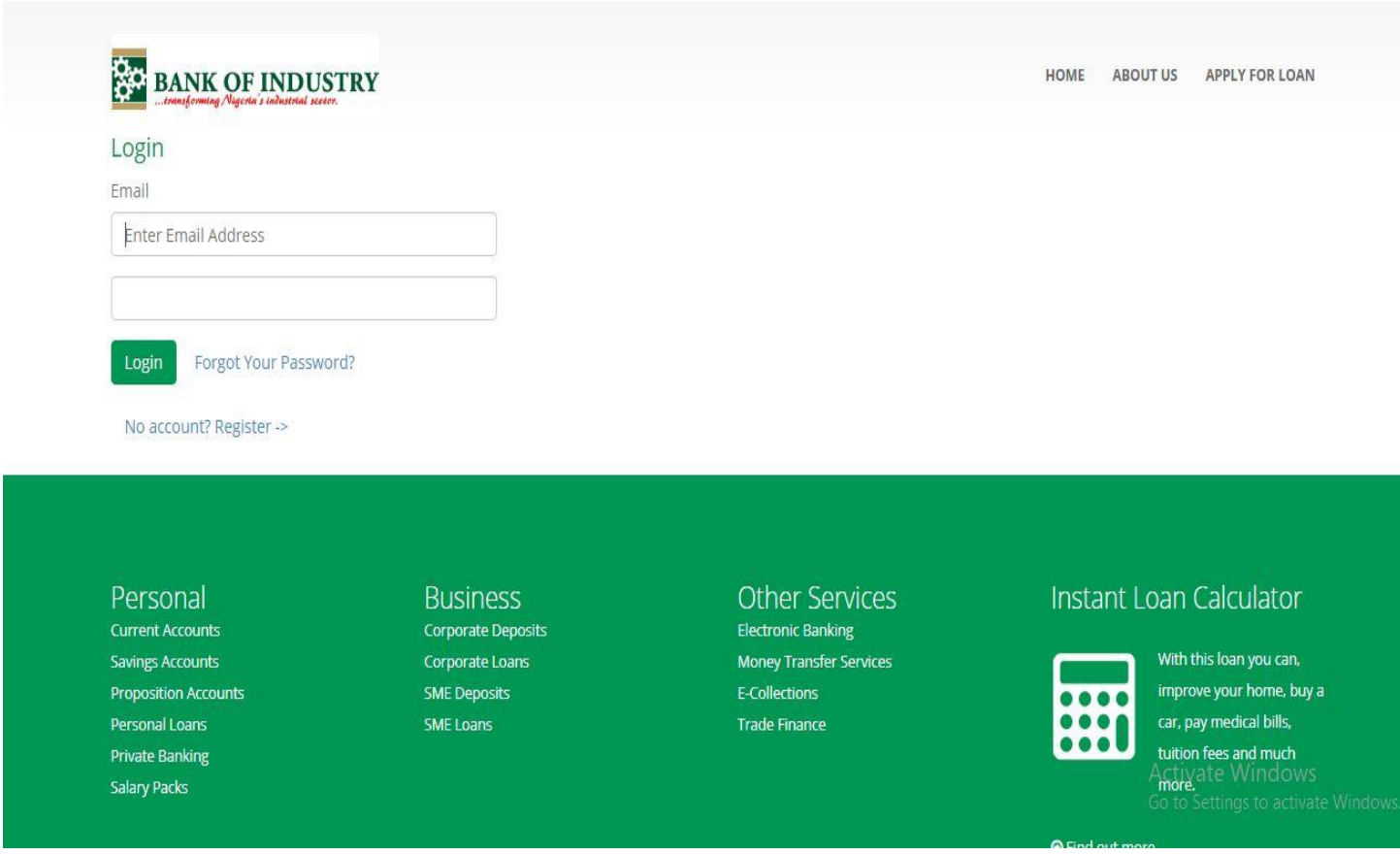

Figure 4.5: Login Page

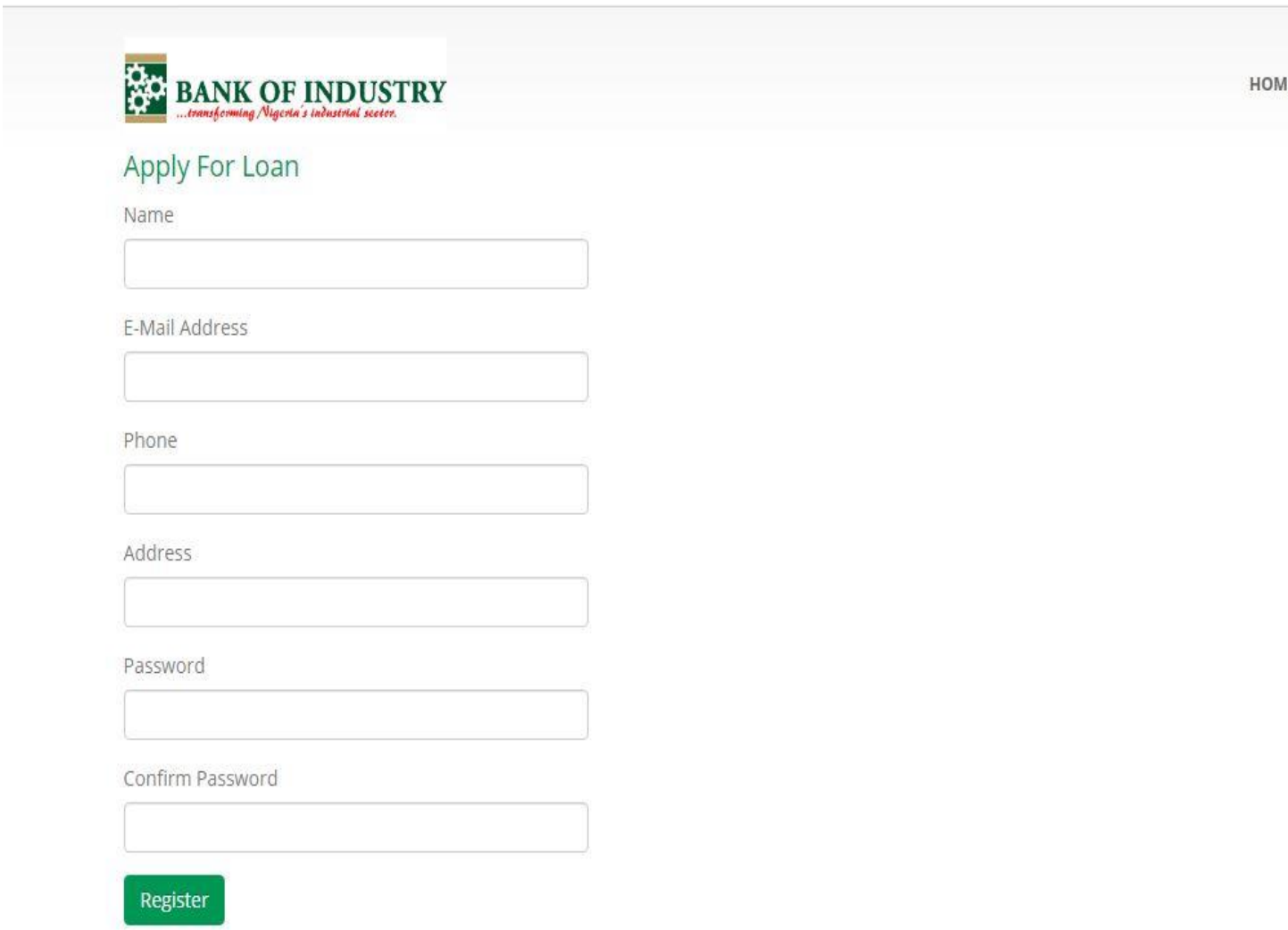

Figure 4.6: Registration Page

Administrator Environment

This is restricted environment; it is used by the administrator to change system content. It's accessed by logging in with the admin username and password on administrator. Once the correct admin password is entered the person will have access to modify/ delete and all control of the system.

a) File Upload Interface

This interface is used by the administrator to upload files in the system. Files uploaded here can then available for the particular department it is addressed to. In here the administrator can create a new file or upload an existing file

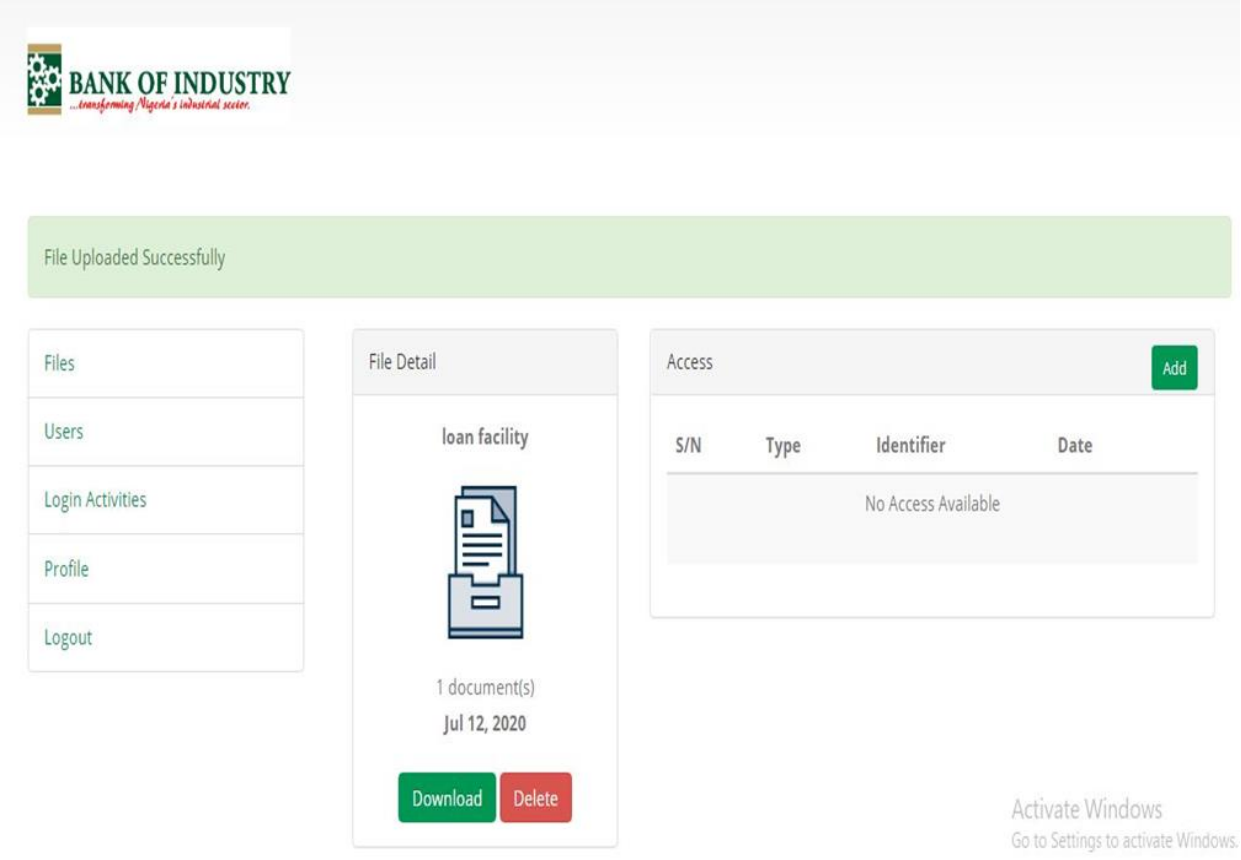

Figure 4.7: File Upload Interface

b) Login Activities Interface

This interface is used by the administrator to monitor login activities by users.

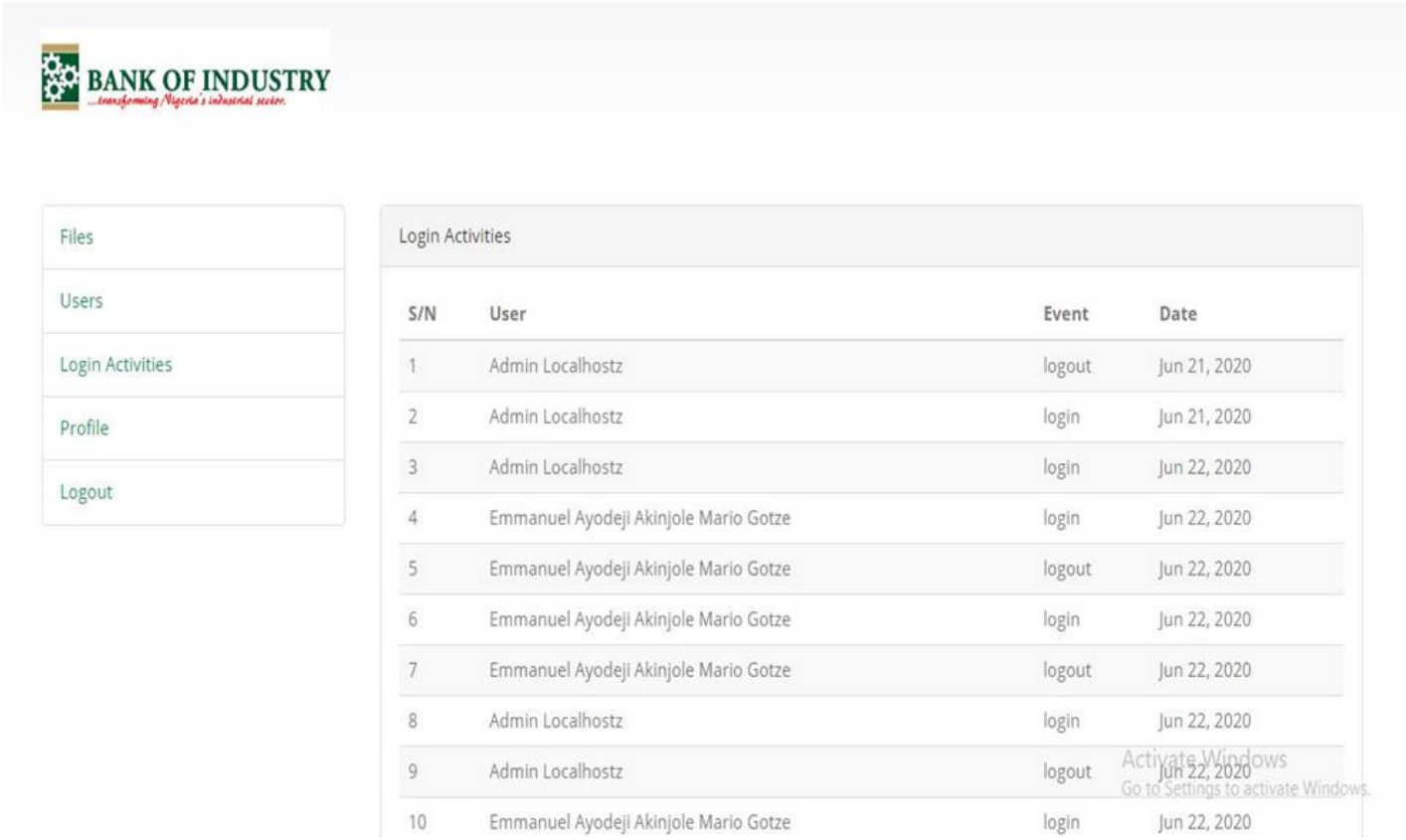

Figure 4.8: Login Activities Interface

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.0 Introduction

This chapter presents the summary, conclusion and offers useful recommendations.

5.1 Summary

This research project was carried out in an attempt to develop an intrusion prevention system using Bank of industry as the case study this project is an application that will enhance Productivity, effectiveness and efficiency by reducing work intensity, less tedious and enhance speed optimization. It will help the admin to monitor activities and prevent intrusion, also it makes work less tedious for the staff. It also enables the admin to know the users who try to intrude. The challenges of the existing system were; poor performance experienced during information auditing and network analysis, the current system provides an effective and efficient platform for admin and users, day to day activities. The challenges of the existing system can be solved when the proposed system is adopted. The researcher gathers data through primary and secondary sources which includes textbook, journals and the internets. This software is developed using Php 7.2 programming language and Laravel framework 8.0. The new system has more advantages over the manual system in terms of speed, efficiency, accuracy, storage and easy retriever of information for decision making.

5.2 Conclusion

The introduction of the internet and the world wide web for data computing and processing has brought so much improvement and increased productivity and has also reduced the amount of time spent in accomplishing task compared to the system were things were done manually which was done through paper works or some sort of methods which resulted to some deficiencies in data or loss of data. Advancement to businesses through technology has revolutionized the system but the dangers still remains the fact that confidential information if not protected through a secure means will be accessed and used for malicious purposes, which is what the proposed system tends to offers a more secured approach to ensure activities are monitored and auditing of the network to filter out activities that pose as great dangers to the underlying system and its users. as compared to the previous system which has recorded high data loss and insecurities, but with the proposed system users can go to sleep with their two eyes closed with the assurance that data is secure and safe.

5.3 Recommendations

Below are the recommendations of this research work

- The researcher recommends that the administrators and staff should be trained on how to use the system, thus enabling them to understand the functionality of the entire system.

i. There is need for the system upgrade as user's requirements change. User requirements differ with time therefore, it is of great help for the system to be flexible enough.

ii. The framework should be produced affordable to promote patronization of the scheme by customers

iii. However, a lot of system access is protected by a username and password, the entire computer system should be shielded from unauthorized individuals in order to prevent misuse and system component harm.

iv. Users should closely select distinctive usernames and very powerful passwords to prevent system safety breaches, so they should not have brief passwords, using the names of their colleagues or families as passwords.

v. In case of hardware or software malfunction, backups should be done frequently to avoid data loss.

5.4 Constraints of The Study

In carrying out the research work, some challenges were faced that limited the study such as:

Time: The time given for the completion of the research work was too short hence the researcher had to speed up the research work to meet up and this has an impact on the study.

Limited Materials: A few materials were found pertaining to the research area and this limited the bulk of the literature review.

Finance: The high cost of textbooks, internet browsing and transportation to different libraries to gather materials stood as a constraint to the research work.

REFERENCES

Abdelkarim, A. A., & Nasereddin, H. H. (2011, January). Intrusion Prevention System. *INTERNATIONAL JOURNAL Of ACADEMIC RESEARCH, 3*, 432-434. Retrieved October 11th, 2020

Arntz, P. (2013, May 11th). *Host Intrusion Prevention System (HIPS).* Retrieved October 13th, 2020, from Malwarebytes LABS: https://blog.malwarebytes.com/101/2013/05/whatiships/

Beal, V. (2005, July). *Intrusion Detection (IDS) and Prevention (IPS) Systems.* Retrieved October 10th, 2020, from Webopedia: https://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp

CNSS, C. (2010, April 26th). *Cyber attack*. Retrieved October 10th, 2020, from Wikipedia: https://en.wikipedia.org/wiki/Cyberattack

Gurubaran, S. (2019, July 9th). *GBHackers on Security.* Retrieved October 12th, 2020, from Intrusion Prevention System (IPS) In-depth Analysis: https://gbhackers.com/intrusion-prevention-systemips-and-its-detailed-funtion-socsiem/

Lerner, P. (2012, November 26th). *Implementing IPS securely.* Retrieved October 10th, 2020, from Networkworld: https://www.networkworld.com/article/2161673/10-tips-for-implementing-ips-securely.html

Petters, J. (2020, March 29th). *IDS vs. IPS: What is the Difference?* Retrieved October 12th, 2020, from varonis: https://www.varonis.com/blog/ids-vs-ips/

SECURITYTRAILS. (2018, October 16th). *Network Security Threats Explained.* Retrieved October 12th, 2020, from Security trails: https://securitytrails.com/blog/top-10-common-network-security-threats-explained

Techopedia. (2020). *Network-based Intrusion Prevention System (NIPS).* Retrieved October 13th, 2020, from techopedia: https://www.techopedia.com/definition/4030/network-based-intrusion-prevention-system-nips

Vacca, J. R. (2014). *Network and System Security* (2nd ed.). (N. McFadden, Ed.) Pomeroy, Ohio, USA: Steven Elliot. Retrieved October 12th, 2020

APPENDIX

LOGIN ACTIVITIES BY USERS

```
<link rel="stylesheet" type="text/css" href="http://ajax.aspnetcdn.com/ajax/jquery.dataTables/1.9.0/css/jquery.dataTables.css">

    <link rel="stylesheet" type="text/css" href="http://ajax.aspnetcdn.com/ajax/jquery.dataTables/1.9.0/css/jquery.dataTables_themeroller.css">


@extends('layouts.app')


@section('title', 'Transactions')




@section('content')

<div class="container" style="padding-top:50px;">

<div class="container">
```

```
    @include('layouts.partials.errors')
<div class="col-md-3">
    @include('layouts.admin_menu')
</div>
<div class="col-md-9">
    <div class="panel panel-default">
        <div class="panel-heading">ALL TRANSACTIONS </div>
        <div class="panel-body" align="center">
<table  id="myTable"  class="table table-hover" width="100%">
    <thead>
        <tr>
            <th>S/N</th>
            <th>Account No</th>
            <th>Name</th>
            <th>Transaction Type</th>
            <th>Date</th>
```

```
            <th>Amount</th>
            <th>Status</th>
            <th>Transaction Action</th>
          </tr>
        </thead>
        <?php $rows = 0; ?>
        <tbody>
          @foreach($transactions as $transaction)
          <tr>
            <td>{{$rows = $rows + 1 }}</td>
            @if ( $transaction->user)
              <td> <a href="/admin/transaction_history/{{$transaction->user->username}}"> {{ $transaction->user->username }}</a></td>
              <td>{{ $transaction->user->name }} </td>
              @else
              <td>N/A</td>
              <td>N/A</td>
            @endif
```

```
<td>{{$transaction->type}}</td>

<td>{{$transaction->amount}}</td>

<td> <small>{{ date('d-M-Y m:s', strtotime($transaction->created_at)) }}
</small></td>

<td>

@if($transaction->status == "Successful")

<span class="text-success"> {{ $transaction->status}} </span>

@else

<span class="text-danger"> {{ $transaction->status}} </span>

@endif

</td>

<td>

@if($transaction->status == "Successful")

<span class="fa fa-icon fa-check-circle" style="color: green"></span>

</td>



@else($transaction->status != "1")
```

```
<form class="form-inline" method="post" action="/admin/activate/{{$transaction->id}}">
    {{ csrf_field() }}
    {{ method_field('PATCH') }}
    <div class="col-md-6">
      <small>
        <div class="input-select">
          <select name="status">
            <option selected="" value="">-- Select --</option>
            <option value="Successful">Activate</option>
            <option value="Pending">Pending</option>
          </select>
        </div>
    </small>
    </div>
    <div class="col-md-4">
   <button type="submit" class="btn btn-primary btn-xs">Activate</button>
    </div>
```

```
    </form>
@end
            @endforeach
          </tbody>
        </table>
            </div>
          </div>
        </div>
</div>
</div>
<!-- Container End -->
<script>
    $(document).ready(function(){
        $('[data-toggle="tooltip"]').tooltip();
    });
</script>
@endsection
```

```
@extends('layouts.app')


@section('title', 'Home page')


@section('content')
<div class="col-md-9">
      <div class="panel panel-default">
         <div class="panel-heading">Login Activities</div>
         <div class="panel-body" align="center">
            <table id="myTable" class="table  table-striped table-hover">
               <thead>
                  <tr>
                     <th>S/N</th>
                     <th>User</th>
                     <th>Event</th>
                     <th>Date</th>
                  </tr>
               </thead>


               <tbody>
                  @forelse($logs as $log)
```

```
                <tr>
                    <td>{{ $loop->index + 1 }}</td>
                    <td>{{ $log->user->name }}</td>
                    <td>{{ $log->event }}</td>
                    <td>{{ $log->created_at->toFormattedDateString() }}</td>
                </tr>
                @empty
                <tr>
                    <td colspan="4">No record found</td>
                </tr>
                @endforelse
            </tbody>
        </table>
    </div>
</div>
</div>
@endsection

@push('script')
<script>
    $(document).ready(function() {
        $('[data-toggle="tooltip"]').tooltip();
    });
```

</script>

@endpush

@push('css')

<style> </style>

@endpush

@prepend('css')

<link rel="stylesheet" type="text/css" href="http://ajax.aspnetcdn.com/ajax/jquery.dataTables/1.9.0/css/jquery.dataTables.css">

<link rel="stylesheet" type="text/css" href="http://ajax.aspnetcdn.com/ajax/jquery.dataTables/1.9.0/css/jquery.dataTables_themeroller.css">

@endprepend