**CHAPTER THREE**

**SYSTEM ANALYSIS, DESIGN AND METHODOLOGY**

**3.0 INTRODUCTION**

This chapter takes an overviews on the system design and the entire research work, it is important to note that a poorly designed system will equally produce an incorrect output as such this chapter presents a skeletal approach to the design and analysis of the entire system.

System analysis has to do with examining a system in order to understand its step by step operations so as to identify its benefits and areas of limitation that require improvements.

**3.1 Analysis of the existing system**

Data security has been one of the most challenges faced by many organizations whose applications are hosted on the cloud that’s is been controlled through the remote networks.

Cloud computing are the most vulnerable targets for intruder’s due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDS are not suitable for cloud environment as network based IDS (NIDS) cannot detect encrypted node communication, also host based IDS (HIDS) are not able to find the hidden attack trail.

Due to data security challenges encountered by users were intruders or hackers hack into people’s privacy due to lack of security measures used in web application.

Users will be login in to launch their application through any internet enabled devices and take their continuous assessment were the system monitor and record the exact time ip address of the student.

**3.1.2 Advantages of the existing system**

1. the existing system were able to present users data on the cloud environment
2. it helps system administrators to manage there service and also reach global range
3. intruders can easily hack into the system since is not secured
4. it encourages data encryption

**3.1.3 Disadvantages of the existing system**

1. it is easy for intruders to hack into the system
2. data can be compromised
3. prone to many security risk as both the vendor and host stand a risk of losing their data to hackers
4. lost of data integrity
5. server cannot process the query from the user in a proper manner

**3.2 Analysis of the proposed system**

Intrusion Prevention is one of the main challenges of Internet security today, Most of Internet’s security is hosted on the network’s edge. However, the majority of attacks occur internally. In this scenario, not only an Intrusion Detection Systems, but also a Prevention System, which takes actions in order to block the attack, is required.

Intrusion detection system plays an important role in the security and perseverance of active defence system against intruder hostile attacks for any business and IT organization or to a cloud based application. Software Defined Network can be a useful tool for an Intrusion Prevention System, due to its capability to both mirror the network traffic and block the malicious flow as soon as the Intrusion Detection System notifies the controller. Due to the challenges stated above we propose a Software defined Network intrusion detection system. The SDN IDS will be deployed in a continuous assessment portal to monitor the server and user logs and also reports any attempt to intrude into the system using the SDN.

**3.2.1 Advantages of the proposed system**

1. High volume of data in cloud environment could be handled by a single node IDS through a Software Defined Network approach.
2. It will save lecturers time and will improve students leaning experience.
3. It will promote data integrity as the system is more secured using the software Defined Network Intrusion Detection system.
4. Software Defined Network IDS would be capable to carry out concurrent processing of data analysis, which is an efficient approach for intrusion Detection.
5. It will provide a better security system when compared to the existing system

**3.2.2 Disadvantages of the Proposed System**

1. The major disadvantage of the proposed system is that it cannot be used without the presence of good internet connections. So if a user is in an area where there is no internet service then he will experience some difficulties or may not be able to access the system and also required a trained staff for management.
2. IDS implementation requires an efficient, scalable and virtualization-based approach.
3. It require a trained staff for management

**3.3 System Design**

The system design pertains to the layout of the system and it consists of the input and output layout.

We are going to deploy the proposed methodology in developing an online examination system using multi- threaded intrusion detection system which will assist the administrator to manage the application, which will pop- up alerts to administrator whenever there is an attempt to intrude into the system.

**3.3.1 System Development Methodology**

A system development methodology (SMD) refers to the framework that is used to structure, plan, and control the process of developing an information system. In this study, we adopted the object Oriented Analysis and Design Methodology (OOD). The methodology employed for the development of the system is the OOAD. The OOAD development model comprises the elements of both design and prototyping. The model has four stages namely:

* Planning
* Analysis
* Evaluation
* Development

Object oriented analysis (OOA): This is the process of defining the problem in terms of object: real world with which the system must interact, and candidate software objects used to explore various solution alternative. The nature fit of programming objects to real world objects has a big impact here in the all real world objects can defined in terms of their classes, attribute and operations. Moreover, object oriented design (OOD) is the process of defining the component, interfaces, objects, classes, attributes, and operations that will satisfy the requirement. You typically start with the candidate object defined during analysis, but add much more rigor to their definitions, then you add or change objects as needed to refine a solution.

**3.3.2 Proposed system architecture**

**Storage**

**Detector**

**Responder**

**Collector**

**User interface**

**Figure3.1 proposed system architecture diagram**

System architecture is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system it buttress the exchange of information within the cloud systems which is organized in such a way to function together as a system. The database server connect to the internet, this makes the entire system accessible to all at any given time.

**3.3.3 Proposed system dataflow model**

Internet

**S D N**

**IDS SYSTEM**

**STUDENTS**

**User interface**

**LECTURERS**

**IDS RESPONDER**

**DATABASE**

**Fig3.2 data flow model for the proposed system**

This is the process of identifying, modelling and documenting how data moves around an information system. Data Flow Modelling examines processes (activities that transform data from one form to another), data stores (the holding areas for data), external entities (what sends data into a system or receives data from a system), and data flows (routes by which data can flow).

**3.3.4 Proposed system use case diagram**

Lecture

Student

Figure 3.3 use case diagram

The Use Case Diagram represents the lecturer and student behaviour. It defines the behaviour of both while using the system.

**3.3.4 Proposed system flow chart**

IDS Start

Session

SDN

Login

IDS

No

Login  
 true

Send Log

Yes

Lecture

User

Student

Assessment result

Student

Update assessment

Take Assessment

Activate & deactivate

Profile

Management

View all students

View students

Print

Figure3.4 proposed system flowchart

Flowcharts are used in designing and documenting complex processes. Like other types of diagrams, they help visualize what is going on and thereby help the viewer to understand a process and perhaps also find flaws, bottlenecks, and other less obvious features within it. The flow chart indicates a step-wise transition of the actions and decisions taken.

**3.4 Input Design**

The input to the system comes from the input form. Each of these forms has the function of collecting specific data from the doctors, patients, nurses and pharmacist as the case may be.

**3.4.1 Login Page layout design**

USER NAME

PASSWORD

LOGIN

LOGIN AS ADMIN

Figure 3.5 input login form

The login input form is what users use to access and login into the application.

Here the students are provided with login details which is there name and a default password which they can now change it immediately they are login in

**3.4.2 Input Design Layout**

Registration

Full Name

User Name

Department

Gender

Mat. No

Level

Add new student

Figure 3.6 add new student form

**3.4.3 input design form for lecturer**

**Continuos accensement data input**

QUESTIONNAIRE

OPTION 1

OPTION2

ANSWERES

OPTION3

UPDATE

Figure 3.7 input form for question

**3.5 Output specification design**

Continuos Accensement portal

Software defined network intrusion detection system

**Accensements management**

**Students**

**Detected Logs**

**Home**

SEMU

**Detected Intruders**

Footer session

Figure3.8 out put design of the proposed system

The out put display shows the outcome out come of our design which is based on user input and the design.