An Improved Intrusion Detection in Cloud Virtualization for National Open University of Nigeria (NOUN)

Kossisochukwu Okafor, Friday Onuodu

Abstract— **One of the major problems in cloud virtualization is security. To allow the smooth flow of this communalism around the physical resources, there ought to be a level of monitoring and security to ensure that each tenant has the resource availability, data integrity and process confidentiality that is required for operations. In Cloud virtualization, an extension of these capability is in a public environment which is prone to intrusion and needs to be secured. In this work, we developed an improved intrusion detection system that can sense and alert on attempted intrusions on a cloud based system. The proposed system was implemented with PHP programming language as front end and MySQL Relational Database Management System as backend. We adopted Waterfall lifecycle methodology in this approach. Our system has the ability to log and keep records of details of attempted intrusions for analysis as well as send alerts on an event of ongoing brute-force attack. This work could be beneficial to businesses, to tertiary institutions, to Government Agencies and to any other data storage centres that deal with big data.**

Index Terms— **Cloud, Detection, Intrusion, Security**

I. INTRODUCTION

Cloud is a general term used in computer networking to describe a heterogeneous internetwork of devices and machines that can be accessed through a connection to the internet. [1] Described Cloud computing as a way of catering for the demand of internetwork access or link to a managed system of configurable computing resources ranging from applications to Data Centers with the help of the Internet. Cloud computing infrastructure stores the software, applications and data. The applications are accessible from any device, including a laptop, cell phone and smart phone when these applications are connected to the internet. Virtualization is simply the ability to create instances of a real object to form virtual objects that behave as though they are real objects by themselves. In cloud virtualization the object to be virtualized is in actual existence in a Data Center in a distance location which in most cases unknown to the customer or user. These virtual objects can be used to provide a wide range of computer solutions and services.

In recent times cloud solutions have suffered some of the most brutal attacks of different forms causing the most devastating denial of service of all time. Such attacks reiterate and highlight adequate the need for security system in a cloud environment. An Intrusion Detection system for a Cloud Virtualization environment will improve the alertness to attacks, preventing devastating repercussions and reassure the cloud service subscribers and users of the confidentiality, integrity and availability of their data and services.

II. RELATED WORKS

[2] Presented a Moving Target Defense for the Placement of Intrusion Detection System in the Cloud identified and established a method that employs different elements of intrusion detection in a cloud virtualization which are either network based intrusion detection or the host based detection to mitigate threat by moving around the intrusion detection at the different layers. This work improved security against strategic attackers that circumvent to learn the placement of the intrusion detection. One of the limitation of the technique employed in the aforementioned work is that the switching relies on the computer to perform or execute the alternations thereby increasing the consumption of computing power and network bandwidth creating high power usage and overhead respectively.

[3] Proposed a collaborative intrusion detection which manages the intrusion detection in a cloud environment by harnessing a collaborative effect of the Network based intrusion detection which has to do with monitoring and flagging of malicious network traffic patterns and the host based intrusion detection system which primarily observes and handles insider infiltrations and attacks. The major limitation of the system is the complexity and cost of deploying more than one intrusion detection systems as security.

[4] presented a hybrid Network intrusion detection system that works by deploying sensors to the cloud environment, monitoring every node, scanning for network traffic in a bid to differentiate the intrusion traffic from the normal authorized traffic. The idea was conceptualized with anomaly detection, this makes it very conscious of malicious activities and this increases the chance of threat discovery but adversely will be a lot of overload on the network infrastructure in the environment.

[5] Presented a multi-level intrusion detection in cloud that reduced drastically, the amount of resources required in the implementation. The system organized users in different

security groups based on anomaly level which is an indication of the degree of the anomaly triggered by their activities. The model divided and demarcated anomaly level as a way of determining access levels.

[6] Proposed a hybrid intrusion detection in a private cloud by using an algorithm that detects an anomaly in the authentication process. The process of authentication involves the details supplied by the attempted log-on, getting compared to the already predefined log on credentials already stored in the database by the administrator. In an event where the details supplied does not match the information stored in the database or the connection request does not meet the predefined criteria established by the administrator to be met before a valid authentication, an alert is triggered. This algorithm favoured scalability but the time of response can be improved upon.

[7] presented a work on Collaborative intrusion detection system to manage the security of critical, vital and service oriented smart grid system which ideally functions like a cloud of infrastructure connected to each in a heterogeneous network, to exchange information and often require to authenticate across each cluster to maintain the connection used to exchange information. The work exposed a technique of using a collaborative measure which comprises of the network and host based intrusion detection to curb the security vulnerabilities of the set-up which could arise from the exposure of the heterogeneous network of the cluster to the internet. The work and the practicalities are herculean for certain small scale application.

III. MATERIAL AND METHODS

A. Analysis of Existing System

In the current Cloud Virtualization environment, the infrastructure consist of a data centre with serialized processors, array of data Storages, parallel Memory(RAM) and an Internet domain network. These component are configured to be allocable to subscribers based on their subscriptions. Some customers may require a certain specification such as certain amount of RAM, Number of CPU cores, a size of Data Storage or a specific capacity of bandwidth. These specifications are scalable and can be modified as the user or subscriber's requirement increases. After a cloud virtualization subscription a URI (unique resource identifier) string is assigned and issued to the subscriber, accompanied by the credentials or an electronic encrypted key which is to be presented at the authentication portal whenever the subscriber attempts to access the cloud resources.

Admittedly, the authentication process is the only mechanism to approve who is to be granted access to the cloud environment and electronic premises. The authentication credentials provided is matched against the credential database and once there is a match subscriber is authorized, the designated profile and infrastructure is loaded for the user. In an event of an attempted intrusion, the line of defense is either network based detection system which is programmed to monitor and report unusual traffic to the administrators, and host based detection that monitors the activities on the host to detect malicious operation and attempts by cloud tenants to access resource with authorization. This setup is assisted by a collaborative coordinator which collates the reports for the agents to detect anomaly.

Figure 3.1 is the Architecture of the Intrusion Detection in Cloud Virtualization which will allow us analyze the present system.

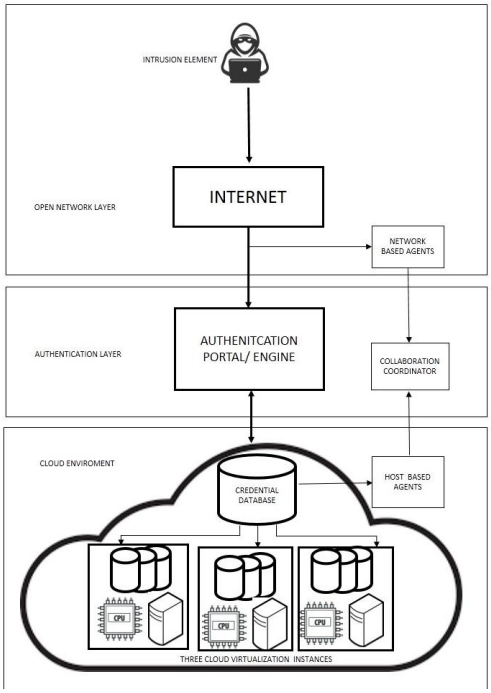

Figure 3.1 Exiting Architecture of the Intrusion Detection in Cloud Virtualization

1) Components of Proposed System

a) Intrusion Element: This is the initiation point of an unauthorized access to a cloud virtualization environment. This could be an individual hacker, an opportunist or an application designed for the sole purpose of malicious attacks,

b) Internet: This is the medium in which the intrusion element or cloud user is able to reach authentication portal for verification and authorization to access resources and service in the cloud environment.

c) Authentication Portal and Engine: This is the interface for the authentication process where the user provides the credential and the engine authenticates the provided credentials against the credential database and returns a reply to the interface.

d) Credential Database: This is the database used for the storage of the user credentials that is used to authenticate the user to gauge who is granted access to the cloud environment and the access level.

e) Knowledge Base: This is a database of incidents, logs of thread and crucial details of the threat such as originating IP address and Duration of attack.

f) Application Based detection System: This is an application that synchronizes with the knowledge base to identify abnormal traffic and

detection unauthorized activities within the virtual environment

2) Advantage of the Existing System

a) The Existing system is robust and is capable of handling detection a large data center.
b) It comprises of agents that work in different layer making detection effective.
c) It enables blocking of the intrusion element

3) Disadvantages of the Existing System

a) The existing system is large and hardly scaled down for small infrastructure.
b) The malfunction of the agents will tamper the detection system.

B. Analysis of the Proposed System

The Proposed system is an improved Application Based Intrusion detection System that detects intrusion by analyzing the traffic around the authentication portal and the process initiation within the NOUN cloud environment. This system does not include a collaboration coordinator. Alternatively, this system provides an application that intelligently understands a baseline behave of a normal traffic and uses it to flag an abnormal traffic. The application also observe the NOUN cloud environment for attack from within, by monitoring the file operation, infrastructure navigation and processes initiation. The system encrypted session recognizes all the level of access granted to every user of an instance of the cloud virtualization and will flag any activities of any authenticated user that might threaten to jeopardize the cloud resources of another user in the environment. The system include a credential hashing technology to encrypt the password of the user so as to prevent even the administrator from being able to view the credentials of the users.

Additionally, the system will include a knowledge base stored in a special database used to recognize threats and malicious activities. The system will be able to detect the Internet Protocol address of an intruder who illicitly attempts to gain access to the environment by supplying fake credentials and will store the address in the database for future anaylsis. If the intruder has employed the use of a hack tool for brute force attack which automates the generation of random credentials to try against the authentication portal, with the ability to detect the IP address, the system detects the number of attempts within a particular span of time and alerts the administrator and if programmed, blocks the specific IP address from further accessing the authentication layer from the open network layer. When a tenant user tries to access the cloud infrastructure of another tenant, an alert is sent to the cloud administrator.

1) Advantages of Proposed System Design over the Existing System

a) The proposed system is highly scalable and can function independent of agents.
b) It contains a knowledge base that will contain information about threat and can be reviewed by the administrator easily.
c) It is highly flexible and easily modifiable to feature new detection techniques against new intrusion behaviours.
d) It can algorithmically develop mnemonics of the systems to able to learn from previous threats.

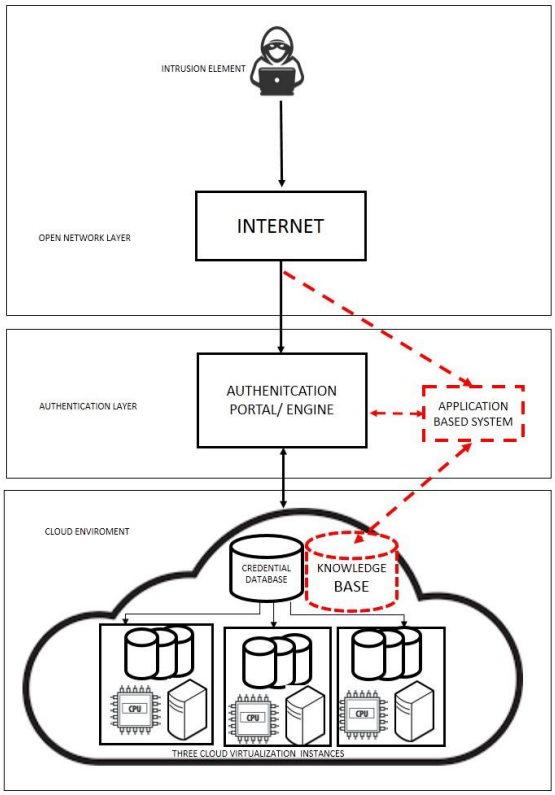

Figure 3.3: Architectural Design of the Proposed System

2) The Methodology adopted for the Proposed System Design

The Methodology adopted for Enhanced Intrusion detection is Waterfall Lifecycle Methodology. The System Development Lifecycle Methodology (SDLC) entails the use of a standardized procedural tasks in a bid to improve and enhance an existing work. It consists of stages that reference exact functions or activities. These involve Investigation, analysis, design, build, test, implement, maintenance and support.

3) Implementation Algorithm

We analyzed the existing and the Proposed Intrusion Detection system Algorithm. The algorithm are comparative Algorithms that use Iteration and variables model for their implementation. The following variable were declared before the initiation of both algorithms:

T, C, I, S, Q1, Q2, Q3, D, L, A, EQ, NE

Where T represents the Threat element to be detected,

C represents the credential to be supplied by the Threat element,

I represents the public IP address of the network of the Threat element,

Q1 represents the memory partition for authentication details in the general database of the system,

Q2 represents the memory partition for knowledge base in the general database of the system,

Q3 represents the memory partition for Network details in the general database of the system,
D represents the Authentication Result and Decision of the system,
L represents network link for the cloud virtualization infrastructure,
A represents the alert system of intrusion,
EQ represents equal to and NE represents not equal to.
Additionally, the following constants were also declared:
0= Invalid, 1-Valid.

ii) Proposed (Modified) Intrusion Algorithm
Step 1: START
Step 2: DECLARE T, C, I, S, Q1, Q2, Q3, D, L, A, EQ, NE
Step 3: AUTHENTICATE C OF T
Step 4: IF T = 0
Step 5: ADD I(T) TO Q3
Step 6 SAVE
Step 7: S++ WHILE S<5
Step 8: RETURN TO STEP 3
Step 9: IF S > 5
Step 10: ADD I(T) TO Q2
Step 11: SAVE
Step 12: INPUT I(T)
Step 13: MATCH I(T) TO Q3
Step 14: IF (I(T) EQ I(Q3)) EQ 1
Step 15: PRINT D EQ 0
Step 16: SEND A
Step 17: IF T SETS L
Step 18: MATCH C(T) TO Q1
Step 19: IF C(T) TO Q1 EQ 1
Step 20: PRINT D EQ 1
Step 21: ELSE
Step 22: MATCH I(T) TO Q2
Step 23: IF (I(T) EQ I(Q2)) EQ 1
Step 24: PRINT D EQ 0
Step 25: SEND A
Step 26:STOP

4) Flowchart of The Proposed System

The proposed system is designed in a flowchart as shown in Figure 4.1 which demonstrates the flow of the logic through the detection process. The decision making system is able to use the application and database to mitigate threats and intrusion as described in the flowchart.

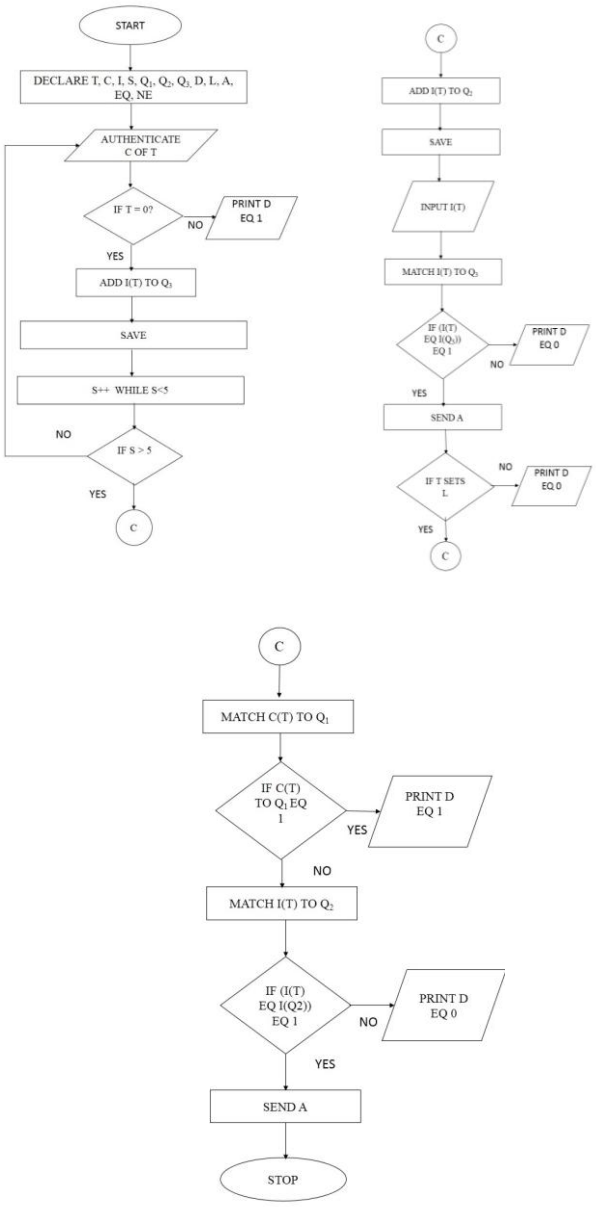

Figure 4.1: Flowchart of the Algorithm of the Proposed System.

IV. RESULTS AND DISCUSSION

A. Discussion of Results

Figure 4.2 is the introductory page of the system. It is the first page that is displayed as soon as the cloud domain home address is inputted into the address bar of any optimal and up-to-date browser. This display was ergonomically and graphically structured with Hypertext Markup Language, cascading Style Sheet (CSS), Bootstrap and JavaScript and in the backend to handle the functionalities is Hypertext Preprocessor. This page is to welcome the cloud user or prospective cloud user to the domain officially. The page is composed of majorly two interactive links closely positioned to each and they are brightly coloured with their functions clearly written out.
On visiting the landing page, the visitor should identify themselves as either a new user who therefore wishes to register a new cloud database account by clicking the link that indicate the "Register a Cloud Account" or a returning

cloud user who has an already existing cloud account in the cloud domain. The scope of the work focuses on protecting the accounts of the already existing user from intrusion, and threats with malicious motives concerning the vital information or data belonging to the already existing user but we are going to highlight on the functionality of the registration process. The registration link leads to a registration page which prompts the visitor to input an email Id and also to input and confirm the password as show in Figure 4.3. When the user inputs a valid email which is confirmed by a Regular expression that evaluates the email Id inputted to confirm if it is in a valid email format, the input is accepted and the user is redirected to the login page to login with the new credentials. In the background a very sophisticated operation takes place just before the redirection to the login page. This process involves the encryption of the password supplied by the new user. As shown in the database table of the user credential in Figure 4.4, the password is encrypted and unreadable thereby protecting the user's password from being broken. This encryption is done using the BlowFish 128bit encryption.

On clicking the "Already a Cloud User? Login" link, the visitor is directed to the next page where the authentication takes place. The page as shown in figure 4.5 requires the visitor to input their email Id and password which is presumed to have been registered. The page has two input fields, a link that redirects to the registration page and a button that fires the authentication process. If the provided log-on credential do not match any of the user details in the database the visitor is alerted as show in figure 4.6. If the visitor further attempts to login with incorrect login credentials for another five times, or attempts to use a hacking software to randomly guess the authentication details of the cloud portal user, the visitor will be alerted that they have been barred for a period of 30 minutes as shown in figure 4.7 and the system elicits the current Internet Protocol Address of the visitor and inserts it into the knowledge base then further alerts the administrator of the illicit attempt by activating the intrusion alert function in the Simple Mail Transport Protocol server.

The administrator will receive a mail instantly within microseconds in the configure mailbox address as show in figure 4.8. The mail will contain the type of attempt which in this case is an authentication intrusion and the IP Address of the intruder. This mail can be configured to be received on-the-go via a cellphone as shown in Figure 4.9.

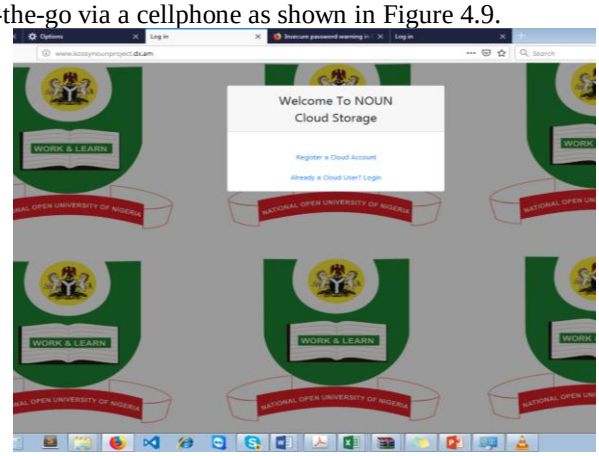

Figure 4.2 Welcome Page of the Proposed System

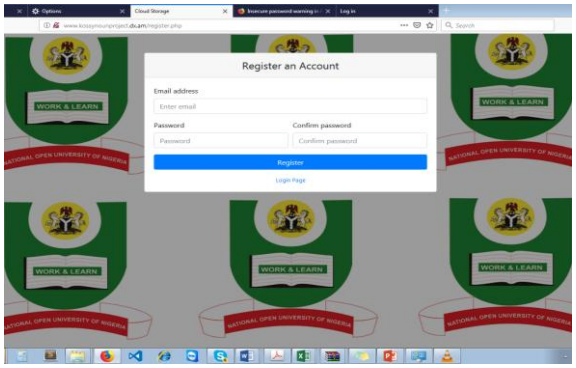

Figure 4.3 Registration Page

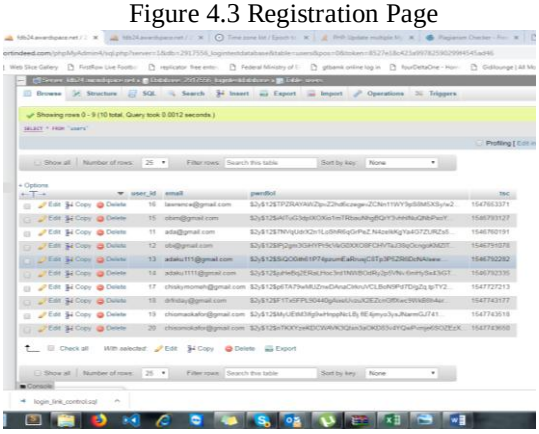

Figure 4.4 The Encrypted Passwords in the Database

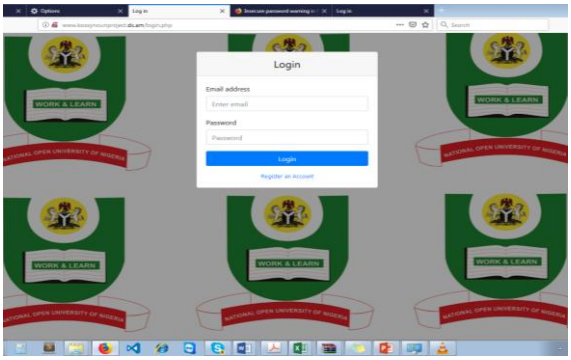

Figure 4.5 Login Page of the Proposed System

Furthermore, if an intruder who is familiar with the architecture of the home link on the domain network attempts to evade the logon authenticator and points their browser directly to the home page without having initially logged on with an active session. An active session here means that the token issued to the user's browser during their initial login is not expired and is still valid. The Application Decision system will perceive it as a malicious attempt with an ulterior motive. The information about the initiating visitor is inserted into the knowledge base database and a mail alert function is initiated which is sent to the administrator to alert of the likely threat.

If the visitor's authentication credentials are confirmed and matches the information of an existing cloud account, a session token is created and assigned to the user's browsers as a cookie. This token is encrypted and hashed with the

BlowFish 128 bit encryption as show in Figure 4.10. The session is stored in a special database to manage the access of the users to the cloud resources to enable easy and quick availability. This means that the user will not require subsequent requests for login credentials till the token created expires or the user decidedly logs out from the environment. After the session is created, configured and stored, the user finally arrives at the home page shown in figure 4.11

When the administrator is called to attention about an attempt, he proceeds to logon in the administrator interface of the system shown in figure 4.12 to critically analyze the intrusions detected. The administrator's interface is lightweight to avoid unnecessary graphic user interface that might deter quick access to information about ongoing threat. The administrator is required to login as shown in figure 4.12. After login comes the administrators landing page which displays vital information about the cloud system and users as well as threats to the cloud environment. The display include Total number of users, Number of link intrusions, Number of Authentication intrusions and the total number of Intrusions as shown in fig 4.13. The administrator can further view details of the intrusion by clicking the corresponding link in the left pane. To view details of the Authentication intrusion shown in figure 4.14 and also to view the detail of the link intrusion as show in figure 4.15. The administrator will be able to analyze the ongoing attack by monitoring the counter information displayed under the "Attempts" column in the respective links and determine the source of the intrusion by the different shown IP address

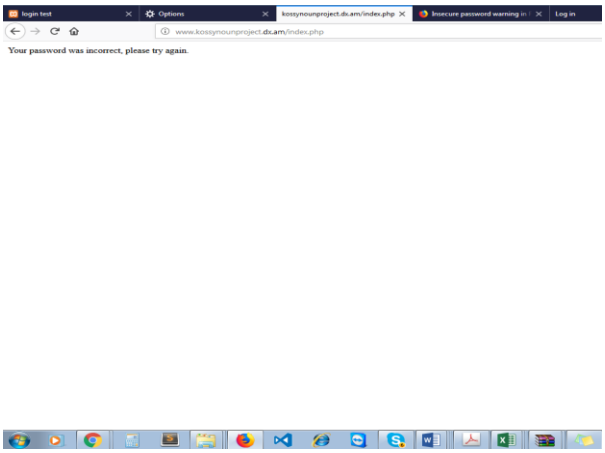

Figure 4.6 Login Error Page

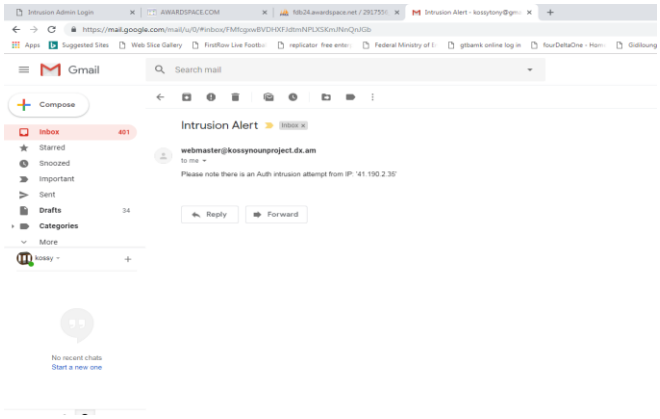

Figure 4.8 Mail Alert sent to the Administrator

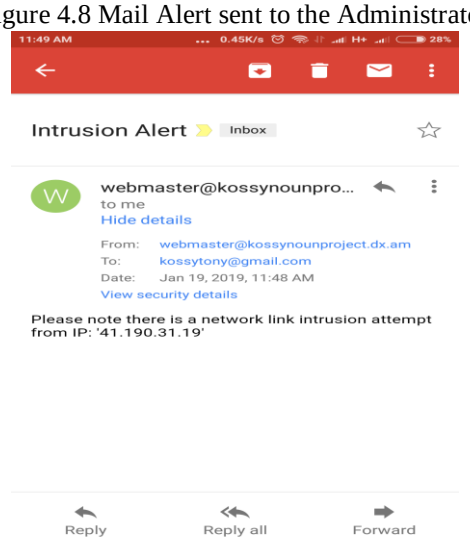

Figure 4.9 Mail Alert sent to the Administrator on-the-go via Mobile Phone

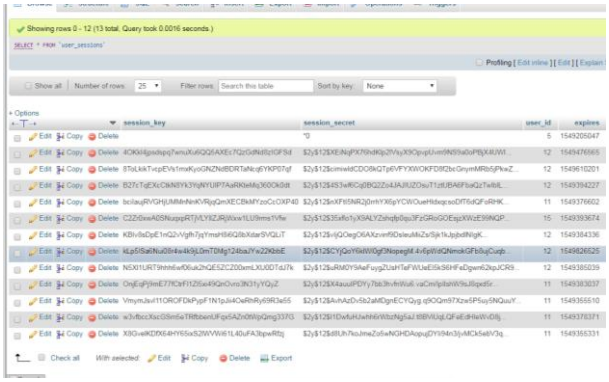

Figure 4.10 Encrypted Session information stored in Database

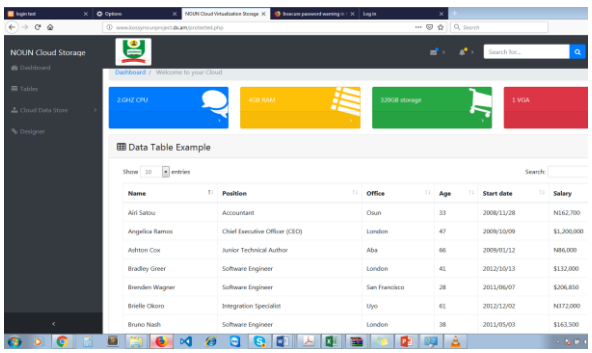

Figure 4.11 Cloud Home Page

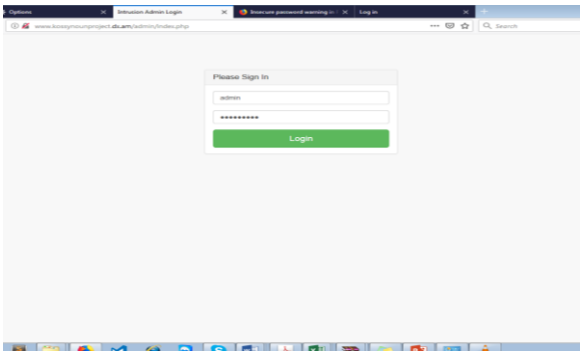

Figure 4.12 Administrator Login Page

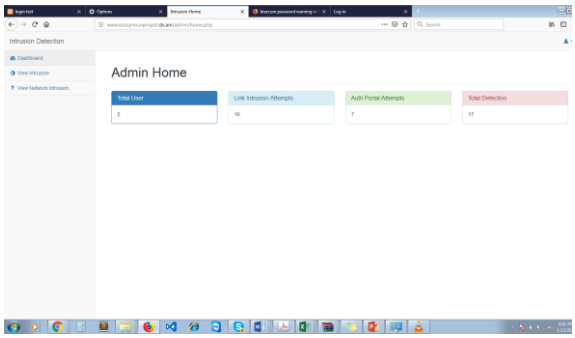

Figure 4.13 Administrator Home Page

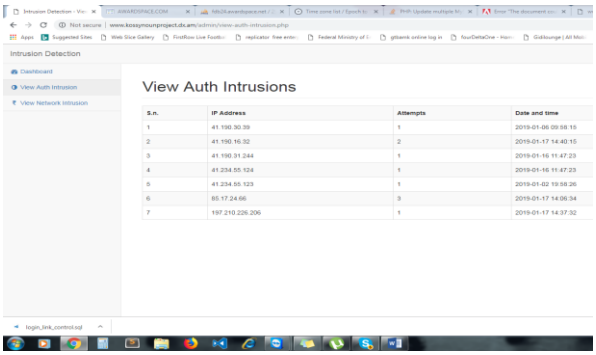

Figure 4.14 Authentication Intrusion Details

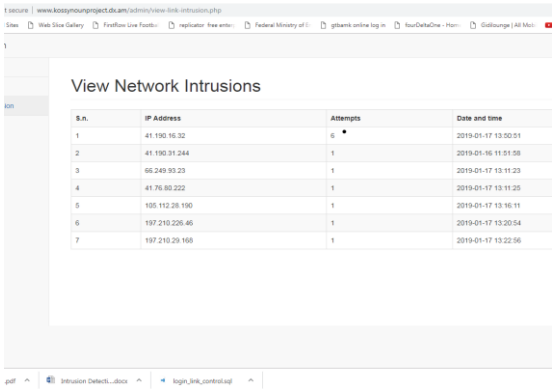

Figure 4.15 Network Intrusion Details Page

B. Comparative Analysis of the Existing and Proposed System

We critically evaluated the existing system to comparatively analyze the rate of false alarm generated by the systems. The false alarm rate is an important parameter to be considered as it impacts heavily on the system's ability to decipher the behaviour of an intrusion element from the behaviour of regular traffic to enable an adequate response or action. This will enable the cloud administrator to minimize the waste of resources invested in handling or responding to false indications of threats to the environment

We compared [1] where the experimental results of the work showed a level of accuracy when the false alarm rate was reviewed, with our technique and there was a substantial reduction in false alarm rate as we allowed more attempts to be made before obtaining the information to be forwarded in the alert. Also we comparatively reviewed against the result of [5] which had a good level of accuracy in detecting intrusion on the network layer architecture.

Secondly, we compare the scalability of the system by looking at the techniques that are deployed on the system. We reviewed the experimentation of the existing systems with more components and they proved to be hardly scalable than when they are comprised of fewer components. [3] had a very impactful level of accuracy when reviewed with respect to false alarm but the technique required a lot more component to be deployed in the different segments of the system. This greatly reducing the scalability of the system to a miniature configuration that will deliver the same level of accuracy as it will deliver to a more robust and costly setup. Our work compares well in scalability as the application runs in the system and requires minimal computing power to evaluate the threats in the system.

Table 4.1: Comparative Analysis of the Existing and Proposed Intrusion Detection System

SYSTEM MODEL	TECHNIQUE	ACCURACY RATE (%)
Tan et al (2015)	COLLABORATIVE (NETWORK AND HOST)BASED	75
Wakhade et al (2016)	NETWORK BASED	63
Potteti et al (2015)	HYBRID (ANOMALLY AND HONEY POT)BASED	70
Rajendran et (2015)	HYBRID (ANOMALLY AND MISUSE) BASED	75
Patel et al(2016)	COLLABORATIVE (NETWORK AND HOST) BASED	85
Okafor (2019)	APPLICATION BASED	93

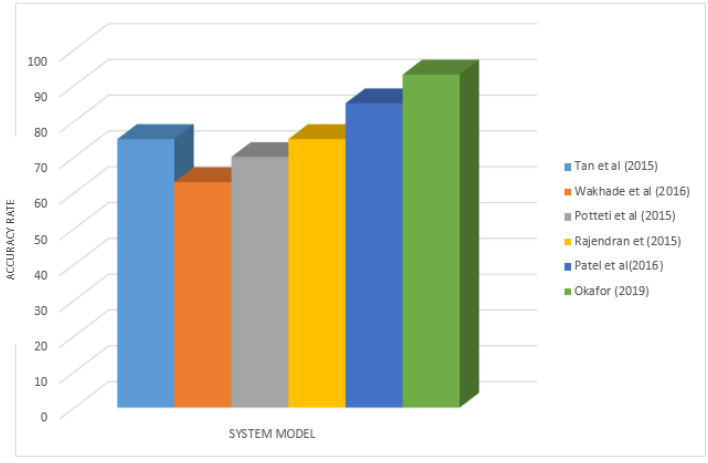

Figure 4.15 System Model versus Accuracy Rate Chart

V. CONCLUSION

The viability of Cloud Storage is growing at a significantly high rate. More people are using Cloud Virtualization as a way of storing vital information. An Application based Intrusion Detection system will improve the security of data from threats that will cause data unavailability or ruin the integrity and confidentiality of data. An Intrusion Detection system is a system incorporated as a part of a larger system which is responsible for the security of that system in the sense that it stays alert awaiting threat that may pose a potential danger to the system which it is a part of. Intrusion Detection in Cloud Virtualization is when a measure is put in place in a cloud environment to evaluate and manage threats in the manner of intrusion which could jeopardize the entire operation of the cloud environment, or the data integrity of the information or data stored in the cloud environment. When intrusion Detection in cloud virtualization is Application based, it is lightweight, fast and can deliver information about threats in record time to enable the quick and prompt response or counter-action to neutralize imminent hazard that could be associated with the threat in the environment. The Application based Intrusion Detection works effectively and intelligently with the aid of a knowledge base managed in a database associated with the system, to counter attacks by learning and storing information about the threats which is harnessed to mitigate subsequent strikes against the environment.

Recommendation and Contribution to Knowledge

The importance of data security in the cloud environment in this era of big data and strict privacy governance cannot be overemphasized. Therefore, this work will be highly beneficial to data storage centers, as sturdiness and accuracy in securing data is a current prerequisite to reliable cloud data storage services. This work has been enhanced by the addition of a knowledge base which facilitates the detection and response to threats to the cloud environment.

Suggested For Future Improvements

The issue of intrusion detection in cloud virtualization is still an open problem. We suggest research in in security against virtual private network hooping intrusion in cloud. This will enable security system to be more fortified.

REFERENCES

[1] D. Wankhade and K. Rupali, "Virtualization Intrusion Detection System in Cloud Environment", *International Journal of Scientific & Engineering Research*, vol. 7, no. 2, 2016.
[2] S. Sengupta, A. Chowdhary, D. Huang and S. Kambhampati, "Moving Target Defense for the Placement of Intrusion Detection Systems in the Cloud", *International Conference on Decision and Game Theory for Security*, vol. 11199, 2018.
[3] Z. Tan, U. Nagar, X. He., P. Nanda. And R. Liu, "Enhancing Big Data Security with Collaborative Intrusion Detection", *IEEE Cloud Computing*, vol. 10, no. 11, pp. 27-33, 2017.
[4] C. Modi and D. Patel, "A Feasible Approach to Intrusion Detection in Virtual Network Layer of Cloud Computing", *Indian Academy of Science*, vol. 43, no. 113, pp. 6-12, 2018.
[5] P. Rajendran, M. Rajesh. and R. Abhilash, "Hybrid Intrusion Detection Algorithm for Private Cloud", *Indian Journal of Science and Technology*, vol. 9, no. 35, pp. 0974-5645, 2015.
[6] A. Patel., H. Alhussian., M. J. Pedersen., B. Bounabat, J. Celestino Júnior and S. Katsikas. "A Nifty Collaborative Intrusion Detection and Prevention Architecture for Smart Grid ecosystems". *Computers & Security*, vol. 63, pp. 92-109, 2016.

Kossisochukwu Okafor is a post-graduate student at the Department of Information Technology of National Open University of Nigerian. Research interest includes Cloud infrastructure, big data and network Security.

Friday Onuodu is a Senior Lecturer in the Department of Computer Science in the University of Port Harcourt, Nigeria. Research interest include big data, Hybrid technology systems.