JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-10, Oct 2019 E-ISSN: 2347-2693

An Improved Hybrid Cloud Computing Security Architecture Using Network Based Intrusion Prevention System

P.J. Ebiriene[1*], N.D. Nwiabu[2]

[1,2]Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

**Corresponding Author: paulforsureonline@yahoo.com, Tel: +2348038659070*

DOI: https://doi.org/10.26438/ijcse/v7i10.914 | Available online at: www.ijcseonline.org

Accepted: 08/Oct/2019, Published: 31/Oct/2019

Abstract **-** Cloud computing is a rapid rising technology and of a great degree acceptable computing prototype round the globe resulting from its merits on prompt deployment, monetary value (on staging up and environment), big storage capacity, likewise worry free privilege to system anytime, anywhere. This work is aimed at defining various attack patterns that affect the accessibility, confidentiality and integrity of resources and services in cloud computing environment. In addition, the research ushers in a network based intrusion prevention system (NIPS) to discover and stop suspecting actions by monitoring configuration of the system, logs files, network traffic changes, and activities of end-users in the cloud computing network using predefined signatures (rules). This rules classified IP address of users to white list for real user and blacklist for attacker. Results shows that block IP addresses found in blacklist were redirected to attackers (intruders) log, detailing the IP addresses, username, date/time and action. The system security is strong; users whose IP addresses, username and password were found in white list could use the system.

Keywords – Cloud Computing, Hybrid Cloud, Network Security, Honey Pot, Network Based, Intrusion, Prevention, Detection.

I. INTRODUCTION

Cloud computing comes as a newly prototype with a primary target to provide safe, fast, suitable network computing service and data storage. Not minding that cloud computing strongly minimizes how the IT industry is been maintained, matters regarding security wreaks a pertinent function. To a great extent several IT companies are moving to cloud based service like Public, Private and Hybrid cloud computing. But in like manner, they are interested so much about security issues [1]. [2] defined cloud computing as a frame work for enabling suitable, on-demand network privilege to a shared pool of configurable computing resources (e.g., servers, networks, applications, storages, and services) which is capable of given out minimum service provider interaction or management attempt ”. A cloud computing that has a well known user interface with proper entry regulatory mechanism is capable of restricting access and increase the chance accountability. Notwithstanding, a merge data system with several people using more divers kinds of data via several applications can in reality make it difficult to correctly reduce entry and discover abuse [3]. Typically, the IPS can be designed on the bases of IDS hence the detection ability is required in an IPS model. [4] Proposed Learning Intrusion Detection System is to make available a network operation for mobile gadget security. It has the ability to discover and react to mischievous attempt with the aid of engaging security systems in use. It appears like a network operation that can filmy configured for end-host mobility and help those known countermeasures to extenuate discovered attacks. The authors didn’t make available an intensive way out for discovered attack attempt with several rating required to configure the best reply process with regard to threats. [5] Proposed classifier detection framework that employ data mining methods. Many companies have adopted cloud computing technologies without considering the network security challenges involved. Security of data is of paramount importance, with the recent growth of internet technologies there is need to protect the data stored in cloud against hackers and data loss. Nigeria alongside other developing countries are facing serious hacking problem due poor security of information. The aim of this research is to develop a Network-based Intrusion Prevention System (NIPS) in hybrid cloud computing environment against malicious users. This is achieved by analyzing existing firewalls and antivirus solution for better network security, identify and prevent suspicious activities in the cloud computing network using honey pot, signatures (rules) and to evaluate the prototype system to see how it can detect threat in a hybrid cloud computing system.

The rest of the paper is organized as followed: section I contains introduction of Intrusion Detection System, Section II contains the Related Work of different cloud computing and Intrusion detection and prevention systems, section III explains the methodologies and use case diagram of the system, section IV contains the architectural and the essential steps taken to prevent intruders, section V describes the result and discussion of the system are presented, section VI concludes the research work.

II. RELATED WORKS

Li, proposed a GA-based method for IDS which considers the two quantitative and unconditional characteristics in getting sorting process using GA. Their work provides effective and fast decisions [6]. A genetic algorithm based method for deducing a group of arrangement process from network audit data was proposed. Here, they employed the association rules model to find the support and confidence on each rule which eventually generated processes that are applied by the authors to arrange and discover intrusions in the network. However, it must be enhanced to suit the dynamic nature of the cloud data [7]. Xiang and his group made a proposal for new IDS that work on the bases of misuse intrusion detection using a hybrid classifier. Their system employs collections of both Decision Tree and clustering set of rules to discover intrusions effectively. The main advantage of their work is that they reduced the false alarm rate [8]. Two strategies for safe storage in the cloud for which so many files with some code where imbedded for correction. They then employ an inspection that engages a probability theory that guaranteed that sufficient blocks are gotten back to rebuild the file. In their scheme, the encoder engrafts exceptional blocks into the data file after which it was encrypted [9]. Intrusion Prevention System is meant to checkmate traffic and independently do away with packets that has involve mischievous, scrutinizing sessions that are suspicious or involving some other reactions in instant real time feedback to an attack. Trusted Intrusion Prevention gadget will examine all inward and outward traffic [10]. Data mining system network intrusion detection system was proposed here. The both data mining methods were employed by the author for anomaly, misuse and hybrid detection. The random forests algorithm was used in data mining arrangement algorithm and in developing the technique that has to do with misuse detection. This algorithm builds the intrusion method from equilibrate training dataset and then classifies the seizure network connection to the principal kinds of intrusions with respect to the built-in system [11]. These authors studied Network Security for Cloud Computing (NetSecCC) on the ways internet traffics will have protection from attacks, both from outward and inward using a scalable and an architectural system that can tolerate security fault in cloud computing. Their work covers experiment and simulations that proved their concept and had prototype to validate the possibility some level of flexibility in scalability, and fault-tolerance can be managed effectively [12]. An intrusion detection system was proposed here, the system which is being monitored from the cloud and can protect consumers' infrastructure especially when connected to the public cloud. They proposed the Intrusion Detection System as a Service (IDSAAS) for users' virtual machines protection. The proposed framework allows consumers to have within their cloud space a virtual private area where they can set security policies and enforce these polices [13]. These authors have studied intrusion prediction on systems in cloud computing. They proposed multi-concept approach to determine incidents. They described a single technique method of intrusion detection/prevention that works deploying some predictive statistical methods for building solutions for predicting intrusions. Some of the concepts combined in their models are risk assessment and game theory methods [14]. These authors talked about the administration of Cloud computing security in concentrating on Gartner's list of security issues with respect to cloud and the discoveries which he got from International Data Corporation enterprise. Gartner was able to recognized seven issues on security which should be looked into and then enterprises can see if they can switch to the cloud computing framework [15].

III. METHODOLOGY

This paper adopts constructive research method and agile software methodology to develop the entire system. The constructive research approach was used for the technical, operational and mathematical relevance of the study [16]. It helps to solve practical problems while producing an academically valued theoretical contribution [17]. The construction proceeds via thinking of design that makes projection into the future (artifact, creating theory,) and it fills conceptual and other knowledge gaps [18]. Agile Methods split apart the product into small growing builds. These builds are provided in repetition. At the end of the repetition, a working product is unfolded to the user and stakeholders of high importance. It helps in carrying out construction of software that is unpredictable and perceptions achieved from the review of repetition are employed to decide further step in development.

Network based Intrusion Prevention system (NIPS) is proposed applying signature rules-based prevention technique (often called inline prevention system) it's geared to help offer solution for Network-based security. Network Intrusion Prevention System (NIPS) anchor their decisions on data gotten by observing the traffic network to which the hosts are connected. NIPS sit intermediately between the network traffic movements, among two or more network interface, observing network dealings at a collection point they react to any case almost immediately. The unfeigned ability of NIPS is their power to forcefully stop traffic that is offensive.

NIPS examine the entire packet which goes through and then analyze the traffic for the attack patterns that are known, aimed to taint the system. When a pattern is aligned and the NIPS discovers an attack, it carries out an action in form of an alert, log, send and reset or blocked the accompanying packet stopping the attack from occurring, generate a notification. A magnanimous NIPS server can be set up on a backbone network, to monitor all traffic; or little systems can be frame-up to supervise traffic for certain particular server, switch, gateway, or router.

IV. SYSTEM ARCHITECTURAL DESIGN

The system architecture for the proposed system gives the overall view of how the system should be structured. Figure 1 shows the Network-based intrusion prevention system.

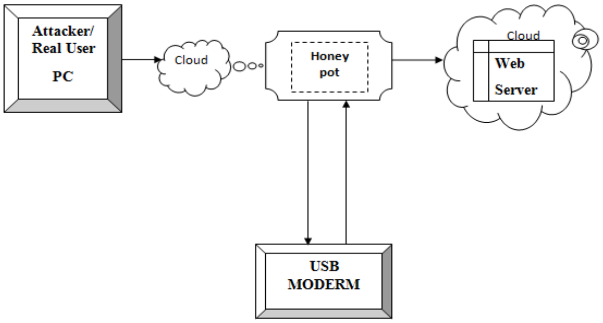


Figure 1 Architecture of the Proposed System

Network based Intrusion Prevention System (NIPS) is design to get hold of the network traffic from the network as it journeys to a host. This can be examined carefully for a particular signature or for strange or irregular manners. Honey pot program is used to supervise network movement. If any untrusting or anomaly behaviour takes place then it automatically prevent it, and then trigger an alert via an email and the message is then pass to the central computer system and administrator (which monitors the honey pot) then response is generated to stop intrusion, furthermore the administrator with the use of USB modern and a cell phone with some sort of short message code can also take decisions as regards to intrusion attempt either to confirm or delete. This research will use systems predefined rules- (signature)-based to predict, detect and prevent anomaly attacks.

A. Attacker / Real User Personal Computer

It's a computer used by attacker (unauthorized access) or real user to input text, malicious code, viruses that try to reach the server from the internet. Using the confusion matrix of two class problems having positive and negative class values, which in this case normal (Real User) and abnormal (attacker) classes. Table 1 shows the two-class confusion matrix.

Table 1 Confusion matrix for a two-class problem

	Positive	Negative
Positive	True Positive (TP)	False Positive (FP)
Negative	False Positive (FP)	True Positive (TP)

Identify real user and attacker is obtained as follows;
The accuracy (Acc) of the classifier is defined as:

$Acc = TP + TN / TP + FN + FP + TN$ - - - (1)

True Positive is the percentage of the positive cases that were classified correctly as they belonged to the normal (Real User) class, defined as follows:

$TPrate = TP / TP + FN$ - - - - (2)

False Positive is the percentage of the negative cases that were misclassified as they belonged to the normal class, defined as follows:

$FPrate = FP/ FP + TN$ - - - - (3)

These measures were employed to assess the purported intrusion detection system classifiers based on attacker and real user.

B. Honey pot

The honey pot is design to help the system discover intrusion which has the propensity to interrupt the intruder in gaining access to the entire network. When it is successful, then the attacker will not know that they are monitored. Figure 2 shows the structure of honey pot.

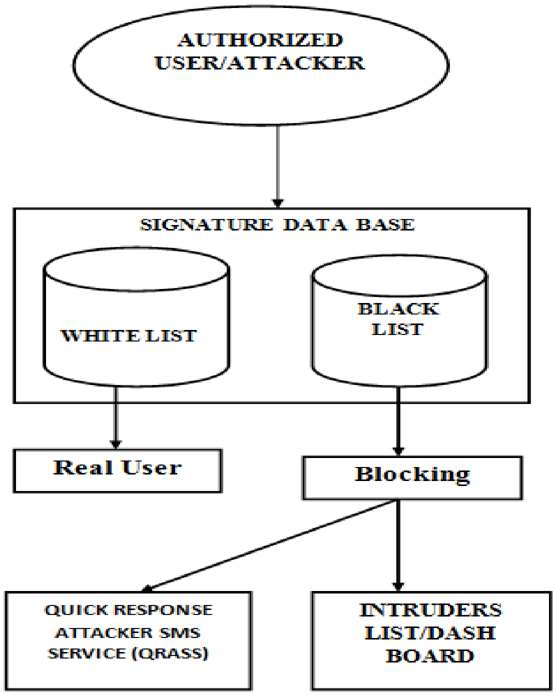


Figure 2 Honey Pot model for the proposed system

Honey pots carry the packet as input from the network and also supervise the time assigned for incoming stream. While supervising the time assigned and packet, honey pot discovers the malicious time assigned and ascertain distrustful stream and pull out the malicious stream from the traffic, and it work on and bring forth the new filtering regulation. Signatures are built from the filtering rule for intrusion detection. The seize packets are employed as an input in the honey pot and precede the packet to obtain the information for every specific system from the beginning of the packet. Honey pot come before the packet analysis and generate reply to occupy the client system from host.

- *White listing and Blacklisting (Signature Database)*

The data base contains the signatures i.e. predefined rules which include the IP address, users' password and name through which a legitimate user can access the protected servers. It also contains blocked blacklisted IP addresses, users' name, password which is threat to the protected server. Signature database stores previous patterns or behaviour of an attacker. It consists of IP address of attacker and real user and classified them into white list of real user IP address and blacklist of attacker IP address.

Certain rules are used for detection; these rules tally against network traffic data. Any divergence in the rule aligning operation is reported as an intrusion. The manner of the rules in the P-BEST rule base includes two layers. The first (lower) layer is employed to align certain kind of case such as number of user login, user IP and then fires new case by setting up a specific benchmark of distrust. Rules in the second (higher) layer process these suspicions and resolve whether the system should put up an alert or not. Figure 1 and Figure 2 shows intrusion detection rules.

- *Quick Response Attacker SMS Service*

The quick response attackers SMS service is designed to send an intrusion alert to the administrator via SMS, which also give the administrator the chance of responding to intrusion attempt very quickly, either blacklisting or white listing an intrusion attempt.

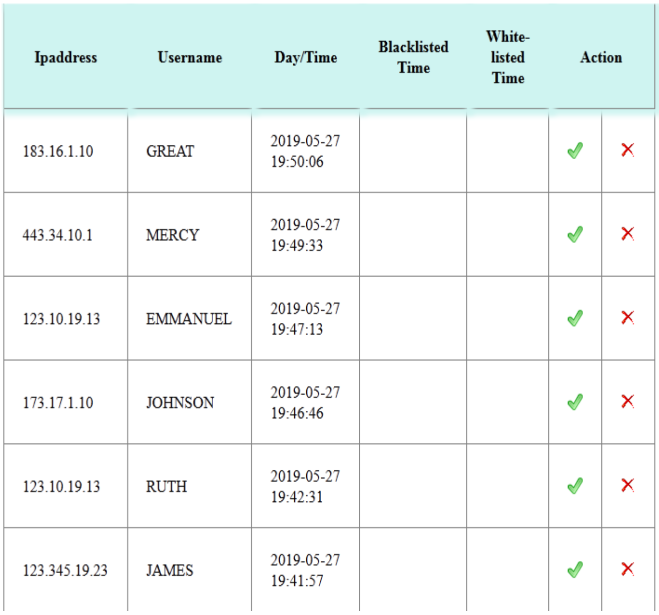
- *Intruders List/Dashboard*

Its use to outline various intrusion attempts which include intruders IP addresses, Location, User name, Password. It also gives the administrator the privilege to decide the fate of an intrusion attempt, either blacklisting or white-listing intrusion attempt.

V. RESULT AND DISCUSSION

The result for the simulation of the proposed system is presented. The results show the different aspect of the Hybrid cloud computing security using Network Based Intrusion prevention system. When an unregistered user tries to access the system, they are blocked and if such IP is not recognized by the admin, the user is regarded as intruder/ attacker and is blacklisted. A quick response attacker SMS is being sent by the administrator for a prompt response if the admin is not on seat at the time the intruder attacks the system. This SMS service provides a quick response to the system by retrieving and blacklisting the supposed attacker. Below are the figures and tables that show the blacklisted intruders and tables showing their frequency of attempt and the graphical representation both from the simulated interface and QRASS.

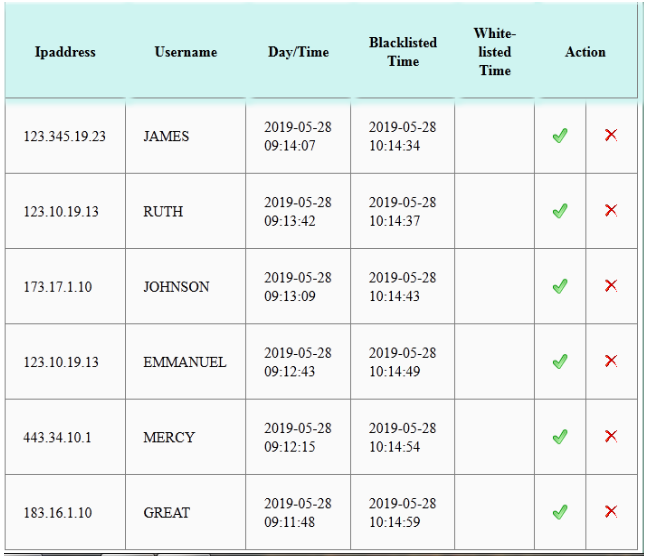
A. *Blacklisted Intruders*



Ipaddress	Username	Day/Time	Blacklisted Time	White-listed Time	Action	
183.16.1.10	GREAT	2019-05-27 19:50:06			✓	✗
443.34.10.1	MERCY	2019-05-27 19:49:33			✓	✗
123.10.19.13	EMMANUEL	2019-05-27 19:47:13			✓	✗
173.17.1.10	JOHNSON	2019-05-27 19:46:46			✓	✗
123.10.19.13	RUTH	2019-05-27 19:42:31			✓	✗
123.345.19.23	JAMES	2019-05-27 19:41:57			✓	✗

Figure 3 Blacklisted Intruders via the simulated system

B. *QRASS Black List*



Ipaddress	Username	Day/Time	Blacklisted Time	White-listed Time	Action	
123.345.19.23	JAMES	2019-05-28 09:14:07	2019-05-28 10:14:34		✓	✗
123.10.19.13	RUTH	2019-05-28 09:13:42	2019-05-28 10:14:37		✓	✗
173.17.1.10	JOHNSON	2019-05-28 09:13:09	2019-05-28 10:14:43		✓	✗
123.10.19.13	EMMANUEL	2019-05-28 09:12:43	2019-05-28 10:14:49		✓	✗
443.34.10.1	MERCY	2019-05-28 09:12:15	2019-05-28 10:14:54		✓	✗
183.16.1.10	GREAT	2019-05-28 09:11:48	2019-05-28 10:14:59		✓	✗

Figure 4 Blacklisted Intruders via QRASS

C. Frequency Tables and Graphical Representation

Table 2 Intruders frequency table for the simulated system

IP Address	Intruders username	Date	Frequency/ No of attempt
183.16.1.10	GREAT	2019/5/27	6
443.34.101	MERCY	2019/5/27	8
123.10.19.13	EMMANUEL	2019/5/27	9
173.17.1.10	JOHNSON	2019/5/27	7
123.10.19.13	RUTH	2019/5/27	5
123.345.19.23	JAMES	2019/5/27	8

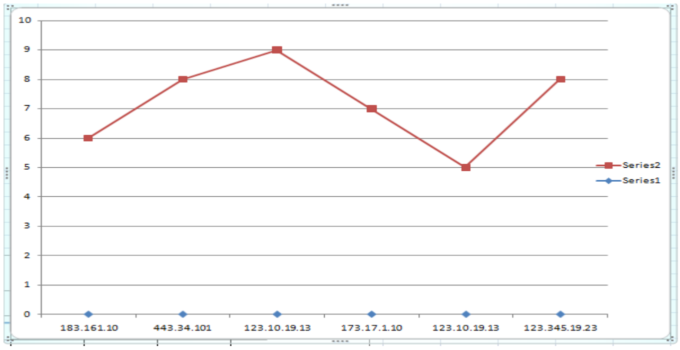


Fig. 5 Graphical representation of the frequencies of hackers' attempt

Table 3 Intruders frequency table for QRASS

IP Address	Intruders username	Date	Frequency/ No of attempt
123.345.19.23	JAMES	2019/5/28	1
123.10.19.13	RUTH	2019/5/28	2
173.17.1.10	JOHNSON	2019/5/28	1
123.10.19.13	EMMANUEL	2019/5/28	1
443.34.101	MERCY	2019/5/28	2
183.161.10	GREAT	2019/5/28	1

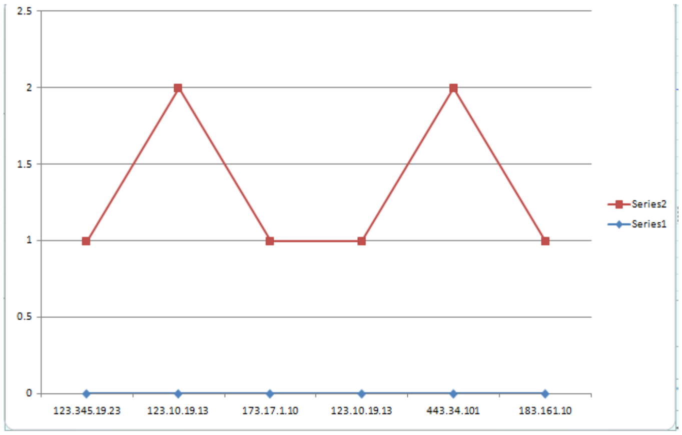


Fig. 6 Graphical representation of frequencies of hackers' attempt using QRASS to blacklist

D. Comparing with Existing System

Table 4 Comparing Existing System with Proposed System

System		Security	Detect novel attacks	Prevent novel attacks	Sends Alert by Email	Host Based /Network Based	Black-list/white-list intruder Via SMS	Send alert via SMS
Ajeet et al, 2012	Hybrid IDS in Cloud Computing	Strong	Yes	No	Yes	Host Based	No	No
Proposed System	IPS in Cloud Computing	Strong	Yes	Yes	Yes	Network Based	Yes	Yes

E. Result Discussion

In other to quantify the operation of our proposed approach, successions of experimentations were carried out. To have access to the system, the user logs in providing a username and a password. The system automatically gets the IP address of the user and verifies it if the user's IP is duly registered, the verification will be successful and access granted to the user. But, if the user verification is not successful, which means that the user is not a legal user and such user is regarded as an intruder and therefore all details of the user especially the IP address will be blacklisted. The admin has the right to allow users and to delete users especially if the users are new users of the system and their details have not been saved.

Figure 3 shows list of blocked user IP address of those trying to have access to the system. Here in the intruder has been blocked not to gain access to the system but has not been blacklisted; at this point the intruder still has the chances of repeated trial hence he has not been blacklisted. It consists of "IP address", "Username", "Day/Time", "Action" of intrusion. Action column consists of (confirm symbol) and (delete symbol); admin decide to confirm (white listed) or delete (blacklisted), if the admin clicks the delete button the record will be blacklisted and if admin clicked to confirm the user details, then the user will be white-listed.

Figure 4 Shows black listed intruder list, at this point the intruder has lost the chances of further attempt; the system doesn't have any information about the intruder apart from the already saved one. These black listed intruders were carried out by the quick response attacker SMS service (QRASS) and record huge success. A message was sent by the admin to blacklist the attacker from accessing the data stored in the cloud.

Table 2 shows intruders' frequency table when testing the simulated system to blacklist an intruder, user name "EMMANUEL" have the highest numbers of attempt (9) followed by "MERCY and JAMES", with eight (8). User name JOHNSON attempted seven (7) times, while user name RUTH happen to be the least with just five (5) attempts as shown. Figure 5 and figure 6 are graphical representations used to illustrate the frequency of attempts when the system is simulated and when the QRASS was sent to black list attackers.

Table 4 is the comparison of the existing system and the proposed system. From the experimentation, it shows that the proposed system is preferred to the existing system having all the features of the existing system and some additional features like the SMS alert and quick response attacker SMS (QRASS).

VI. CONCLUSION

Hybrid clouds proffer a great tractability to business while providing options in terms of preserving control and security. Hybrid clouds are normally deployed by organizations on their volition to push part of their workloads to public clouds either for cloud bursting purposes or for projects requiring faster implementation. Because hybrid clouds differ based on company needs and pattern of implementation, there are no size-fits all solution. Since hybrid domain imply both on-premise and public cloud providers, some extra infrastructure security preconditions come into the picture, which are usually link up with public clouds. Any business planning to engage hybrid clouds should understand the various security demands and adhere to the industry best practices to extenuate any risks. Once secure, hybrid cloud domain can assist business passage, more application into public clouds, providing extra cost savings. Public and private clouds are in two other whitepapers where security precondition and solution on these domains are discussed. Adding the quick response attacker SMS service (QRASS) it makes the proposed security system to identify an intrusion attempt in a timely manner and respond quickly whether to blacklist or white-list an intrusion attempt, on like other systems that depend solely on the intruders dashboard for such action (white-listing and blacklisting) to be carried out, which takes longer time and as well put the system on risk.

REFERENCES

[1]. G. Robert. "*Privacy in the clouds: risks to privacy and confidentiality from cloud computing*." In Proceedings of the World privacy forum, **2012**.

[2]. Badger, L., Tim G., Robert P., and Jeff V., "*Cloud computing synopsis and recommendations.*" National Institute of Standards and Technology (*NIST),* special publication 800 pp.**146 2012**.

[3]. Stolfo, S. J., S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, S. W. Smith, eds. *Insider attack and cyber security: beyond the hacker*., Springer Science & Business Media, Vol.**39, 2008**.

[4]. S. Richard, S. Bahargam, A. Bestavros. "*Software-defined ids for securing embedded mobile devices."* In *2013 IEEE High Performance Extreme Computing Conference (HPEC)*, pp. **1-7**, **2013**.

[5]. N. H. Anh, D. Choi. "*Application of data mining to network intrusion detection: classifier selection model."* In *Asia-Pacific Network Operations and Management Symposium*, Springer, Berlin, Heidelberg, pp.**399-408**., **2008**.

[6]. L. Wei., "A genetic algorithm approach to network intrusion detection." *SANS Institute, USA* Vol.**15**, pp.**209-216**, **2004**.

[7]. G. R. Hui, M. Zulkernine, P. Abolmaesumi. "*A software implementation of a genetic algorithm-based approach to network intrusion detection."* In Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Network, IEEE, pp.**246-253**., **2005**.

[8]. Xiang, C., and S. M. Lim. "Design of multiple-level hybrid classifier for intrusion detection system." In *2005 IEEE Workshop on Machine Learning for Signal Processing*, pp.**117-122**., **2005**.

[9]. Shacham H. and Waters B. (2008). "Compact proofs of irretrievability," in Proceedings of Asiacrypt'08 of LNCS, vol.**5350**, pp.**90–107**.

[10]. Scarfone, Karen A., and Peter M. Mell. *Guide to Intrusion Detection and Prevention Systems (IDPS)*| National Institute of Standards and Technology *(NIST).* No. Special Publication (NIST SP), pp.**800-94**. **2007**.

[11]. Reda M. (2013). "A hybrid network intrusion detection framework based on random forests and weighted k-means." Ain Shams Engineering Journal 4.4, 753-762.

[12]. H. Jin, M. Dong, K. Ota, Minyu F., G. Wang. "*NetSecCC: A scalable and fault-tolerant architecture for cloud computing security*." Peer-to-Peer Networking and Applications, Vol.**9**, Issue.**1** pp.**67-81, 2016**.

[13]. Alharkan, T., P. Martin. "*Idsaas: Intrusion detection system as a service in public clouds.*" In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012), IEEE Computer Society, pp.**686-687**. **2012**.

[14]. Mohamed, K. Kifayat, Qi S., W. Hurst. "*A system for intrusion prediction in cloud computing*." In Proceedings of the International Conference on Internet of things and Cloud Computing, ACM, pp.**35, 2016**.

[15]. R. Sumant, Mariki M. E., E. Smith. "*The management of security in cloud computing*." In 2010 Information Security for South Africa, IEEE, pp.**1-7**, **2010**.

[16]. K. Eero, K. Lukka, Arto S., "*The constructive approach in management accounting research*.", Journal of management accounting research, Vol.**5**, Issue.**1** pp.**243-264, 1993**.

[17]. L. Liisa, J. Junnonen, S. Kärnä, L. Pekuri. "*The constructive research approach: problem solving for complex projects*." Designs, Methods and Practices for Research of Project Management. Gower, **2016**.

[18]. G. D. Crnkovic, "*Constructive research and info-computational knowledge generation*." In Model-Based Reasoning in Science and Technology, Springer, Berlin, Heidelberg, pp.**359-380**, **2010**.

Authors Profile

Mr. P. J. Ebiriene pursed Bachelor of Science from Rivers State University, Port Harcourt, Nigeria in 2014. He is currently pursuing Masters of Science from Department of Computer Science, Rivers State University, Nigeria since 2016. His main research work focuses on Intrusion Detection System. He has 1 year of research experience

Dr N. D Nwiabu pursed Bachelor of Science from Kwame Nkrumah University of Science & Technology, Kumasi, Ghana in 2002, and Master of Science from University of Port Harcourt, Nigeria in year 2006. He also obtained PgCert in Research Methods and PhD from Robert Gordon University, Aberdeen, UK in 2009. He is currently working as a lecturer in Department of Computer Science, Rivers State University, Nigeria since 2012. He is a member of IEEE computer society since 2011, a member of the NCS since 2005 and CPN since 2005. He has numerous publications and conference papers in reputed international journals including IEEE and it's also available online. His main research work focuses on Situation-aware systems, Pipeline monitoring, Decision support system, prediction system, etc. His work won awards in the North Sea, IEEE, MIT and EIM. His work has also got an application area in sociology to monitor crime. He has 16 years of teaching experience and over 10 years of Research Experience.