ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Implementation of Artificial Intelligence for IDS in Cloud Data Centers

Snehal G. Kene[1], Deepti P. Theng[2]

PG Student, Department of Computer Science & Engineering, G.H.R.C.E Nagpur, India[1]

Assistant Professor, Department of Computer Science & Engineering, G.H.R.C.E Nagpur, India[2]

ABSTRACT: Cloud computing provides large scale computing resource to each customers. Cloud systems can be threatened by numerous attacks as cloud provides services to no trustworthy system. As the speedy usage of personal computer system and computer network in business organization and government organization are Bringing up day by day, the computer network is the mass medium over which attacks are put together. It comes final result in completely destroyed, unauthorized utilization and modifies in private data and demeans the reliability of computer network. To providing protection in computer network Artificial intelligence has latterly contributed intrusion detection system. This paper presents intrusion detection system which automatically updates the suspicious activity of cloud users therefore whenever new user try to access the data or try to use cloud it will compare with the log database which is present at administrator side.

KEYWORDS: Cloud Computing; Cloud Security; Intrusion Detection System; Signature; Anomaly

I. INTRODUCTION

As Cloud Computing is the rapidly growing field of IT [1]. Cloud Computing is defined as an Internet based computing in which virtually shared servers that is data centers provide software, platform, infrastructure, policies and many resources [2]. A cloud data center can be defined from a different perspectives, and the most popular are categorized by IaaS, PaaS, and SaaS proposed by the NIST [3]. However, with the increasing use of cloud computing, security issues are came out on a growing scale. It is important to solve these security issues to contribute to the wider applications of cloud computing [4]. The increasing number of network security related incidents makes it necessary for organizations to actively protect their sensitive data with the installation of intrusion detection systems (IDS). To overcome such problems, an intrusion detection system (IDS) comes into play. The IDS plays very important role in the security of cloud and instead of detecting only known attacks, it can detect many known and unknown attacks [5]. IDS are defined to preserve the confidentiality, integrity, and availability of network [6]. IDS could be software, hardware or a combination of both. It captures the data from the network under examination and notify to the network manager by mailing or logging the intrusion event [7]. Rest of the paper is structured as follows: Section II describes the system architecture, Section III result and discussion and section IV contains conclusion and references.

II. LITERATURE REVIEW

Over the past 3 decades, there has been a large increase in the number of real problems correlated to; Fault detection (Monitoring), Safety of multipart systems (Rockets, Airplanes, Cars), and Monitoring physiological variables in patient healthcare. More recently, anomaly detection in information technology settings is becoming vitally important and gaining momentum. This is due to the occurrence of exploding information and the model of cloud computing which has formed a demand for huge number of servers known as data centers. A data center is a very intricate operating environment and its smooth operation is dangerous to keep enterprise businesses running powerfully. While the complication and size of the data centers is constantly increasing, methods to monitor the numerous processes and metrics are still relatively undeveloped. Unnecessary to say, monitoring using dependable methods that are light weight, and scale with increasing number of servers and number of metrics is necessary for optimal and economical operations. Detection of immediate or fast changes, untimely prediction of imminent anomalies, and detection of anomalies in a relatively stable system typically constitute the taxonomy of change-point detection techniques [8]. IDS is split into two categories: misuse detection systems and anomaly detection systems [9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Misuse detection is used to recognize intrusions that match known attack scenarios. However, anomaly detection is an attempt to explore for malicious behavior that deviates from recognized nor-mal patterns. In order to detect the intrusion, different approaches have been developed and proposed over the last decade. In the early stage, rule based expert systems and statistical approaches are two typical ways to detect intrusion. A rule-based expert IDS can detect some well-known intrusions with high detection rate, but it is difficult to detect new intrusions, and its signature database needs to be updated manually and frequently. This paper advances anomaly detection schemes by considering ranking of anomalies based on severity in conjunction with flagging anomalies.

III. SYSTEM FLOW

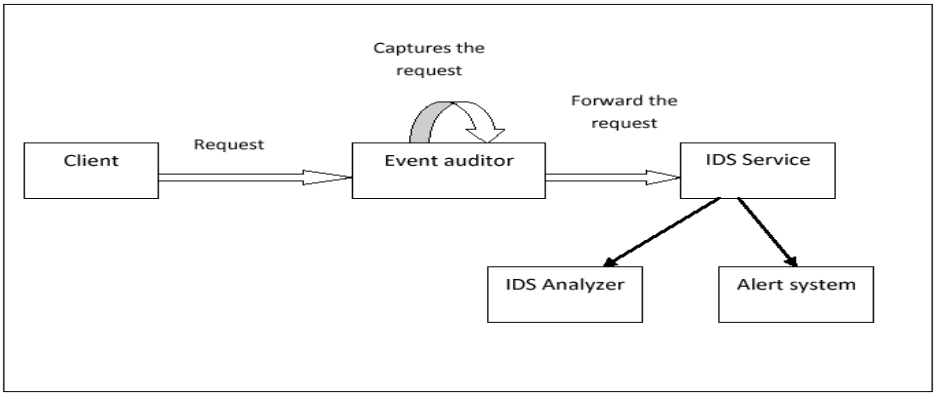

Figure 1: Client request with proposed system

The Intrusion Detection Service (IDS) [8] service enhances a clouds protection level by providing two methods of intrusion detection. First approach is performance approach which orders how recent user actions are compared to the normal behaviour. The second approach is information approach that marks cognized trails resulted by attacks or some sequences of actions from the user who represents an attack. The inspected data is sent to the IDS service core, which examines the conduct by using artificial intelligence to find deflections. This has two subsystems namely analyzer system and alert system. The analyzer uses the profile history database to find out the distance within a distinctive user behavior and the suspicious behavior and conveys this to the IDS service. The rules analyzer obtains audit packages and finds out if a rule in the database is worn out. It delivers the result to the IDS service core. With such responses, the IDS find out the intruder that the action comprises an attack and alarms the other nodes if the suspicious behaviour is high. This subsystem will work when intrusion is detected. If any node among the cloud system is affected by intrusion then this alert system will alert the remaining nodes about the intrusion.

The storage service is a database system which contains two types of services namely information based service and performance based service. Whenever a node gets requests or responses, the analyzer system compares the node information in the storage service. This paper used audit information from a log system as well the communication system to evaluate the information based system. The created a series of rules to illustrate security policies that the IDS should monitor. The information service is nothing but set of rules which is formed from previous attacks.

IV. RESULTS AND DISCUSSIONS

1. Login Page:

In login page we provide userid and password so that any user who is an authenticated person is able to login in the system to enjoy the environment provided by the cloud for communication. The following screen shot gives the complete idea about the login page.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Fig 2: login page for end users

For the end users it is the easiest way to login with the cloud communication. There is link provided for the new users which are not registered with the cloud to register themselves with the cloud environment. After the registration of new user the request of registration is sent directly to the admin for activation of the user. The admin have to check the documents of new registered user physically. After verifying the documents the admin decide the activation of new user. Only after that the user is able to login.

2. Admin Login Page:

Fig 3: Admin login page

In admin login we provide the admin with some functions like main, view attacker and logout. Main contains two services user authentication and log maintenance. In user authentication admin would check the log and packet data of particular user and then provide the authentication to that user. View attacker provides the attackers view that make the attack on system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

2. User Authentication and Log Monitoring

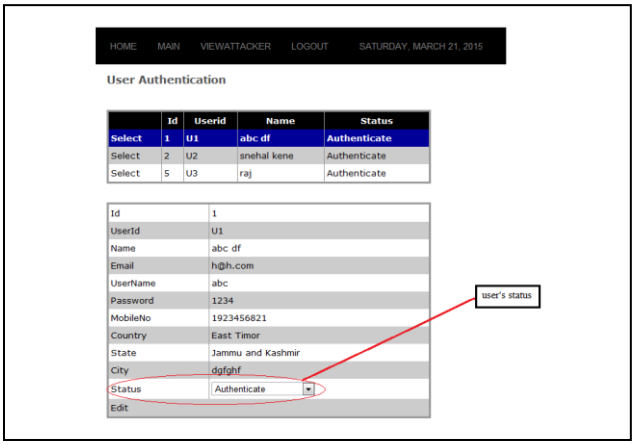

Fig 4: User Authentication

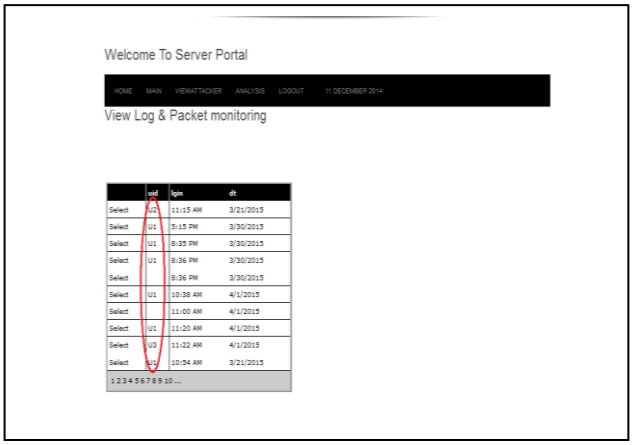

Fig 5: Log Monitoring and packet monitoring

In admin login page we provide user id and password so that any user who try to login to the system, an admin will analyse the user. Whether the user is authorised or not, if the user is genuine then admin change his states to authenticate otherwise keep it as new.

System provide log monitoring in which we keep the log maintainance of user. System provide unique id (such as U1, U2, and so on as shown in fig 11) to each user so that noone can get or hack the user log. Log and packet monitoring page contain unique user id, login time, date and log out time and the file which is uploaded and downloaded by the user.

4. View Attacker Record:

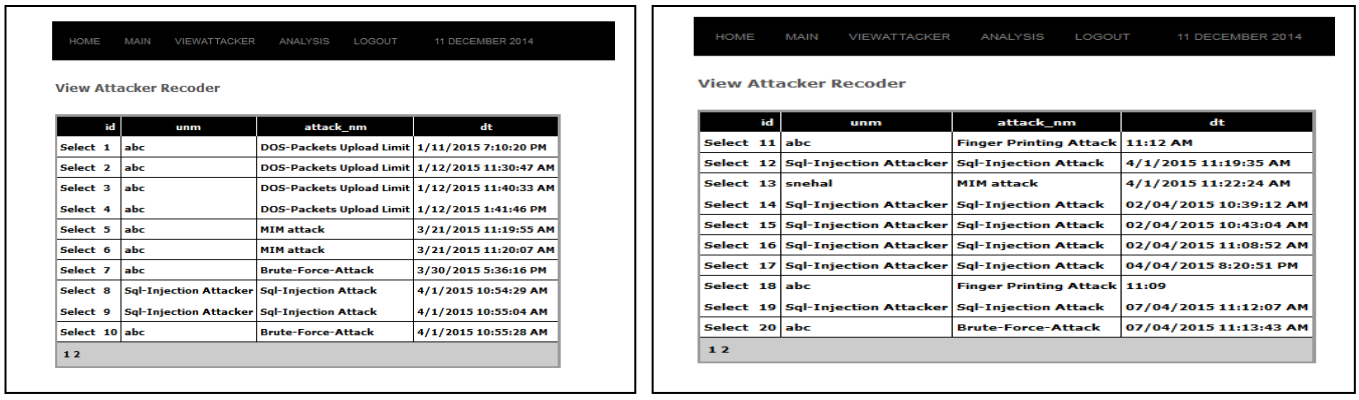

Fig 6: Attacker Record

The admin side shows the attacker view in which admin keep the record of previously occured attacks. The proposed system detect some attacks like DDos, Man-in-middle attack, fingerprinting attack, SQL injection and brute force attack . The attacker record contain user name, user id, attack type and date of occurance

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

V. CONCLUSION

As data centers grow in size and complexity, automated techniques to detect anomalous behavior in the data centers become important. We presented automated intrusion detection technique compares current user activities against previously loaded logs of users. System offers the potential advantages of reducing the manpower needed in monitoring, increasing detection efficiency, providing data that would otherwise not be available, helping the information security community learn about new vulnerabilities and providing legal evidence. We have developed secure cloud storage system architecture and have shown that the system has several superior characteristics such as constant encryption and decryption of data. From our experiments, we observe that both encryption and decryption computations are efficient on the client side as well as server side.

REFERENCES

[1] Snehal G. Kene, Deepti P. Theng "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges", IEEE sponsored 2nd international conference on electronics and communication systems icecs '2015.
[2] Shefali Singh, Krati Saxena, Zubair Khan "Intrusion Detection Based On Artificial Intelligence Techniques", International Conference Of Advance Research And Innovation (Icari-2014).
[3] Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, And Junwei Cao"Collaborative Network Security In Multi-Tenant Data Center For Cloud Computing", Tsinghua Science AndTechnology 1, February 2014.
[4] P. Praveen Kumar, K. Bhaskar Naik, "A Survey on Cloud Based Intrusion Detection System" International Journal of Software and Web Sciences (IJSWS) 2013.
[5] R. Quick, "5 reasons enterprises are frightened of the cloud", http://thenextweb.com/insider/2013/09/11/5 reasons enterprises- are-frightened-of-the-cloud, 2013.
[6] R. Bace, P. Mell, "Intrusion Detection Systems", National Institute of Standards and Technology (NIST), Technical Report, 800-31, 2001.
[7] U. Oktay, O. K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", ISBN: 978-1-4673-5613-8, 2013, IEEE, pp. 98-104.
[8] Krishnamurthy Viswanathan, Lakshminarayan Choudur, Vanish Talwar, Chengwei Wang*, Greg Macdonald, Wade Satterfield, "Ranking Anomalies In Data Centers" 2012 IEEE.
[9] A. Haeberlen," An Efficient Intrusion Detection Model Based on Fast Inductive Learning," Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007. Tavel, P. 2007.
[10] Sanjay Ram M, Velmurugan N, Thirukumaran S, "Effective Analysis of Cloud Based Intrusion Detection System" International Journal of Computer Applications & Information Technology Vol. I, Issue II, September, 2012.
[11] Theng, D.; Hande, K.N., "VM Management for Cross-Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2012 International Conference on , vol., no., pp.731,735, 11-13 May 2012
[12] Theng, D., "Efficient Heterogeneous Computational Strategy for Cross-Cloud Computing Environment," Emerging Research in Computing, Information, Communication and Applications (ERCICA), 2014 Second International Conference on, vol., no., pp.8,17, 1-2 August 2014.

BIOGRAPHY

Snehal G. Kene has completed Bachelor of Engineering (Computer Science & Engineering) from Wainganga college of Engineering & Management, Nagpur in 2013. She is currently pursuing final year of M.Tech (Computer Science & Engineering) from G.H. Raisoni College of Engineering, Nagpur. Ms. Snehal G. Kene has presented 1 paper in international conference.

Prof. Deepti Theng received her BE and MTech in Computer Science and Engineering in 2007 and 2012 respectively. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering. She has totaled 30 National and International papers published including publications of IEEE, Elsevier, Springer and many more. She is an active Professional Member of IEEE, SMC, ACM, and CSI. Her research interest includes Parallel and Distributed Computing, Cloud Computing, High performance Computer Architecture.