National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Cloud Security Mechanism : Prevent Access with Location

Prof. Prashant D. Londhe
Department of Computer Science, Gogate-Jogalekar College, Ratnagiri, Maharashtra, India

ABSTRACT

Cloud Services are efficiently used in large organizations and educational sector. Security is major concern whenever anyone is using cloud services and operating system. Cloud Security is highly vulnerable to threats, which results in Data loss. The purpose of this research is to develop Cloud security model. In this paper, we have developed cloud security mechanism with location tracing. We have also analyzed various security mechanisms available and trying to develop a model, which will be least costly and affordable to small organization.
Keywords : Cloud Security, Honeypot, Tonido, Security, Location Tracing.

I. INTRODUCTION

Many Industries, organizations and Individual person uses Cloud as Data storage mechanism in increasing way. High scale Company also do not store the data on own servers, they choose cloud Storage considering reliability. Due to this Cloud security becomes important security aspects due to confidential information and responsive data[4]. Cloud computing is very emerging computer science mechanism which provides computing services and data storage at very effective cost. This cost is quite acceptable and affordable consider metrics provided by parent cloud organization[1]. High availability, Cost saving feature and High scalability makes cloud services more favorite to use. There are three types of Service model used in Cloud architecture[2].

1) **IaaS (Infrastructure as a Service)** : Users get resources like CPU time, Processing power, Network Bandwidth and storage. After registering service user can treat is as its own machine having desired Operating System[2].

2) **PaaS (Platform as a Service)** : Users get resources like Hardware infrastructure and Networking environment. Many Large Scale organization uses this system as base of development[6].
3) **SaaS (Software as a Service)** : Users get access to application without any restriction on operating system, Network Bandwidth and Environment[5].

Figure 1 : Cloud Architecture

Characteristics of Cloud Architecture is as below[7]:-

1) **Scalability:-** Architecture changes according to demand of the application. If need is less it will take less space and high in case of higher with a single click.
2) **Cost-effectiveness:-** Cloud computing reduces hardware expenses, as hardware is provided by a vendor without any need of buying ,installing, configuring and maintaining server.
3) **Immediate availability:-** This applications are immediately available.
4) **Performance:-** Application are of high caliber providing proper output.
5) **Security:-** Cloud infrastructure is kept in safe data centers to ensure security with data back-up and recovery.

II. INTRUSION DETECTION SYSTEM

An Intrusion detection system (IDS) monitors cloud network traffic for abnormal, suspicious transaction, activities and provides alert messages if discovered. This prevents system form malicious activity or traffic which can be dangerous to server. It eventually blocks the activity in seek of security[6].

IDS are mainly developed to block intrusion detection but they are highly prone to false alarms. Therefore developer needs to set and configure IDS properly[14,18].

Different types of intrusion detection systems:-

A **Network intrusion detection system (NIDS)** is developed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network[18].

Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems[18].

Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software[20,21]

Anomaly-based intrusion detection systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity[12].

Historically, intrusion detection systems were categorized as passive or active; a passive IDS that detected malicious activity would generate alert or log entries, but would take no actions. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources[13].

Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems, and a version is available for Windows as well[15].

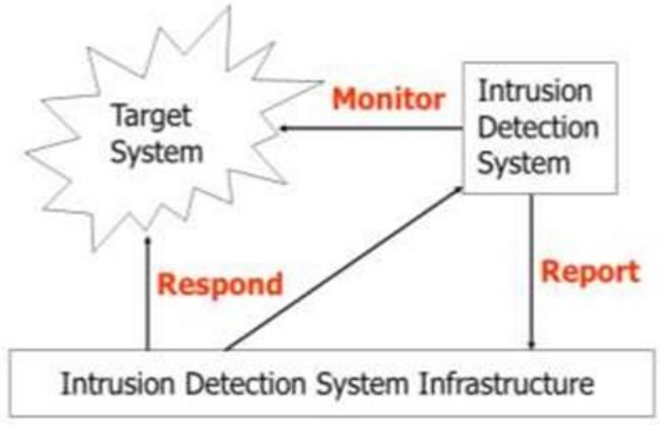

Figure 2: Intrusion Detection System Infrastructure

Capabilities of Intrusion detection systems:-

Intrusion detection systems monitor network traffic in order to detect when an intrusion is being carried out by unauthorized entities. IDSes do this by providing some or all of these functions to security professionals[15]. monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks[16]. providing administrators a way to tune, organize and understand relevant operating system audit trails and other logs that are often otherwise difficult to track or parse[20]. including an extensive attack signature database against which information from the system can be matched[15].recognizing and reporting when the IDS detects that data files have been altered; generating an alarm and notifying that security has been breached; and reacting to intruders by blocking them or blocking the server[11].

An intrusion detection system may be implemented as a software application running on customer hardware, or as a network security appliance; cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments[10].

Benefits of intrusion detection systems

Intrusion detection systems offer ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks, and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks[3,4].

Intrusion detection systems can also help the enterprise attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements[1].

Intrusion detection systems can also improve security response. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the operating systems of services being used. Using an IDS to collect this information can be much more efficient that manual censuses of connected systems[12].

III. RELATED WORK

Many research works is carried out considering Intrusion detection system. [8] represents intrusion detection based on regression models deciding the security features and load balancing monitoring techniques to maintain specific trust level. Paper [1] represents security features required to maintain trust in cloud system. A new security framework is defined based on Genetic algorithm. Author [9] states different strategically issues in cloud computing services regarding to security suggesting solutions. There are many ways to migrate cloud data securely in IaaS [2]. In [10] different Cloud Security threats are explained and discussed accordingly. Identify and Authentication management specifically focuses on secure access in cloud system with having proper

authority and privileges. The Markovian process algebra PEPA is used to evaluate the models behavior under different scenarios [5]. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider[5,6]. In paper[10,19], risk factors and solutions regarding these technologies are reviewed then current and future trends are discussed. This paper studies the modeling and analysis methods of some key problems of data security in cloud storage, such as encryption storage, integrity verification, access control, and verification and so on[12]. The simulation carried in [13] results demonstrate that the use of Support Vector Machines (SVM) is an efficient concept for simultaneous image segmentation and data protection.

IV. METHODOLOGY

1) Intrusion detection with mobile agents:

This method mainly focuses on device to device interconnecting security. It correlate on suspicious transactions in different monitored host. These agents are autonomous, goal-driven, reactive, social , adaptive and movable. IDS –AM-CLUST is defined in Java Agent Development (Version 3.7) and JDK 7 has following network traffic process[17].

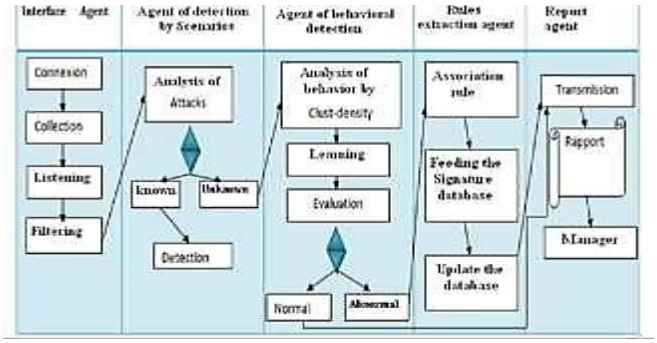

Figure 3 : IDS Architecture

2) Honeycomb :- Honeycomb is a pattern detection engine that monitors any network traffic that Honeyd receives and creates NIDS signatures for any patterns that occur regularly [5]. It is assumed that any regular traffic that Honeyd receives is malicious in nature, as honeypots in general serve no other network purpose and should not be receiving valid traffic. The advantages to use Honeycomb include reducing overhead caused by using additional programs to perform the same task and it is integrated into Honeyd hence will not have any synchronization issues. Additionally the creation of NIDS signatures could be very useful for detecting very new automated mobile malware and integrating the signatures into Network Intrusion Detection Systems on wireless networks to track the spread and effect of such malware [17].

3) Honeynet :- Honeynet is high interaction honeypot. Data capture, Data control and Data analysis are main three component of Honeynet. Data capturing is nothing but monitoring and capturing all activities regarding to cloud services. Data control checks possibility of attacker in cloud services. Data analysis is used to analysed retrieved information which will be responsible for detection of malicious attack.

V. EXPERIMENTAL SETUP & RESULT DISCUSSION

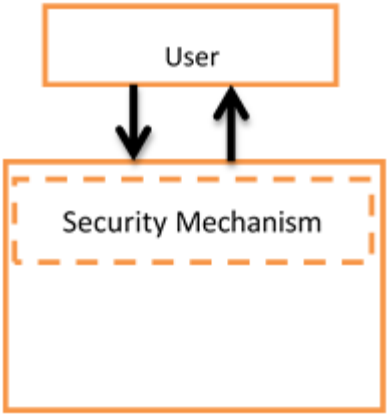

Figure 4: Proposed Model

In Figure we are proposing model for cloud security Where we are implementing security

part in cloud server itself. We are developing a private cloud server with Tonido Interface which provides free cloud architecture for Server as well as client (Computer or Mobile).

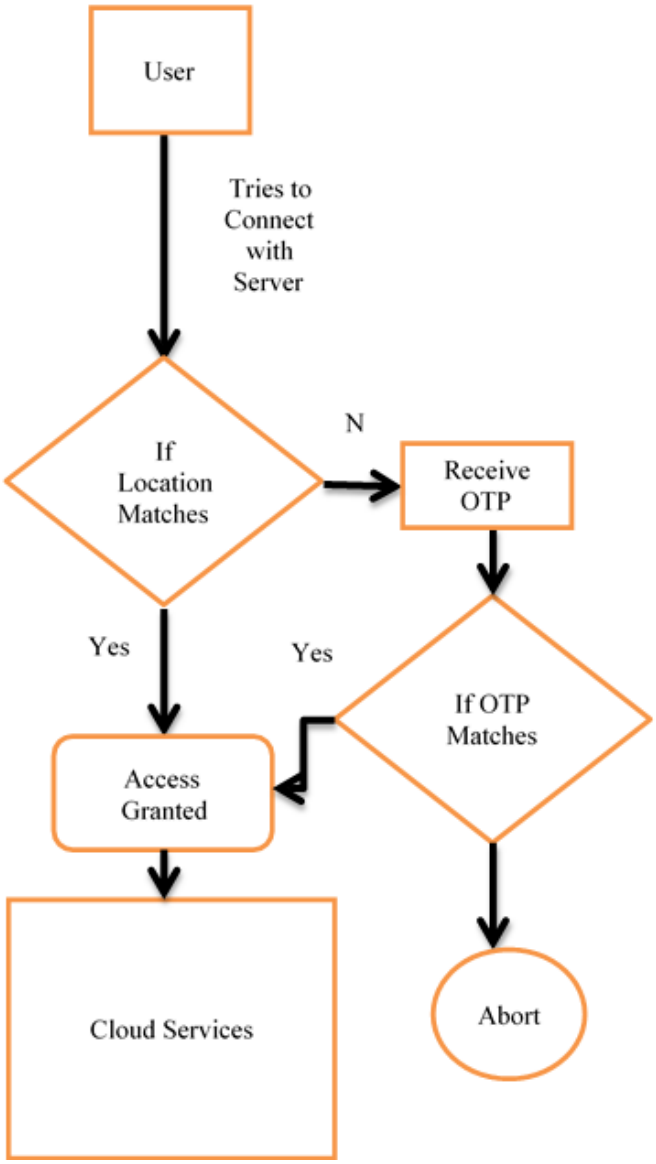

Figure 5 : System Flow of Proposed Model

The Experimental Setup is done with computer having following configuration

1) **Client Machine:-** Pentium Core2 Duo, 500 GB HDD, 4 GB RAM, Window 7 OS
2) **Server Machine:-** Pentium Core I5, 1 Tb HDD,8 GB RAM, Window 7 OS

Setup provides URL to access the server Machine. https://pdlpdlpdl.tonidoid.com is url for cloud server.

Currently we are considering location blockage to prevent unauthorized access to the application. The current location is recorded while logging from the person and if it is found different it is blocked by server otherwise allowed. False alarm is generated when authorized user tries to login from different location. In such case user will receive SMS to registered mobile and after submitting OTP user will be able to login to specified account.

VI. CONCLUSION

In this paper we are trying to avoid unauthorized access to cloud server developed based on Location tracing. We found it as one of the innovative and easiest way of implementing security mechanism. False alarm may arises when an authorized user is trying to login from the different location but it can be solved with OTP received. Still pros and cons are there like everything depends location at now case still there is chance of improvement.

VII. REFERENCES

[1]. Mall, S., & Saroj, S. K. (2018). A new security framework for cloud data. Procedia Computer Science, 143, 765–775. https: //doi.org/10.1016/j.procs.2018.10.397

[2]. Chawki, E. B., Ahmed, A., & Zakariae, T. (2018). IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors. Procedia Computer Science, 134, 328–333. https://doi.org/10.1016/j.procs.2018.07.180

[3]. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2016). A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network. Procedia Computer Science, 83, 1200–1206. https://doi.org/10.1016/j.procs.2016.04.249

[4]. Ghosh, P., Saha, A., & Phadikar, S. (2016). Penalty- Reward Based Instance Selection Method in Cloud Environment Using the Concept of Nearest Neighbor. Procedia Computer Science, 89, 82–89. https://doi.org/10.1016/j.procs.2016.06.012

[5]. Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57–65. https://doi.org/10.1016/j.aci.2016.03.001

[6]. Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. Procedia Computer Science, 127, 35–41. https://doi.org/10.1016/j.procs.2018.01.095

[7]. Kamil, S. N. S., & Thomas, N. (2018). Investigating the Cost of Transfer Delay on the Performance of Security in Cloud Computing. Electronic Notes in Theoretical Computer Science, 337, 105–117. https://doi.org/10.1016/j.entcs.2018.03.036

[8]. Khan, N., & Al-Yasiri, A. (2016). Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. Procedia Computer Science, 94, 485–490. https://doi.org/10.1016/j.procs.2016.08.075

[9]. Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud

[10]. Computing. Procedia Computer Science, 125(2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

[11]. Majhi, S. K., & Dhal, S. K. (2016). Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation. Physics Procedia, 78(December 2015), 33–39. https://doi.org/10.1016/j.procs.2016.02.007

[12]. Mall, S., & Saroj, S. K. (2018). A new security framework for cloud data. Procedia Computer Science, 143, 765–775. https://doi.org/10.1016/j.procs.2018.10.397

[13]. Manogaran, G., Thota, C., & Kumar, M. V. (2016). MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing. Procedia Computer Science, 87, 128–133. https://doi.org/10.1016/j.procs.2016.05.138

[14]. Marwan, M., Kartit, A., & Ouahmane, H. (2018). Security enhancement in healthcare cloud using machine learning. Procedia Computer Science, 127, 388–397. https://doi.org/10.1016/j.procs.2018.01.136

[15]. Mazini, M., Shirazi, B., & Mahdavi, I. (2018). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2018.03.011

[16]. Prasad, V. K., Shah, M., Patel, N., & Bhavsar, M. (2018). Inspection of Trust Based Cloud Using Security and Capacity Management at an IaaS Level. Procedia Computer Science, 132(Iccids), 1280–1289. https://doi.org/10.1016/j.procs.2018.05.044

[17]. Saadi, C., & Chaoui, H. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. Procedia Computer Science, 85(Cms), 433–442. https://doi.org/10.1016/j.procs.2016.05.189

[18]. Saadi, C., & Chaoui, H. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. Procedia Computer Science, 85(Cms), 433–442. https://doi.org/10.1016/j.procs.2016.05.189

[19]. Saeed, A., Ahmadinia, A., Javed, A., & Larijani, H. (2016). Random neural network based intelligent intrusion detection for wireless sensor networks. Procedia Computer Science, 80, 2372–2376. https://doi.org/10.1016/j.procs.2016.05.453

[20]. Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of

Things: A review. Procedia Computer Science, 112, 1516–1522. https://doi.org/10.1016/j.procs.2017.08.050

[21]. Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and Access Management as Security- as-a-Service from Clouds. Procedia Computer Science, 79, 170–174. https://doi.org/10.1016/j.procs.2016.03.117

[22]. Wang, R. (2017). Research on Data Security Technology Based on Cloud Storage. Procedia Engineering, 174, 1340–1355. https://doi.org/10.1016/j.proeng.2017.01.286

Cite this article as :

Sh