International Journal For Technological Research In Engineering
Volume 2, Issue 8, April-2015 *ISSN (Online): 2347 - 4718*

SURVEY ON INTRUSION DETECTION SYSTEM IN CLOUD COMPUTING

Sandeep Kaur[1], Divya Sourbhi[2], Shailendra Narayan Singh[3]
Amity School of Engineering, Amity University, Noida, India

Abstract: Cloud computing is a buzz word today. It provides on demand services to the end users with more of flexibility and less of investment. The technology uses various standards, protocols and formats for management. As the use of cloud computing is increasing so its security issues. So one of the major concerns today is how to protect data from theft. This paper explains some of the intrusions and some techniques to protect data from those intrusions.
Keywords: Cloud Computing, Intrusion, Intrusion Detection Ssytem, Intrusion Prevention System, Intrusion Detection and Prevetion System

I. INTRODUCTION

For last few years Cloud computing is emerging as the fastest growing technology. It provides scalable, on demand infrastructure and services to the user. Cloud users rent the usage from a third-party provider as they do not own the physical infrastructure. They consume resources as a service and pay only for resources they use.[4] What they only need is a personal computer and internet connection. Once a cloud is established it has three basic models: Software as a Service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS). SaaS facilitates the use of services and applications hosted in the cloud. It makes the user to install all the software directly in the cloud only, no need for having more copies on the our device where the application is running. PaaS facilitates access to the platform so that user can deploy their software and applications in cloud. It allows the user to rent the servers, operating systems and other hardware over the internet. IaaS provisions processing, storage, network and other fundamental capabilities. Cloud computing is progressing with great pace but still is in its infancy. So security is major concern for all. As cloud services are provided through internet; it runs through various standard protocols, so security of data is a key issue. Data is travelling over the internet, stored at remote location, and cloud providers serve multiple customers simultaneously which raises the number of possible breaches significantly. Cloud computing emerge as promising technology in order to provide the services remotely. But there are many security issues in cloud computing. For example in February, 2010, the Amazon network host service, S3 (Simple Storage Service) was broken down for 4 hours. This made people think about the security of cloud computing again. So security is major issue which cannot be neglected. Rest of the paper is organized as follow. Section 2 discusses various attacks applicable in cloud computing. Section 3 discusses various intrusion detection measures. Section 4 introduces various intrusion detection systems. Section 5 explains intrusion prevention system. Section 6 explains intrusion detection and prevention system and section 7 concludes with references at the end.

II. INTRUSION TO CLOUD SYSTEM

This section explains various types of intrusion attacks which can be done on cloud services.

A. Insider attack

Any malignant assault done on a computer system or a network by an individual who has full approved access to cloud assets goes under insider attacks. These sorts of intrusion pose real danger as a large portion of the information ruptures are done by approved persons. Insider attacks don't get effortlessly recognized as most associations concentrate on security from outer attacks [1]

B. Flooding attack

In this kind of attacks the victimized person gets overpowered with network packets, for example, TCP, UDP, ICMP or blend of these. The victimized person (server) gets to be so over weighed with packets that lead to incomplete connection request and no more ready to process honest to goodness demands. In case of cloud, DoS or DDoS attackss are the sort of surge attacks where the client is denied of administrations which he regularly hopes to have. It doesn't really bring about burglary of any data however can cost an organization a lot of time and cash [3]

C. User to root attack

Attacker with the help of packet sniffer can intercept data flowing in the network which can lead to unauthorized access to sensitive data. A sniffer cannot cause network damage but can steal PINs, password and other confidential data especially data which is in plain text. Buffer overflow is used in whole process; in which a large amount of data is sent, beyond the capacity of the buffer and information is captured by the attacker with this overflowed data. [17]

D. Port scanning

It is an act of scanning computer's port. It tells us about open ports and closed port. A port is an important part when we are working on internet. It acts as a gateway from where all the data comes in and goes out of computer. Port scanning techniques is used by the technicians to audit computer for vulnerabilities. However it is also used by the hackers to target victims. They try to find out open port and attack on the services running into it [5]. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning

attacks

E. Backdoor channel attack
It is a kind of passive attack used to get the confidential data by attacking the infected machine. The hacker gets the control of infected machine's resources by authentication and make it zombie to initiate DDos attacks.[3,5]

III. INTRUSION DETECTION SYSTEM(IDS)

Intrusion detection system is a software application which monitors target system for any malicious activity. It inspects the network to find any activity which can be considered to compromise the confidentiality, integrity and security of the system.

A. Signature Based Intrusion Detection System
This framework deals with predefined rules. They work on known pattern. "Marks" looks like the foot shaped impressions of attack. Each intrusion abandons a few foot shaped impressions and this foot shaped impressions are known as 'Signature'. For each action they match the signature of that movement with the database and in the event if it matches, they report it to head. Figure 1 shows how Signature based IDS functions. The greater part of the systems utilizes Signature based intrusion detection system as they give adequate precise results. These systems are easy to execute and are light weight. They create less false alarms which spares the administrator's time.

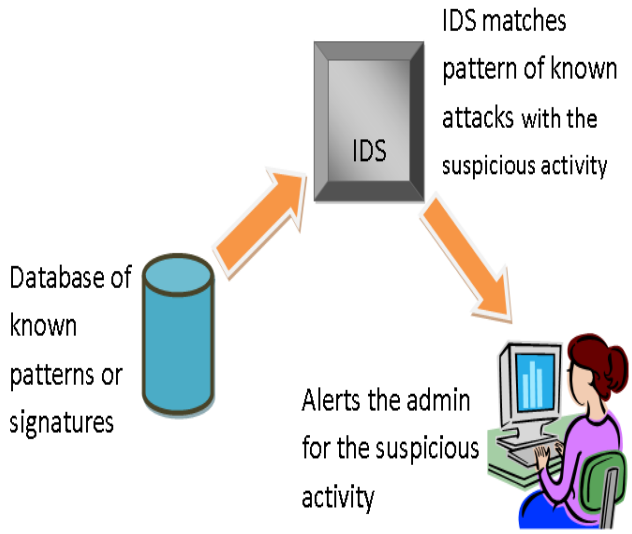

Figure 1: Signature based intrusion detection system

Signature based systems are not good when unknown attack is detected because our database won't be have the pattern for that. It works similar like an anti- virus where pattern for already known attacks are stored, it matches the malicious activity with the known pattern and if it matches it reports the administrator. If new pattern is received it is recorded, database is updated.

B. Anomaly Based Intrusion Detection System
This framework distinguishes the intrusion on the premise of deviation from the conduct [10]. An anomaly detection system first makes a pattern profile of the typical framework, system, or project movement. From that point, any movement that goes amiss from the pattern is dealt with as a conceivable intrusion [7]. In baseline model right qualities are encouraged into it, so that a typical action shouldn't get considered as intrusive movement. The real playing point of this IDS is it can distinguish obscure patterns which beforehand never known.

C. Artificial Neural Network based IDS
It utilizes ANN (artificial neural network) as a pattern recognition technique [8]. An ANN framework is propelled by the human sensory system. As human sensory system has neuron which takes information, creates some information and go to next layer, in the same way ANN based framework work. The fundamental unit in ANN based IDS is neuron. Every neuron is a neural system go about as an autonomous unit. The sorts of ANN utilized as a part of IDS are as per the following: Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptron (MLP) and Back Propagation (BP)[5].

D. Genetic Algorithm Based Intrusion Detection System
Genetic Algorithm takes a shot at rule of characteristic choice. First and foremost the chromosome like information structure develops to make population. An assessment function is utilized to compute the "integrity" of every chromosome. Amid assessment, two fundamental operators, crossover and mutation, are utilized to reenact the regular proliferation and transformation of species. The selection of chromosomes for survival and mix is one-sided towards the fittest chromosomes [9]. Genetic Algorithm is utilized to produce rules for IDS. These guidelines are then used to separate between typical action and an intrusion. The rules are put away in the following structure [20]
If { condition } then {act}
In above rule, condition comprises of numerous features like Source_Port, Destinatio_Port, Source_IP, Destination-IP, Duration, Protocol utilized. The above rules are matched with the defined standards. In the event that they don't match a ready report is sent to the administrator. GA based methodology is utilized to distinguish anomalous conduct. It distinguishes little number of network features nearly with network attacks taking into account common data between network features and kind of intrusion [5]

E. Fuzzy logic Based Intrusion Detection System
Author in [14] proposed a framework which utilizes fuzzy based system to identify and suspect DoS attacks known as Fuzzy Intrusion Detection System (FIDS). It includes three fundamental parts. The main segment is Filter and Parser Module (FPM). The second part is Fuzzy Rule-Based Detectors (FDs) and the last one is Warning System (WS). First and foremost part catches packets which are filtered and gathered by predefined attack signature. The second segment, FD examines the seriousness of the attacks of the filtered traffic. The last segment makes attack report for the overseer if the attack is identified.

F. Association Rule based IDS

Data mining technology can be utilized to produce new signatures for obscure attacks which can decrease false alarm rate and redundancy rate[16]. Association rule of data mining are utilized to concentrate the relationship features between the things which obliges two variables support and confidence and produces short patterns. Authors of [16] proposed the thought of length-diminishing support constraint that serves to discover long patterns with low support and also short patterns with high support.

IV. TYPES OF IDS USED IN CLOUD

Depending on their source of input data, IDSs can be classier as either network-based IDS (NIDS) or host-based IDS (HIDS) or distributed intrusion detection system (DIDS) [1]. Network-based systems collect data from network traffic (e.g., packets from network interfaces in promiscuous mode) while host-based systems collect events at the operating system level, such as system calls, or at the application level [6]

A. Host Based Intrusion Detection System

Host based intrusion detection system is a framework which screens a specific machine. It gathers data from a particular machine and checks them for any noxious action. The HIDS programming is introduced at one host to screen the traffic.

HIDS are further divided into four types [11].
File system monitors
Log file analyzers
Connection analyzers
Kernel based IDSs
In order to optimize the security of a host four aspects are taken into consideration as follows:

- Features
- Ease in installation and maintainability
- Techniques for evading the IDS
- Ways to alter the implementations in order to mitigate the effects of evasion attempts [11]

FileSystem monitor checks all the attributes (features) of a file like authorization, Inode, proprietor of gathering, size, registry and so on. The configuration needs the documents which are to be checked; rules to be performed. At that point a database is made which is introduced which keeps an eye on the documents on regular basis. As the documents changes regularly so its viability is troublesome. Techniques for evading IDS imply that how the framework works against the attacks. They are great when the document changes seldom overall measure of false positives produced increments. Logfile analyzer frameworks investigate logfiles for patterns demonstrating suspicious movement. By dissecting logfiles one can get the opportunity to know who logged in and can caution the manager about the intrusion if any. The third sort of HIDS is Connection analyzers which examine all the connections made with the host to identify any intrusion endeavor. Author in [11] said cautious configuration is required on the grounds that it may happen that a client connects to the wrong port and framework identifies it as an intrusion. Kernel based IDS is the sort of IDS which recommends that the kernel itself ought to have an intrusion detection framework. They are exceptionally powerful at forestalling and distinguishing intrusions. They can be utilized successfully for protecting system binaries and configuration files. More propelled design is conceivable, yet not recommendable for large scale deployment [11].

B. Network Based Intrusion Detection System

Host based intrusion detection system was intended to screen one and only host, however now a day's a large portion of the intrusion detection system are intended to bolster number of host interconnected by a network. NIDS is a sort of intrusion detection system which works on a network and searches for exercises that is by all accounts suspicious or unapproved. It investigates the network activities for any malignant action.

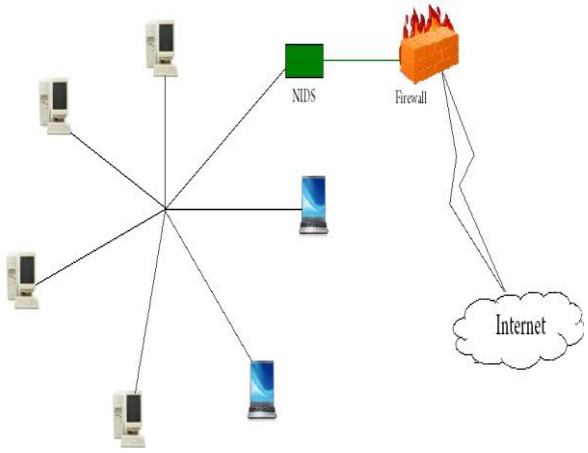

Figure 2: Network based Intrusion Detection System

C. Distributed Intrusion Detection system

A DIDS can be defined as:
"multiple Intrusion Detection Systems (IDS) spread over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data".[19]
DIDS architectural design incorporates DIDS director, single host monitor per host and single LAN monitor. All the data is gathered at every host is refined and transformed provincially and sent to the DIDS director for further activity. Host monitors are mainly in charge of gathering the data of particular host and send information to LAN monitor who further examines and investigate the information; any perceptible occasion taken into record is sent to DIDS director for further assessment and activity.

V. INTRUSION PREVENTION SYSTEM

Intrusion prevention system is a framework or system which monitors the framework for suspicious or noxious movement. It permits all the system movement to go through it aside from the particular case that is unequivocally not permitted. Not at all like Intrusion Detection System (IDS), IPS is not passive; it sits inline on the network and serves to anticipate intrusions [18]. The primary idea of intrusion

prevention system is to stop intrusion before they really happen.

Sorts of IPS

IPS basically comes in two flavors: Network based IPS (NIPS) and Host based IPS (HIPS). [12]

A. Network Based IPS

As the name proposes Network based IPS are responsible for the entire network, it assesses the traffic packet top to bottom, endeavors to notice the known vulnerabilities. They utilize both attack signatures and examination of network and application protocols in contrasting system action of every now and again attacked applications against anticipated that conduct would recognize suspicious movement. The fundamental capacity of NIPS is to shield the system from DDos attack. The majority of the NIPS utilize three techniques as takes after:

•Signature based detection: This technique is valuable when pattern of attacks are now known. At the point when any pernicious action is perceived it is contrasted with known patterns and proper move is made.

•Anomaly based recognition: This system is utilized for obscure attacks; the system first makes a baseline for the ordinary exercises, in the wake of making the gauge if any action discovered to be digressing from the standard is considered as suspicious movement.

•Protocol state analysis detection: this technique experiences the deviation of protocol states from the predefined rules

B. Host Based IPS

HIPS deal with stand out host on which they are installed. It represents the assessment of procedures which attempt to damage the host. Host Intrusion prevention system gives the capacity to the HIDS operators to piece or reject particular applications, practices, and changes to the local system configuration.[12]

VI. INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Alone Intrusion detection system and intrusion prevention system can't handle the cutting edge world intrusions; there is a requirement for the framework which can do the work of both IDS and IPS. So here is the framework which can do the work of both, known as Intrusion Detection and Prevention System (IDPS). It is the mix of IDS and IPS, IDS screens the movement for the malignant action yet can't stop activity though IPS can screen and stop the interruption before it really happens. IDPS is ordered into three general classes: Signature-based, anomaly based and stateful protocol analysis. There are numerous sorts of IDPS advances. IDPS are separated into four groups based on the kind of events that they screen and the ways in which they are deployed [15]: (a) Network-Based (b) Wireless(c) Network Behavior Analysis (NBA) (d) Host-Based [5]. IDPSs are essentially centered around distinguishing conceivable episodes. For instance, an IDPS could identify when an attacker has effectively bargained a system by misusing vulnerabilites in the system. The IDPS could then report the occurrence to security administrator, who could rapidly launch episode reaction activities to minimize the harm brought about by the episode. The IDPS could likewise log data that could be utilized by the handlers. Numerous IDPSs can likewise be configured to perceive infringement of security policies. For instance, some IDPSs can be designed with firewall ruleset-like settings, permitting them to distinguish system movement that abuses the organization's security or acceptable use policies. Likewise, some IDPSs can monitor file transfers and recognize ones that may be suspicious, for example, replicating a vast database onto a client's laptop.[13]

VII. CONCLUSION

Cloud computing is another idea in the business sector; it gives moderately shoddy assets and high adaptability. Cloud computing is thriving with an enormous rate, so its security and protection issues. Somewhere clients are as yet wavering moving towards the cloud due to the security reasons. With help of the above security measure we can control the intrusion and pernicious exercises.

REFERENCES

[1] Sebastian Roschke, Feng Cheng and Christoph Meinel, "Intrusion Detection in the Cloud," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009

[2] Insider attack, "http://www.techopedia.com/definition/26217/insider-attack"

[3] Naresh Kumar and Shalini Sharma, "Study of Intrusion Detection System for DDoS Attacks in Cloud Computing," IEEE, 2013.

[4] Ms. Parag K. Shelke, Ms. SnehaSontakke and Dr. A. D. Gawande, "Intrusion Detection System for Cloud Computing," International Journal of Scientific & Technology Research vol. 1, Issue 4, 2012.

[5] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. &Rajarajan, M, "A survey of intrusion detection techniques in Cloud," Journal of Network and Computer Applications, pp. 42-57,2013.

[6] Giovanni Vigna, Erland Jonsson and Christopher Kruegel, "Recent Advances in Intrusion Detection", 6th International Symposium RAID, Pittsburg, USA September 8-10, 2003

[7] Animesh Patcha, Jung-Min Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Elsevier, Science Direct,Computer Networks, pp. 3448–3470,2007

[8] Devi krishna K S, Ramakrishna B B, "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks," International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, pp. 1959-1964,2013.

[9] Wei Li,"Using Genetic Algorithm for Network Intrusion Detection," 2004.

[10] Herve´ Debar, Marc Dacier and Andreas Wespi,

"Towards a taxonomy of intrusion-detection systems," Elsevier, Science Direct,Computer Networks, pp. 805-822, 1999.

[11] Pieter de Boer and Martin Pels, "Host-based Intrusion Detection Systems," Feb 2005

[12] Steve Piper, CISSP and SFCP, "Intrusion Prevention System for Dummies," Wiley Publishing Inc, 2011

[13] G Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standard and Technology,Special Publication, 2007

[14] P. Tillapart, T. Thumthawatworn, and P. Santiprabhob, "Fuzzy intrusion detection system," Assump University J Technology (A.U. J.T.), vol. 6, no. 2, pp.109–114, 2002.

[15] J Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," 2007

[16] L. Lei, D-Z Yang, and F-C Shen, "A Novel rule based Intrusion Detection system using Data Ming," 3rd IEEE International Conference on Computer Science and Information Technology, vol. 6,pp. 169-172, 2010.

[17] U. Oktay and O.K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing," 6th International Information Security & Cryptology Conference, pp 71-76, 2013

[18] Aye Aye Thu, " Integrated Intrusion Detection and Prevention System with Honeypot on Cloud Computing Environment," Volume 67– No.4, April 2013, International Journal of Computer Applications

[19] Royce Robbins, "Distributed Intrusion Detection Systems: An Introduction and Review," SANS Institute InfoSec Reading Room, GSEC Practical Assignment, version 1.4b, Option 1,January, 2002

[20] Chris Sinclair, Lyn Pierce and Sara Matzner, "An Application of Machine Learning to Network Intrusion Detection,",1999

