iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Intrusion Detection System in Cloud: A Survey

Neenu Daniel[1]
Department of computer science, MG University

Abstract*—Cloud Computing is becoming popular day by day as many enterprise applications and data are moving into cloud based platforms .With the increasing use and demand of Cloud computing, security has become the major concern. Attack prevention measures such as authentication, encryption alone are not the solution for this; hence Intrusion Detection Systems have come into focus. we need a second wall of defense known as Intrusion Detection Systems (IDSs), to detect and produce responses if necessary. Since cloud computing is distributed in nature, supports multi-user and multi-domain platform, it is more prone to security threats. In this paper an attempt has been made to identify recent approaches used for intrusion detection in cloud. Moreover, the security threats and background of intrusion detection techniques in cloud are discussed.

***Keywords*— Cloud Computing, IDS, HIDS, NIDS**

I. INTRODUCTION

The term Cloud computing is being discussed about a lot these days, mainly in the context of the next generation web. Cloud computing offers some advantages by allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and operating systems), and software (e.g., application programs) provided by cloud providers (e.g., Google, Amazon, and Sales force) at low cost [1]. The current clouds are deployed in one of four deployment models: (a) public clouds in which the physical infrastructure is owned and managed by the service provider; (b) community clouds in which the physical infrastructure is owned and managed by a consortium of organizations; (c) private clouds in which the infrastructure is owned and managed by a specific organization and (d) hybrid clouds which include combinations of the previous three models. Many researchers and practitioners work on identifying cloud threats, vulnerabilities, attacks, and other security and privacy issues, in addition to providing countermeasures in the form of frameworks, strategies, recommendations, and service oriented architectures .Securing data is more critical in the Cloud Environment. Cloud is inherently vulnerable to many attacks including routing attacks, DOS attacks, flooding attacks etc.. For such type of attacks Intrusion Detection System (IDS) can be emplaced as a strong defensive mechanism.

The major contribution of this paper includes various security threats, intrusion detection approaches and techniques in Cloud Computing environment. Section 2 gives the detailed information about the security in Cloud Computing. Intrusion detection basics are discussed in section 3. Section 4 discusses about the various intrusion detection Approaches. Recent Intrusion Detection techniques in cloud are given in Section 5 followed by the conclusion section.

II. SECURITY IN CLOUD COMPUTING

A. Cloud Computing

Cloud computing is new and unique form of accessing data (e.g. Applications, documents, Music files, Video files, User files and much more) from any place across the globe without carrying any data storage devices like Hard drives, Memory cards or flash cards. Primary benefit of the technology is, it sets user free to move from his installed Desktop location to any other place and still can have access to their data anytime from anywhere. Cloud computing is web based processing, whereby shared resources, software, and information are provided to the users on demand over the internet. Cloud computing customers do not own the physical infrastructure. These users avoid capital expenditure on hardware and software. Instead they pay as per their usage. Cloud computing has become a major attraction for Small and medium enterprises (SME) as they get access to the IT services without spending money on procurement of servers and other facilities.

B. Threats in Cloud Computing

Companies can greatly reduce IT costs by offloading data and computation to cloud computing services. Still, many companies are reluctant to do so, mostly due to outstanding security concerns. Cloud Computing give end-users great benefits in terms of mobility, flexibility and productivity, but they also give malicious third parties new routes to breaching security and increase risks. A cloud is subject to several accidental and intentional security threats, including threats to the integrity, confidentiality and availability of its resources, data. Some common security threats [8] are

1) Data loss or leakage: This means a loss of data that occur on any device that stores data. It is a problem for anyone that uses a computer. Data loss happens when data may be physically or logically removed from the organization either intentionally or unintentionally. Compromised data may include: deleted or altered data without first making a backup; unlinking a record from a larger context; loss of an encoding key; and unauthorized access of sensitive data. The possibility of data compromise significantly increases in cloud computing, due to the architecture and operations. Examples of data loss/leakage issues include: insufficient authentication, authorization and audit (AAA) controls; inconsistent encryption; inconsistent software keys.

2) Account or Service Hijacking: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Using stolen credentials, attackers can access critical areas of cloud computing services and compromise the confidentiality, integrity and availability of such services. Examples of such attack s include: eavesdropping on transactions/sensitive activities; manipulation of data; returning falsified information; redirection to illegitimate sites.

3)DDOS Attacks: Spammers, hackers and other criminals take advantage of the convenient registration, simple procedures and relatively anonymous access to cloud services to launch various attacks. Examples of such attacks include: password and key cracking, DDOS .These attacks prevent users of a cloud service from accessing their data or their own applications. These attacks force the cloud service to utilize so much of the system's recourses that it becomes slow, bogged down, and inoperable. This can cause decreased productivity, frustration, and increased costs.

4) Insecure Interfaces and APIs: Cloud computing providers expose a set of software interfaces or APIs that customers then use to manage and interact with their cloud services. Therefore, the security of the system's APIs and its add-ons determines the security and availability of the cloud services. Weak interfaces and APIs expose organizations to a variety of cloud computing security breaches that can compromise confidentiality, integrity, availability and accountability.

5)*Data Breaches:* A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches include malicious insiders, cyber theft etc. A malicious insider might be a current or former employee, or a business partner who gains access to an network, system or data for malicious purposes. The online cyber thieves could use stolen passwords to access users' accounts as well as to launch malicious attacks to users

III. INTRUSION DETECTION SYSTEM IN CLOUD

In a network or a system any kind of unauthorized activities called intrusions. An intrusion detection system is a collection of tools, methods, and resources to help identify access and report intrusions. IDSs produce alerts for the administrators which are based on true positives or true alarms when actually intrusion takes place and false positive or false alarms in case of a wrong detection by the system. Mainly there are three types of IDS in cloud computing systems: Host based IDS, Network based IDS, and Distributed IDS. Host based IDS(HIDS) monitors specific host machines, network-based IDS (NIDS) identifies intrusions on key network points and distributed IDS (DIDS) operates both on host as well as network.

A. Host-based Intrusion Detection Systems

HIDS analyses the traffic to and from the specific computer on which the intrusion detection software is installed. A host-based system also has the ability to monitor key system files and any attempt to overwrite these files.

B. Network -based Intrusion Detection Systems

A NIDS is often a standalone hardware appliance that includes network detection capabilities. It will usually consist of hardware sensors located at various points along the network. It may also consist of software that is installed on various computers connected along the network. The NIDS analyses data packets both inbound and outbound and offer real-time detection.

C. Distributed IDS

Distributed Cloud IDS is a multi-threading technique to improve IDS performance over the Cloud infrastructure. The system then sends intrusion alarms to a third party monitoring service, which can provide instant reporting to cloud user organization management system with an advisory report for cloud service provider.

IV. INTRUSION DETECTION APPROACHES

IDS can be classified into two detection approaches: misuse detection and anomaly detection. Misuse detection approach monitors network traffic or system activities for known misuse, most of the case using table of pattern called signatures. IDS will match the event with the signature to detect the event as misuse or not. Anomaly detection approach on the other hand, detects any intrusion based on its decision using some techniques including statistical and machine learning. The IDS will first learn about the normal behavior of the network or system and create a profile of it. If the is any event that did not match the profile is considered anomalous.

V. INTRUSION DETECTION TECHNIQUES

Many researchers have suggested several IDS especially for the cloud, some of them will be reviewed in the following paragraph.

A. Profile based Intrusion Detection

In this work [9] a nonconventional technique is used for securing cloud network from malicious insiders and outsiders with the use of network profiling. With network profiling, a profile is created for each virtual machine (VM) in cloud that describes network behaviour of each cloud user (an assigned VM). The behaviour gathered is then used for determination (detection) of network attacks on cloud. The novelty of the approach lies in the early detection of network attacks with robustness and minimum complexity. The proposed technique can be deployed with minimal changes to existing cloud environment. The advantage is that it can detect all known attacks but unable to discover new attacks.

B. Multilevel IDS

In this work [2] IDS is applied for each virtual machine increases the effectiveness of IDS by assigning a multi-level intrusion detection system and the log management analysis in cloud computing. In this sense the users will receive appropriate level of security, which will be emphasized on the degree of the IDS applied to the virtual machine, and as well on the prioritization stage of the log analysis documents. This multi-level security model solves the issue of using effective resources and it supports classifying the logs by anomaly level makes the system administrator to analyse logs of the most suspected users first. Therefore this method provides high speed of detecting attacks and effective utilization of resources in cloud computing environment.

C Agent Based Intrusion Detection System.

In this work[10] an Intrusion Detection System (IDS) is proposed based on the features of the mobile agent. The mobile agents are used to collect and analyze the data collected from cloud environment to identify attacks exploited by the intruders. The main objective of the proposed system is to detect the known and unknown attacks exploited by the intruders in the cloud environment. The mobile agent is an agent having the capability of moving from one host to another. It interacts with the other nodes to collect the data. The advantage of mobile agent technology are reduces the network overload, overcoming network latency, robust and fault tolerant and it works in heterogeneous environment. All the mobile agents are configured in order to perform the operations like collecting the data from cloud environment, and these data are analyzed by the misuse detection agent. This agent checks whether the data collected are matching with the attack dataset available in the database. If any collected data is matched then the misuse detection agent informs the alert agent to alert the system about the intrusion. On the other hand, if the collected data is not matched with the dataset then the collected data are analyzed by anomaly detection agent, which uses naïve bayes classifier to detect the unknown or new attacks.

D. Software as a Service IDS

In this work [4]Software As A Service IDS (SaaSIDS) is proposed where traffic at different points of the network is sniffed and the interested packets would be transferred to the SaaSIDS for further inspection. The main engine of SaaSIDS is the hybrid analysis engine where the signature based engine and anomaly based engine which using Artificial Immune System (AIS) will work in parallel. Rule Based Engine will analyze the information received for intrusion detection based on the signature and if the information is not detected, Artificial Immune System Engine will analyze the packet by using anomaly based detection. The SaaSIDS is able to identify malicious activity and would generate appropriate alerts and notification accordingly. The SaaSIDS is able to identify malicious activity and would generate appropriate alerts and notification accordingly. The advantage

of this approach is reduced complexity with strong defensive mechanism .

E. Improved Hybrid IDS for Cloud

This work [3] combines positive features of two different detection methodologies - Honey pot methodology and anomaly based intrusion detection methodology. The Improved hybrid IDS is combination of anomaly based detection and honey pot technology with KF Sensor and Flow matrix. Honey pot attracts more and more attackers, the detection obtained can be used to create new signatures and update the database. Finally anomaly can be used to detect unknown attack in the whole network. KF Sensor is a host based IDS which works on the honey pot based technology, it adds the definitions of that attacker to the database for the next time and restrict the entry of that attacker or intruder to the main network of the organization. Flow Matrix is based on Anomaly based detection methodology. It compares the samples from the normal traffic with the regular samples obtained from the network and the moment it finds the difference between the normal and the regular sample it gives an alert. The advantage is able to detect abnormality with high accuracy.

F. Snort and Decision Tree Classifier based IDS

In this work [5] combined technique of signature based detection and also decision tree is used to address Dos attack. Signature based technique is used to detect known attacks whereas decision tree is used as anomaly detection technique to find unknown attacks. The authors integrate NIDS module in the Cloud offering infrastructure as a Service(IaaS) to detect network attacks. A serial combination of snort and Decision Tree (DT) classifier techniques are used. Snort is used to detect known attacks, whereas Decision Tree will report that the given event is malicious or not by observing previously stored network events. In this way NIDS module ensures low false positives and high detection accuracy with affordable computational cost in Cloud

G. Hidden Markov model based IDS

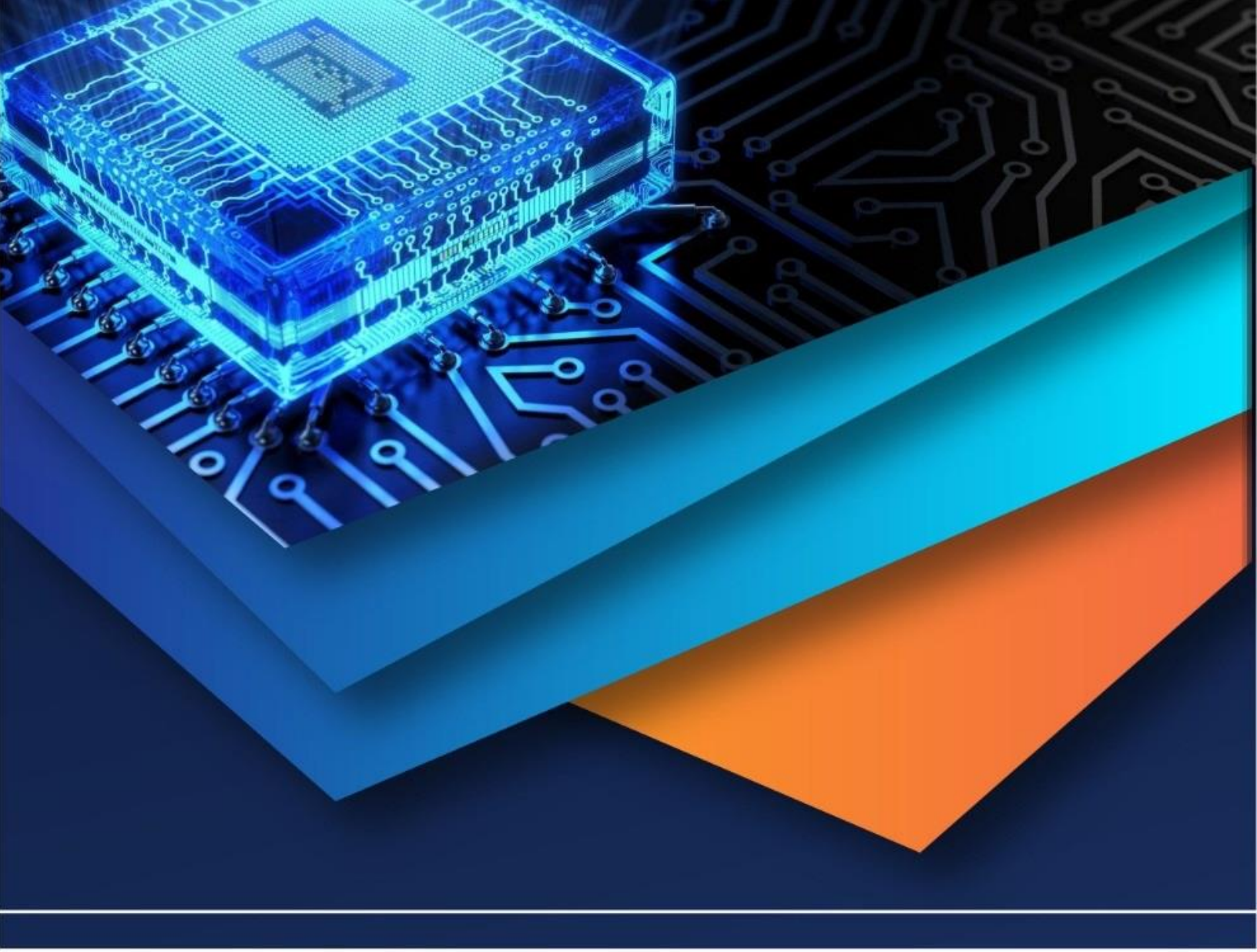
In this work [11] intrusion detection system which analyzes the logs in the cloud to determine the intensions behind the attacks. Sometimes the administrator neglects some stealthy reconnaissance actions for the insignificant number of violations. Hidden Markov model is adopted to model the sequence of attack performed by hacker and such stealthy events in a long time frame will become significant in the state-aware model. This approach analyzes the multiple logs if a machine under attack the proposed approach extracts and analyzes the logs related to observing machine to identify whether attack sequence exists.

VI. CONCLUSION

As the use of cloud has increased, the security in cloud has also become more important therefore, the intrusion detection systems are brought into consideration. Security is an important feature for the deployment of cloud computing environment. This paper summarizes security threat, intrusion detection techniques in cloud and also an attempt has been made to explore the security mechanism widely used to handle those attacks. Recent research findings uniting IDS specifically in Cloud have been discussed. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES

[1].M. Armbrust et al., "A view of cloud computing," CommunicationsACM, vol. 53, no.4, pp. 50-58, Apr. 2010.
[2].M. Kuzhalisai and G. Gayathri, "Enhanced Security in Cloud with Multi-Level Intrusion Detection System", IJCCT, Vol. 3, Issue 3, 2012.
[3].Ajeet Kumar Gautam, Dr. Vidushi Sharma, Shiv Prakash and Manak Gupta, "Improved Hybrid Intrusion Detection System (HIDS): Mitigating False Alarm in Cloud Computing", JCT, 2012.
[4].Azuan Ahmad et.al," Danger Theory Based Hybrid Intrusion Detection SystemsforCloudComputing",IJCCE,Vol.2,no.6,Nov.2013IJCCE,Vol.2,no.6,Nov.2013
[5]. A Novel Framework for Intrusion Detection in Cloud; Chirag Modi, Dhiren Patel, Bhavesh Borisanya, Avi Patel, Muttukrishnan Rajarajan; International Conference on Security of Information and Networks, 67-74, © 2012 ACM.
[6]. Internet Intrusion Detection System Service in a Cloud; Amirreza Zarrabi,International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, 1694-0814, © 2012 IJCSI.
[7] R. Bace and P. Mell, "NIST special publication on intrusion detection systems," DTIC, Document, 2001.
[8] Top threats to cloud computing," in Cloud Security Alliance, 2012
[9] Sanjika Gupta ,Padam kumar Ajith Abraham," A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment" ,IJDSN,,February 2013.
[10] Manikandaprabu.M.et al," intrusion detection system for cloud system using intelligent agents",IJECS,Vol 2,page 1868-1873,june 2013.
[11] Chia-Mei Chen; Guan, D. J.; Yu-Zhi Huang; Ya-Hui Ou, "Attack Sequence Detection in Cloud Using Hidden Markov Model," Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference on , vol., no., pp.100,103, 9-10 Aug. 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY