International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 6 (November-December, 2015), PP. 115-119

A REVIEW OF REVOLUTIONARY INTRUSION DETECTION SYSTEMS FOR DDOS ATTACKS ON CLOUD SYSTEMS

Umang Shah[1], Jinali Gandhi[2], Lakshmi Kurup[3]
Computer Engineering Department
[1,2,3]Dwarkadas J. Sanghvi College of Engineering
Mumbai, India
[1]umang.k.shah@gmail.com
[2]jinaligandhi794@gmail.com
[3]lakshmi.kurup@djsce.ac.in

Abstract— **Cloud computing is rising as a promising business concept and has undergone tremendous growth since the last few years in the IT segment of industries. With the increasing number of companies resorting to employ resources in the cloud, the protection of the users' data is a significant and prime issue of concern. Since a long time, Distributed Denial of Service (DDoS) attacks have been considered as one of the most hazardous attack on Cloud Networks and its security. Companies that are highly dependent on the internet for their business and transactions can face severe problems during the DDoS attacks. This is a critical matter which calls for an effectual method or system that can promisingly reduce the impact of the DDoS attacks. This paper focuses on the DDoS attacks on Cloud and studies the contemporary Intrusion Detection Systems existing to tackle them.**

Keywords- **Cloud Computing; Security and Protection; Denial of Service (DoS); Distributed Denial of Service (DDoS); Intrusion Detection System (IDS).**

I. INTRODUCTION

Cloud Computing can be defined as an Internet based computing where Virtual shared servers provide software, platform, Infrastructure, devices and other resources[2]. A Denial of Service attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing system [1]. In February 2000 major DDoS attacks were carried out against Yahoo.com, eBay, Amazon, ZDnet, Buy.com and FBI. Several other websites had also fallen victim to DDoS attacks, resulting in extensive damage and nuisance to users.[3]

This paper, surveys different threats affecting availability, confidentiality and integrity of Cloud resources and services. It explores the menace of DDoS attacks in particular and studies proposals incorporating Intrusion Detection Systems (IDS) against such attacks. Rest of the paper is organized as follows. Section 2 discusses Cloud Computing Systems and their salient features. Various threats to Cloud Security are discussed briefly in section 3. Section 4, explains the DDoS attack and section 5 presents the IDS technique against DDoS. Section 6 surveys newest proposals of IDS for DDoS attacks. Section 7 concludes with references at the end.

II. CLOUD COMPUTING AND ITS BENEFITS

A cloud computing system can be divided into three layers depending on category of resources provided by each layer.

The lowest layer provides necessary infrastructure components such as CPUs, memory, and storage, and is thus often called the Infrastructure as a Service (IaaS). IaaS provides the organizations with hardware resources that can be used for multiple tasks. The benefit is that instead of purchasing several servers, software, server racks, and having to pay for the datacenter space for them, the service provider rents those resources as per the need.

Above IaaS, more platform-oriented services allow the usage of server environments customized to specific needs, called Platform as a Service (PaaS). The services provided in PaaS model include application design, development, testing, deployment, hosting, team collaboration, web service integration, database integration, and versioning. [4]

The top-most layer contains ready to use applications also known as Software as a Service (SaaS). This can be provided to the user on-demand. As the software is hosted off-site, the customer doesn't have to maintain it or support it.

The advantages of Cloud Computing include:

- Services On-demand
- Pooling Resource
- Scalability and Elasticity

- Measured provision

III. Vulnerability of Cloud Computing Systems

Even as more and more cloud service providers (CSP) are emerging with robust security mechanics, there still seems to be a lack of security among cloud systems. This is mainly because of the following factors:

A. Remote Storage

The cloud is an off-site system to which users outsource their data needs to a third party provider. The provider does tasks like performing updates and maintenance and also manages the security. The issue here, however, is that users are trusting someone else to look after their data. [5]

B. Popularity

Everything stored on the internet is at a risk of cyber attacks and due to the sheer value of resources and data held in cloud servers, they get targeted very heavily by miscreants.

C. Internal Threats

As with any organization, CSPs too suffer from insider threats as company employees possess authorized access to cloud servers and may misuse the power. [5]

D. Lack of Standardization

Due to the lack of guidelines, different CSPs implement their own security measures; this leaves scope for many unwanted vulnerabilities and gaps.[5]

E. Distributed Nature

The distributed nature of cloud systems leaves them exposed many unchecked trap doors and loopholes, it also becomes difficult to maintain such large systems regularly increasing the chance of attackers taking advantage of such shortcomings.

IV. Threats to Security

Cloud security threats may be classified and categorized based on the characteristics and liability of each attack. Following is the categorization of different security threats in cloud environments [6]:

A. Basic Attacks

a) SQL Injection Attack

Using SQL Injection, an attacker tries to gain unauthorized access to a database or system by placing a malicious code in the standard SQL commands. It may be prevented by filtering user input and performing sanity checks on the code.

b) Cross Site Scripting Attack (XSS)

Attackers write malicious scripts and inject them into web content; as a result the website contents may change and may even be harmful for users. It is necessary to scan and fix vulnerabilities to avoid such attacks.

c) Man in the middle (MITM)

An intruder tries to collect details of interaction between two hosts by positioning itself in the network such that all traffic passes through it. Best way to tackle it is use of encryption so that packet data is rendered unreadable.

B. Network Layer Attacks

a) Prefix Hijacking

Here, a wrong announcement of an IP address related with a system is made. As a result, data leakage due to wrong routing information may occur.

b) Fragmentation Attack

Attack may be initiated by malicious insider or outsider. A different IP datagram is used to mask malicious TCP packets to bypass IP filtering mechanisms.

c) Deep Packet Inspection

Usually carried out by an insider, with this attack a malicious user may analyze the network and acquire crucial information to carry out more sophisticated attacks.

d) Port Scan

A port scan attack may reveal the active connections on each network port and thus revealing the complete activity status of the network.

These network layer attacks can be prevented with the use of an IDS and log management system.

C. Application Layer Attacks

a) Denial of Service

A redundant and continuous flow of packets may render the cloud network unusable. DOS attacks downgrade network services and increase the bandwidth usage, even resulting in server crash.

b) Cookie Poisoning

By changing or modifying contents of cookies, attackers can impersonate authorized users and get access to web pages and applications.

c) Captcha Breaking

A variant of DOS, attackers can break Captcha protection system inorder to spam or flood system and exhaust the network resources.

V. DDOS ATTACK

Distributed DoS attacks are one of the major kinds of attacks on Cloud Security and can bring about serious consequences. It is a synchronized attack on the different available services of any target system or network that is launched indirectly through a number of compromised computing systems. It thwarts the authentic user from accessing the required services. The DDoS attack is mainly based on three functional units:

(i) Master: Master is the one who launches attack.

(ii) Slave: Slave acts as a launch pad to the Master. Slave is actually a network.

(iii) Victim: The server which is on the agenda of the Master to be attacked is the Victim.

This attack takes place in two stages. First stage is Intrusion Phase. During which the Master tries to infiltrate an inferior machine to get a support to flood the significant machines with requests. The second stage is DDoS tool installation phase. During this phase DDoS tools are installed in order to attack the victim or main server [7].

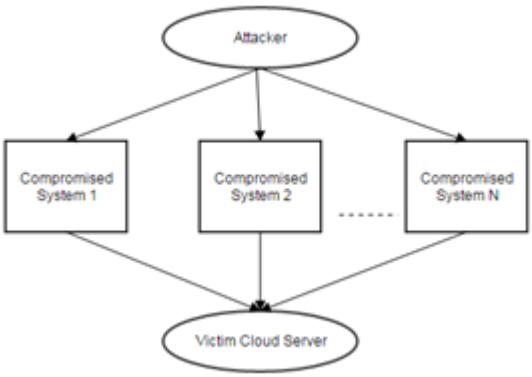

Fig 1. DDOS Attack

The DDoS attacks do not to modify data or get into an illegal access, but instead they aim to crash the servers and the whole networks, disrupting the access of legitimate users [3]. They have certain characteristics such as displaying different appearances in different scenarios which makes the attack very difficult to detect [8]. There are many proposed systems to foil these attacks, but none has been successful to completely overcome the attacks as yet.

VI. INTRUSION DETECTION SYSTEM FOR DDOS

The security aspect is very vital in the cloud scenario due to its distributive nature. Malicious actors are continually changing the game by switching tactics; seeking out new vulnerabilities and even bringing back old techniques that were considered outdated. Ample research is currently going on to guarantee security of the end user's data in the cloud.

The role of Intrusion Detection Systems (IDS) is to preserve Confidentiality, Integrity and Availability of services; they capture data, analyze it and report intrusion events based on behavior and characteristics.

Any IDS should carry out the following functions: [9]

- Monitor User and System activities and analyze them.
- Analyze system configuration and vulnerabilities.
- Assessing System and File Vulnerabilities.
- Recognize patterns typical of attacks.
- Analyze abnormal activity patterns.
- Track user policy violations.

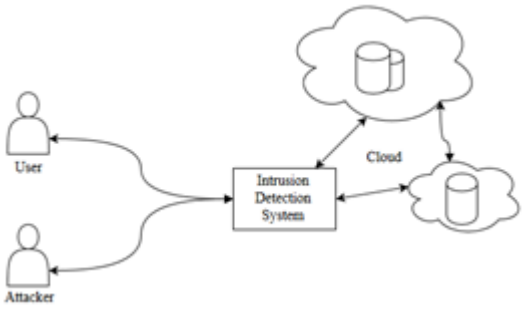

Fig 2. Role of IDS

While Monitoring DDoS attacks, an IDS should look out for attempts to launch flooding attacks, counter or block these flood attempts and ensure that the genuine user is not affected by it. The IDS may rely on Log Records, Packet Signatures, Headers or Statistics to formulate decisions. Detection is successful if the system resources and bandwidth remain, more or less free from damage.

VII. LITERATURE REVIEW

A. Transmission Control Protocol Mitigation Strategy (2014)

Proposed Solution: Aishwarya et.al and Dr. Maliga et.al [3] proposed a TCP Mitigation Strategy; they devise a two layer system. The first layer uses a set of rules for filtering packets based on hop count and then encodes the sequence numbers in the SYN packet that could only be decoded by legitimate clients. The server ignores the connection packets when it does not receive the Acknowledgement (ACK) with correct sequence number from the client which requested the connection. The Second layer uses the Message Authentication Code (MAC) to differentiate between genuine and spoofed IP addresses. In a three way TCP handshake, SYN packets come from the client to the server to begin the connection. The server, after receiving the SYN, sends the SYN-ACK. If it is a valid client, it acknowledges with the ACK to the server otherwise, server can detect the irregularity in the packet and drop any more packets

from the same source. The SYN backlog timer is used to reduce the SYN flooding attack.

Result: The result obtained shows that this Intrusion Detection method drops more number of data packets from reaching the server and hence providing more security. In the cases where, SYN flag is not set and IP is not in the table of server, the attack is more likely to happen and the server drops the packet. The work is tested in multiple scenarios and the results are obtained for it.

B. Intelligent Intrusion Detection System for Cloud Computing (2014)

Proposed Solution: The Intelligent Intrusion Detection System for Cloud Computing (SIDSSC) by Saeed et al Maqbool et al and Robert John [10] aimed to overcome shortcomings of other IDS. The model consists of an IDS Server and a Cloud Server, the IDS server has software like SNORT to analyze traffic. In case of attack like DDoS, the system notifies about an ICMP flood. The Cloud Server then requests the IDS server to detect the IP of the source of attack. During this process, the Cloud server goes into an alert mode to protect the system. Once IP addresses are detected, necessary steps can be taken to block any more packets. Cloud server can then function normally. The additional layer of IDS Server keeps on checking the incoming data for all types of attacks and aberrations.

Result: The proposal was tested on a model implemented using virtual machines. From the test results, they illustrated that IDS Server provides a crucial layer of security to the Cloud Server. It demonstrated ability to counter attacks up to 6000 packets per second. The IDS server always ran in parallel, thus allowing Cloud Server better functionality and security.

C. Finite State Hidden Markov Prediction Model (2014)

Proposed Solution: The Finite State Hidden Markov Prediction Model (FSHMPM) [11] is based on finite state HMMs. It represents a sequence of events that match an attack's signatures as a series of state transitions with a particular probability. The model uses Forward-Back Propagation (FBP), a training algorithm to infer the transition, output probabilities, and other parameters needed for prediction for the attacks of interest. Based on the received alerts, the prediction model predicts any possible multi-step attacks before they compromise the system. The algorithm starts by computing the alert risk and then mapping this risk to one of the 4 defined risk levels. An alert is fired if the final prediction probability is higher than a pre decided threshold. The model is also able to predict the non completed multistage attacks that repeat their attempts.

Result: It is used with the Autonomic Intrusion Detection Framework (ACIDF). A model is implemented which is successful in determining the occurrence of a DDoS attack on a cloud system; it was able to fire early alerts before an attempted DDoS like LLDDOS1.0.

D. Hybrid Statistical Model (2015)

Proposed Solution: The proposal [8] defines a hybrid model that combines two approaches namely covariance matrix and entropy. DDoS attacks are classified by measuring the heightened dependency in the data. The covariance matrix has a multivariate distribution of incoming data packets and uses multiple limit values for testing. By constructing a covariance feature space based on data packet values, a detection problem can be formulated. After that it determines the thresholds and forms a constrained boundary for the attack. Since the boundary is constrained, the covariance matrix approach can identify the unknown attacks. Due to the use of the covariance and entropy double checkpoints, it considers all features of the data statistics to get an accurate result.

Result: The method combines the accuracy of entropy and effectiveness of covariance matrices and aims to provide a reliable solution for detecting DDoS attacks. No experiments have been conducted to assess the practical feasibility.

VIII. COMPARISON OF METHODS

A comparative analysis with respect to the strategies used the architecture of the Models and the type of systems they fall into, of these four types of Intrusion Detection System is presented in Table 1

TABLE I. COMPARISON OF DIFFERENT INTRUSION DETECTION SYSTEM

Factors	A	B	C	D
Based on (Strategy used)	Packet filtering	SNORT for traffic analysis	Finite state HMMs and uses Forward Back Propagation Algorithm	Combines the approach of Covariance Matrix and Entropy.
Architecture (Model)	Two- layered architecture. 1st layer- filtering and encoding of packets. 2nd layer- uses MAC to differentiation between fake and genuine IPs.	Consists of IDS server and Cloud Server. IDS server runs SNORT to analyze traffic. Cloud server detects the source IP and protects the system.	Made of Finite state Hidden Markov Model. It is a prediction model that can predict no of multi-step attacks.	Hybrid architecture – combines two famous approaches to provide reliable detection of DDoS attacks.
IDS type	Network Based IDS	Server Based IDS	Host Based IDS	Network based + Host Based IDS.

IX. CONCLUSION

As the nature of attacks is ever changing our security and detection systems should also keep upgrading and changing. In the paper we have briefly discussed the issues of Security faced in a cloud environment and elaborated on the DDoS attacks. We analyzed the latest proposals for Intrusion Detection Systems for DDoS attacks and evaluated their efficiency as observed from their practical results.

REFERENCES

[1] Stephen M. Specht, Ruby B. Lee," Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". In Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems,2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.

[2] "Luit Infotech: What is Cloud Computing", Download, pp 1-3. http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf

[3] Aishwarya, R.; Malliga, S., "Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment," in *Recent Trends in Information Technology (ICRTIT), 2014 International Conference on* , vol., no., pp.1-6, 10-12 April 2014.

[4] 'Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds', *2010 Fifth International Conference on Internet and Web Applications and Services*, 2010.

[5] '8 Reasons to Fear Cloud Computing', *Business News Daily*, 2013. [Online]. Available: http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html. [Accessed: 05- Nov- 2015].

[6] Deshpande, P.; Sharma, S.C.; Kumar, P.S., "Security threats in cloud computing," in *Computing, Communication & Automation (ICCCA), 2015 International Conference on* , vol., no., pp.632-636, 15-16 May 2015.

[7] Kumar, N.; Sharma, S., "Study of intrusion detection system for DDoS attacks in cloud computing," in *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1-5, 26-28 July 2013

[8] Girma, A.; Garuba, M.; Jiang Li; Chunmei Liu, "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment," in *Information Technology - New Generations (ITNG), 2015 12th International Conference on* , vol., no., pp.212-217, 13-15 April 2015.

[9] M. Sharma, K. Jindal and B. Sharma, 'Analysis of IDS Tools & Techniques', in *International Conference on Advanced Developments in Engineering and Technology*, India, 2014, pp. 35-40.

[10] Alqahtani, S.M.; Al Balushi, M.; John, R., "An Intelligent Intrusion Detection System for Cloud Computing (SIDSCC)," in Computational Science and Computational Intelligence (CSCI), 2014 International Conference on , vol.2, no., pp.135-141, 10-13 March 2014

[11] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.