THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

A Study on Securing Cloud Environment from DDoS Attack to Preserve Data Availability

M. Durairaj
Assistant Professor, School of Computer Science,
Department of Engineering & Technology, Bharathidasan University, Trichy, India
A. Manimaran
Research Scholar, School of Computer Science,
Department of Engineering & Technology, Bharathidasan University, Trichy, India

Abstract:
Security plays a distinctive role in the digital computing. All the operations are automatic and servers maintain large volumes of data. This paper discusses different techniques and extends with the issues such as challenges, security attacks, DDoS attacks and intrusion detection methods. Cloud computing allows huge volume of storage on web which makes available the data and services in distributed environment. Intruders target the cloud based data due to its storage nature. The most famous attack of cloud computing is Distributed Denial of Service (DDoS) attack. The DDoS is the biggest threat in the areas of internet and internet of things (IOT). To prevent these kinds of attack, the intrusion detection system should have strong protective mechanism. This paper delivers an ample survey and comparative study on various cloud security attacks in browser, application, network and server level. The survey includes the DDoS attack types, vulnerabilities and intrusion detection techniques.

Keywords: *Cloud computing security attacks, DDoS attacks, Intrusion detection systems*

1. Introduction

Cloud computing has tremendous technological improvement in recent days scenario, which helps us to make the computer resources maximum utilized. Since, it needs precaution to avoid vulnerabilities using Intrusion detection systems. In the cloud environment Hypervisor and Virtual Machine are more significant for protecting valuable data from attackers [1]. DDoS can be explained as a plan attack for indispose usual service in the network. To maintain the availability of cloud resources, cloud vendor desires to take necessary action against Distributed Denial of service attack, because cloud resources are unavailable to the legitimate user, when large number of request receives server from attackers [2][3]. Sequence of DDoS attacks launched towards a number of companies which anti-spam services. Such attacks compose server unserviceable for a long time, so that strong defense mechanism against DDoS attack is very significant in the present days to reduce the loss in the distributed cloud environment.

To recognize and protest suspicious request, it is needed to install intrusion detection system (IDS) in the cloud servers. Numerous techniques and tools are exists and used to protect the attack on cloud. Secret of cloud computing is that it reveals only what kind of services are provided rather location and storage space. Amazon, Yahoo mail, eBay, and some other websites were became victims and DDoS attacks instantiated against these sites on 9th February, 2009 [3]. These kind of attacks induced companies to push down their services. Intrusion detection system (IDS) plays a crucial role in the cloud computing to defend computer systems and network towards harmful exploitation. This intrusion detection system identifies and responds to the intrusion from malicious host or network. The main classifications of IDSs are Host based and Network based methods, also it requires updating its database by investigating and gathering relevant information. Cloud Intrusion Detection System Service (CIDSS) architecture is built for secure cloud SaaS application data transaction [4]. In Figure 1, the effectiveness of the security mechanisms against the DDoS attacks is shown. Critical barriers which prevent DDoS attacks are shown in Figure 2.

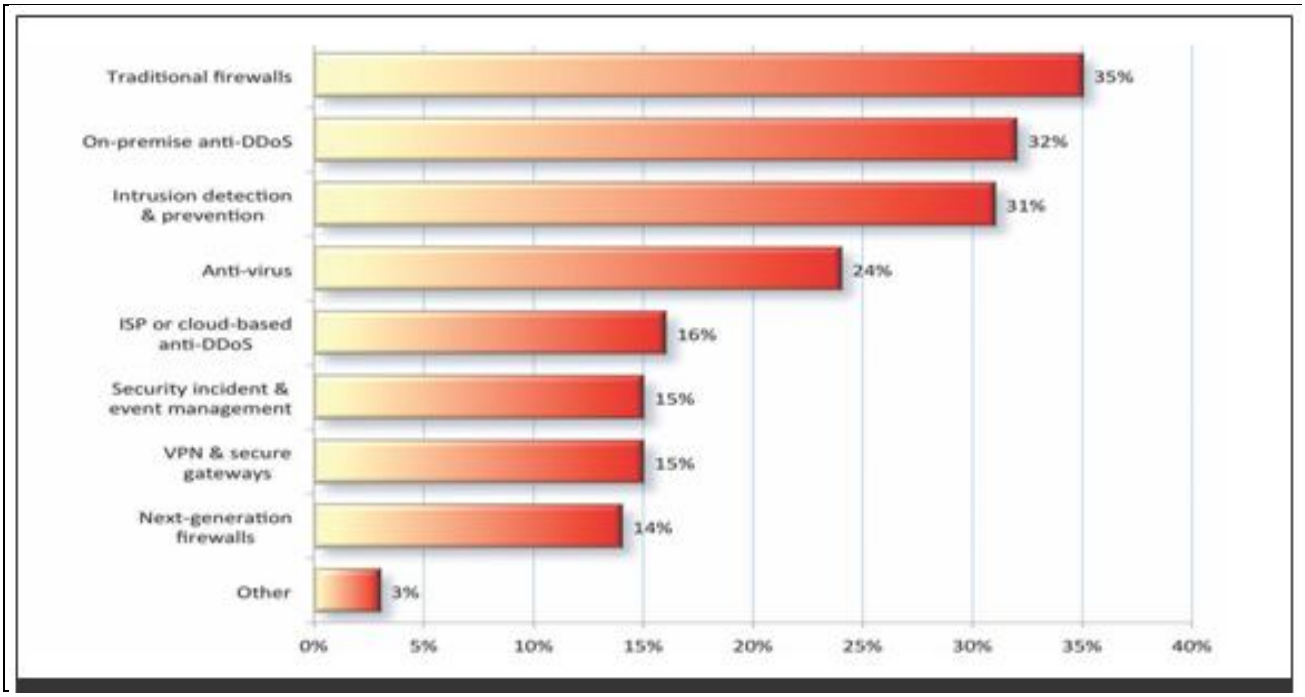

Figure 1: Security mechanisms used to prevent and detect DDoS attacks
Source: Ponemon Institute

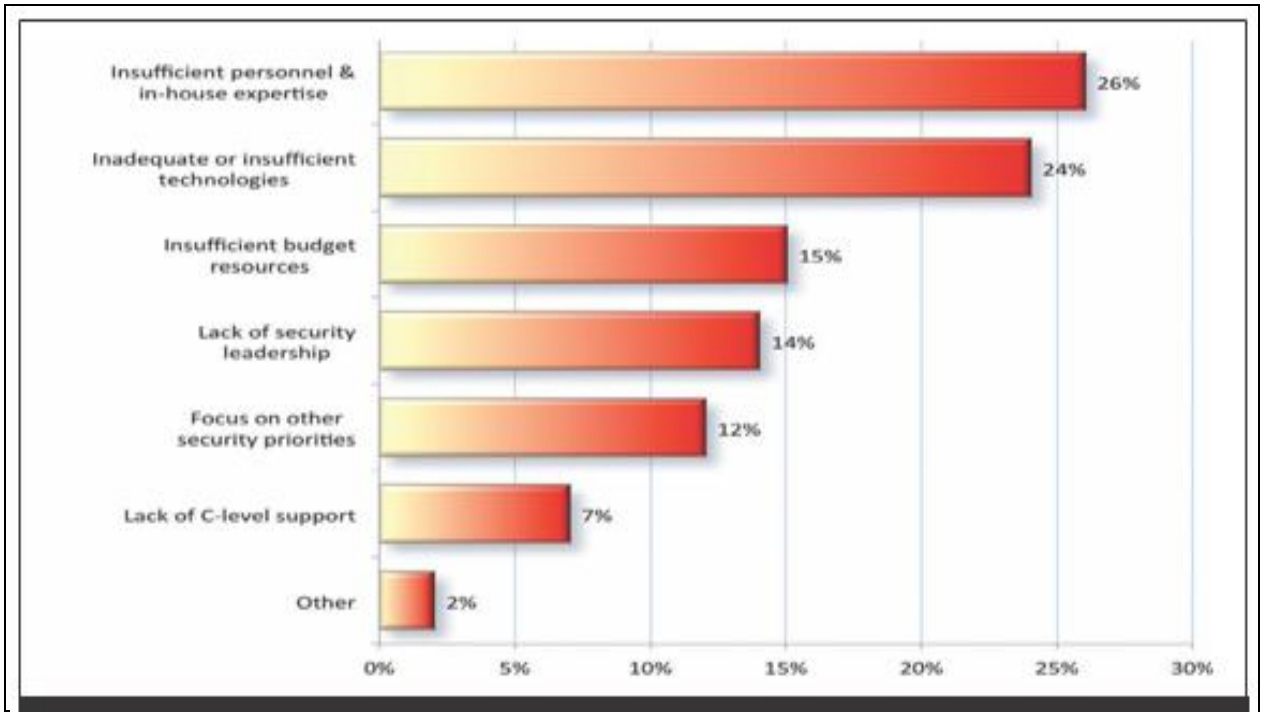

Figure 2: Critical barriers to preventing DDoS attacks
Source: Ponemon Institute

2. Existing Work

Cloud Computing security attacks are classified into four key levels, they are browser level, Application level, Network level, and Server level. Each key level delivers unique attacks, which are encountered in the distributed Cloud environment. The following diagram depicts the feature view of this representation.

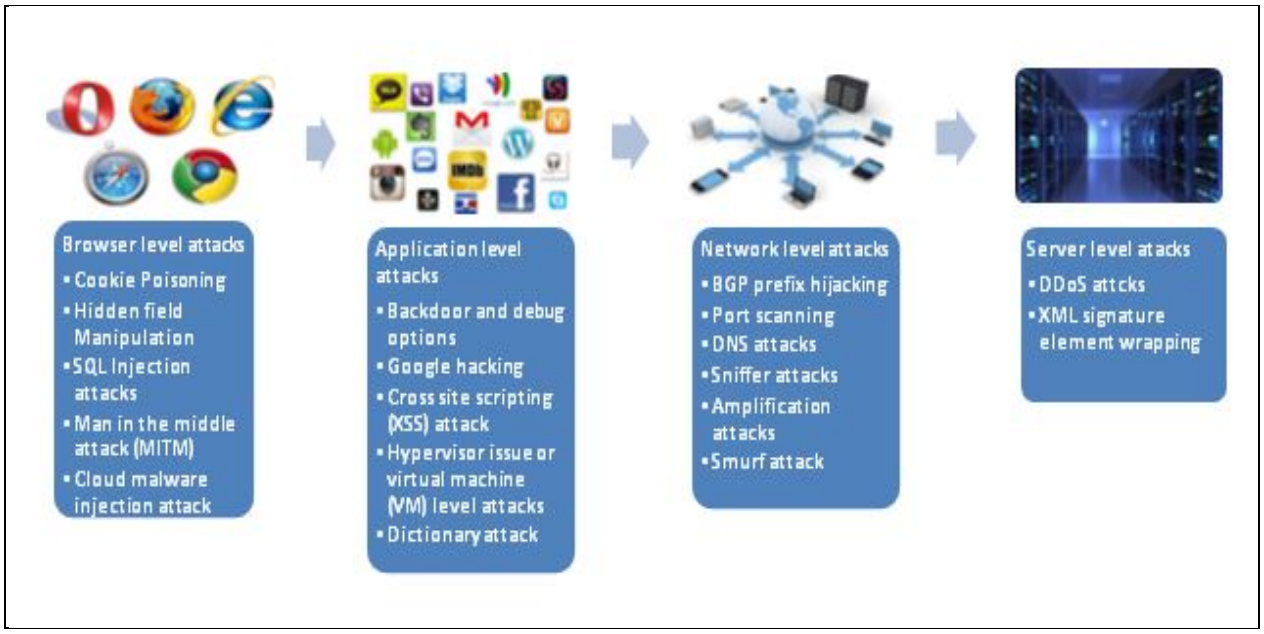

Figure 3

2.1. Cookie Poisoning

Cookie Poisoning attacks conception with the alteration of the data of a cookie with respect to avoid security mechanisms to gain access unauthorized information. Cookies saved on a cloud user's hard drive and parameter consists of user identity, preferences, examine behavior and more. The malicious intruder gets one of this parameter from cloud server and steals user's potential. It is the foundation for many numbers of attacks like cross site scripting, buffer overflow and SQL injection. So that strong encryption techniques are essential unless network firewalls, Intrusion detection and prevention systems are not effective for this attack to trace web application data. Imperva SecureSphere Web Application Firewall (WAF) is actively blocking Cookie poisoning attack [5].

2.2. Hidden Field Manipulation

Hidden field manipulation attack is hacking method to manipulate the hidden field data. Client sensitive information's are stored as hidden field, which comprises webpage related data, which is dealt by web developers. Though, these fields are highly vulnerable to attacks and attackers could manipulate the hidden field value that yields modified webpage information. By disclosing the confidential information, serious security issues exploited [5].

2.3. SQL Injection Attacks

SQL injection attack is web attack mechanisms to access the unauthorized data illicitly by the hackers. Web applications allow users to give input data and retrieve output through web browser. In this scenario SQL commands are backbone for this transaction; attackers inject malicious code and manipulate the standard SQL commands to gain access [5]. Solution for this attack is dynamically generated SQL code to prevent from SQL injection attack.

2.4. Man in the Middle Attack

Man in the middle (MITM) attack also called as Man in the browser attack (MITB) is one kind of cyber attack, where malicious intruder acts as a proxy in the communication session between two different parties. This attack allows malicious intruder to send or receive information across network communication channel [6]. Popular tools to safeguard this attack are Packet Creator, Ettercap, Dsniff and Cain e Abel.

2.5. Cloud Malware Injection Attack

Cloud computing reputation is based on its outstanding services, which compromises its strength because of malware injection attack. Attackers attempt to inject their own malicious service, application and virtual machine into the cloud system, thereafter services are specified as a valid instance with malicious software. All the authorized users receive malware services from the cloud environment, it might consist of Virus program, or Trojan package makes dangerous region in the distributed environment. System hardware and cloud instances are at high risk because of malware program, which leads to data unavailability across the cloud system [6]. There are two recommended steps to prevent cloud malware injection attack. First and foremost step is sending the incoming requests to service instance integrity check. Second step is to adopt the system for valid hash value for every user.

2.6. Backdoor and Debug Options

Hackers and malicious users attack easily through backdoors by exclusively allowing any particular traces in the system. In some cases, web developers permit debug options in the application to alter the source code on the websites [6]. These debug options are

also known as backdoors act which allow hackers to access perceptive information. This leads to influential effects to the cloud application. To avoid this attack, developer can hinder the debug option as a result the application effectiveness will be compromised.

2.7. Google Hacking

Google provides enormous benefits to the users to get everything from the internet. Hackers search information from Google to get secret information, and discover the vulnerability of the target system to gain access in an illegal way. Report says several Gmail account login details were stolen by hackers [7]. In a distributed cloud environment, security loopholes are more in application level (SaaS, PaaS, and IaaS).This is great challenge to the cloud providers to protect user's sensitive information from malicious hackers. There are few points to be implemented while designing application level security to avoid attacks; they are,

- Installing standard security procedures to avoid system vulnerability.
- Not allowing customized login permissions until they are tested accurately.
- Ensuring Continuous Data Protection (CDP) which is essential for data recovery.

2.8. Cross Site Scripting (xss)

Cross site scripting is an application layer hacking techniques, and it injects malicious script on trusted website. Cross site scripting attacks are classified into three types; they are persistent also called as static, non-persistent also called as dynamic, and DOM-based. An injected script is stored forever in the persistent type attack; injected script is reflected away the web server in the non-persistent method, and DOM based attack is sub class derived from reflected XSS [7]. Dynamic websites are more vulnerable and get offended by XSS attacks than static websites because of its dynamism. Trusted users confidential information's are leaked unknowingly by clicking pop-up window on the screen. To prevent this attack some of the techniques are in effect, they are Active Content Filtering; Content based data leakage prevention technology and web application vulnerability detection technology [7].

2.9. Hypervisor or VM level issue

The concept of virtual machine (VM) is a backbone of cloud computing technology. In most of the cloud features accomplishes with the virtual machine concept. The virtual machine monitor or hypervisor in a virtualized environment runs multiple operating systems in a single hardware resource. In security aspect, maintaining system logs while running multiple operating systems is a difficult task. In a shared environment, there is always a risk factor when managing all the operating systems functionality as secured, since any one operating system image with malicious code makes all other operations systems vulnerable to attacks. Hypervisor plays significant role in securing cloud data as the hackers can attack hypervisor only after they could control all other guest operating systems [7]. The security attacks on VM such as VM backdoors, VM escape, and VM Root kits formulate the attacker to have control over cloud system. High protection systems are required to safeguard the cloud system.

2.10. Dictionary attack

Authentication and authorization through strong passwords are more appropriate techniques for securing cloud data. Information security in a distributed infrastructure can be compromised by carrying out Dictionary attack. Dictionary attack refers to possibility of all the word combination and which decrypts the account password unethically [7]. In this method, hackers need to attempt more number of times to get correct passwords for log in. There are two steps against dictionary attacks. One is to get delay response from the server which prevents hacker application to perform permutation in a short time span. Second, lock the account, if attempt exceeds the limit.

2.11. BGP Prefixes Hijacking

BGP prefix hijacking is a network related attacks on cloud infrastructure as it attacks malicious untraceable IP addresses. The IP addresses configured for autonomous systems which transmit data to all its neighbors using Border Gateway Protocol (BGP) [7]. When fault encountered in the autonomous system while transmitting through incorrect IP address, the network direct through transmission other than deliberate IP address.

2.12. Port Scanning Attack

In a network, data packets are transmitted through port that has unique number for identification. Port numbers act as an entrance for transmission to perform entry and depart. Web servers habitually pay attention on TCP port 80 and for mail server port 25. Attackers can easily find the open ports in a system using port scanning application and analyze various running services, even firewalls fail to protect system from this attack [8]. There are numerous port scan detecting tools available, for example, Linux operating systems uses Port scan attack detector (PSAD) for security.

2.13. DNS Attack

DNS (Domain Name Service) is an internet service that translate domain name in to IP addresses. The DNS attack readdresses all arriving packets and redirect to their chosen server, and capture incoming e-mails [8]. There are three types of DNS attacks; first one is cache poisoning attack, which happens after successful insertion of malicious DNS information into legitimate DNS servers by the attackers. Second type of attack happens when attacker controls over one or more authoritative DNS servers. Third type of attack happens when registration of the domain name itself. Prevention methods for DNS attack is to building resolver as private and protected, and configuring DNS application codes to protect DNS server from cache poisoning attack.

2.14. Sniffer Attack

Sniffer software is used to capture the sensitive information at the Ethernet frame point by the attackers, which is also called as network protocol analyzers. Wireshark is one of the tools for sniffer attack, which confine and inspect data across the network. Unencrypted data in a network can be violated using sniffer attack to steal confidential data [9]. Other tools are Dsniff, Etherpeek, sniffit, etc.

2.15. Amplification attack

Packet sending can be amplified by the attacker to make the network traffic. When sending a large number of packets to broadcast IP address, it is hard to reply for all the packets and resulted in service deniable [10]. This leads to leakage of broadcast address information through network devices like routers. The following attacks are impact of amplification attack.

- Smurf attack
- Fraggle attack
- Resource depletion attack
  - Protocol exploit attack
  - Malformed packet attacks

2.16. Smurf attack

Smurf attack creates denial of service (DoS) in a network using IP address and makes the network untreatable. To address the network vulnerabilities, one need to know the basic characteristics of Internet Protocol and Internet control message protocol. Network nodes can control ICMP (Internet Control Message Protocol) and based on the state of the network, ICMP information can be changed by administrators. ICMP used to check the status of others nodes, if they are in operation then it returns ping message [10]. There are two mechanisms work together to prevent this attack. First method is to configure router in IaaS layer to avoid ping command through IP address. Second method is to stop sending ICMP packets to the IP broadcast addresses by configuring operating system in PaaS layer.

2.17. DDoS attack

Malicious attackers use DDoS attacks to make the cloud resources unavailable to the legitimate users. Attackers generate large number of request to the server and cloud system which compromises the data availability. Generally three functional units are used in DDoS attack, A Master, A Slave, and A Victim and this is called coordinated attack. DDoS attacks affect all the layers of the cloud system (IaaS, PaaS, and SaaS) and can occur internally or externally. The target of external cloud-based DDoS attack is Cloud-based Services and this attack takes place outside the cloud environment. This type of attack affects the availability of services. SaaS and PaaS layers are the most affected layers in the cloud system by external DDoS attacks. An internal cloud-based DDoS attack occurs in PaaS and IaaS layers within the cloud system.

2.17.1. IP Spoofing Attack

Internet Protocol (IP) spoofing is one of the very prominent Denial of service attack and the aim of this attack is to flood the victim with irresistible amounts of traffic. In this, Packet transmissions between the end user and the cloud server can be intercepted and their headers modified such that the IP source field in the IP packet is copied by either a legitimate IP address, or by an unreachable IP address. Finally the server will react to the legitimate user machine with defects, which means server is incapable to complete the transaction with unreachable IP address. This makes the server resources underutilized. It is very difficult to trace this kind of attack due to the fake IP address of the IP source field in the IP packet. To find the IP spoofing attack, security methods can be applied in the PaaS layer or in the IaaS layer. A new technique called hop-count filtering (HCF) [11] can be used to differentiate legitimate IPs from spoofed IPs in the PaaS layer because of difficulty in modifying and enriching various types of network resources in the cloud system. The HCF counts the number of hops depending on the value of the Time to Live (TTL) field in the IP header. IP-to-hop-count (IP2HC) mapping is constructed to discover the spoofed packet. Through investigation using network measurement data, the HCF method detected 90% of spoofed addresses [11].A trust-based approach can be used to discover spoofed IP addresses in the access routers on the IaaS layer and also it confronts problem for detecting in distributed routers.

2.17.2. SYN Message Flooding Attack Vector

A SYN message flooding attack is a class of denial of service attacks, in that an attacker sends sequence of SYN requests to a target's system to consume maximum server resources. So that server unable to provide service to the legitimate users. PaaS and IaaS layers are affected by SYN flooding attack [12]. Three-way handshake method is used to get connection from legitimate user to server by sending SYN message in Transmission Control Protocol (TCP). Then, the server acknowledges the SYN message by sending back (SYN-ACK) a request to the legitimate user. To establish the connection, finally the legitimate user sends an ACK request to the server. If server gets huge number of packets from the attackers, then evidently SYN flooding takes place, but three-way handshake method does not complete. This makes the server to wait for completion of all those packets, which affects the resource performance of the cloud system. In the PaaS layer, two mechanisms are used to establish a connection with a legal user request. One is SYN cache mechanism and another one is SYN cookies defense mechanism. Both are not in the satisfactory level due to its request-response time is increased by 15% and poor performance [12].

2.18. XML Signature Attack

Technology behind the XML signature attack is Simple Object Access Protocol (SOAP). SOAP message comprises security header with a signature element which addresses additional message parts. XML messages can be validated by its id; therefore it is possible to attack the information through its web service user id. Normally SOAP message recipient checks whether signature is correctly validated as per norms or not by comparing id. XML signature attack carries on malicious user, who copies the SOAP body and inserts it as element of a header in the request. There on all the control related to SOAP message carried out by malicious attacker. The solution is to follow the WS-Security policy to protect against XML Signature attack [13].

2.19. Intrusion Detection Methods and Techniques

Intrusion Detection Systems (IDS) are indispensable part of securing cloud data in distributed environment. The primary goal of IDS is used here to detect intrusion behavior from malicious host or network and attain appropriate response. IDS is mainly categorized into two types, they are network based and host based. The prominent feature of IDS is to provide unusual activities by sending notification alert to the administrator to block distrusted connection and also able to distinguish among intruders from inside the organization (threat posed by insiders) and from malicious hackers [14]. Intruders can use a variety of attacks to make use of cloud systems, they are,

- DDoS attack
- Insider attack
- Hypervisor level attack
- User to root attack
- Backdoor channel attacks
- Port scanning
- Flooding attack
- Virtual Machine level attack (VM)

2.20. Intrusion Detection System types

There are various types of intrusion detection methods are used in cloud computing.

2.20.1. Host-Based Intrusion Detection System (HIDS)

Host based intrusion detection system is a software which monitor the host machine and sends an alert when a distrustful event occurs. This type of IDS is used to collect all the incoming and outgoing packets traffic from the user terminal. To detect anomalous behaviors, HIDS software can be installed in hypervisors or virtual machines to inspect log files and access control policies.

2.20.2. Network-Based Intrusion Detection System (NIDS)

Network based intrusion detection system monitors network traffic and network packets to detect attacks. In a network, number of host machines are connected and analyzed, NIDS is responsible for listening and defending the network segments. NIDS has the most powerful mechanism to detect network intruders by creating real time comparison and it overcomes the drawbacks of Host based IDS. Cloud server use network IDS on the virtual machine or hypervisor to monitor network packets log and protect from suspicious activity [15]. Cloud provider is only responsible for deploying NIDS in the cloud environment and the major drawback is that any attack happens outside the supervisor there is no guarantee to the data.

2.20.3. Hypervisor Based Intrusion Detection System

Hypervisor based intrusion detection system runs on Hypervisor Layer. Virtual machines are created and executed by hypervisor, each virtual machine in a network is called guest machine. Here network communications are monitored between VMs, Hypervisor and VM, and within the hypervisor. Hypervisor based IDS maintains higher data availability in the cloud server and in the virtualized cloud environment, it contributes more to protect, analyze, and detect malicious intruders [15]. Example of hypervisor based intrusion detection is Virtual machine introspection based IDS (VMI-IDS).

2.20.4. Distributed Intrusion Detection System

Distributed Intrusion Detection System has numerous IDS in a large network connection, which uses host based and network based IDS's. Every single Intrusion detection system communicates each other and central server for monitoring activities. DIDS is appropriate mechanism for Cloud based attack detection and log maintenance. In the cloud environment, DIDS works on host machine or processing server database, and different IDSs gather data from network and host system and convert them to standard format. As a final point, centralized analyzer get the standard format of data from IDS [16].

2.20.5. Network Behavior Analysis Intrusion Detection System

Network behavior analysis (NBA) is a process of improve the protection of a network by supervising unusual traffic flows and observing abnormal actions, such as DDoS attacks, some category of malwares, and strategy violations. DDoS attack is an essential security risk to internet service vendors and large network infrastructures [16]. Based on the network behavior, threats can be identified and maintain the log file.

2.20.6. Intrusion Prevention System (Inline Security System)

Intrusion Prevention System (IPS) is used to prevent the system from threats and observe the network traffic. When a system is vulnerable, the attackers attempt to inject malicious code to the targeted application and get control of an application. IPS (Active system) is advanced and more efficient method of IDS (Passive System) [17]. It has direct communication pathway among source and destination, so that system actively monitor the network traffic and take action according to that, such as

- Sends an alarm signal to the admin
- Avoid suspicious packets
- Jamming network disruption from the starting address
- Refresh the connection

2.21. Intrusion detection techniques

2.21.1. Pattern-Based Intrusion Detection

Pattern based detection is also known as Signature based detection, which detects threats based on the predefined pattern but does not detect latest threats since it does not hold updated recent patterns. This pattern based approach is used in host and network based IDS to monitor the malicious behavior.

2.21.2. Anomaly-Based Intrusion Detection

Anomaly-based intrusion detection is used to detect anomalous, unusual (abnormal) attacks using existing behavior pattern. Existing behavior of the user, host, and network connections over the period of time can be taken and stored in the database; anomaly detectors gather normal or usual data which gives normal behavior [17]. This intrusion detection system detects and gives alarm automatically with the help of existing usual behavior data. IDS has ability to find new types of errors without modifying existing data using Threshold detection, Statistical analysis, Rule based measures, Neural networks, and Genetic algorithms. One disadvantage observed in this system is that to make effective IDS, it needs accurate updating of behavior data.

3. Comparison of Cloud Security Attacks and Analysis

S. No	Name of the Attack	Functions of the attack	Solutions for the attack
1	Cookie Poisoning	modification of the data of a cookie	Imperva Secure Sphere Web Application Firewall (WAF)
2	Hidden field manipulation	control over the hidden field data	Dynamic security mechanisms required to avoid this attack
3	Sql injection attacks	Access unauthorized data using SQL command by the attackers.	Dynamically generated SQL code to prevent from SQL injection attack
4	Man in the middle attacks	Attacker resides middle of the network and to misuse the communication.	Implement widespread email security solution
5	Cloud malware injection attack	Inject malicious codes to the cloud system for anonymous access of cloud data by the malicious intruders.	Incoming requests should be sent to service instance integrity check and adopt the system for valid hash value for every user
6	Backdoor and debug options	Attackers use applications as a backdoor for their entry into cloud system.	Avoid applying debug options in the application itself.
7	Google hacking	Google Search engine processes all users' secret information via internet, which makes vulnerability to the users.	Install standard security procedures and Continuous data protection (CDP) should be essential for data recovery.
8	Cross site scripting xss	Intruders inject malicious script on trusted website.	Active Content Filtering, Content based data leakage prevention technology, and web application vulnerability detection technology.
9	Hypervisor issue or vm level attacks	Once hypervisor gets attack then all the guest operating systems are controlled by the attackers.	VMM application should provide strong authentication.

10	Dictionary attacks	Possibility of all the word combination and which decrypts the account password unethically.	Get delay response from the server and lock the account, if attempt exceeds the limit.
11	BGP prefix hijacking	Permitting the malicious users to access Faulty IP addresses	Autonomous security system
12	Port scanning	Port scan attack takes place because of open port.	Standard encryption technique is required to secure ports
13	DNS attacks	Attacker direct all arriving packets traffic to their chosen server, when converting DNS into IP address and capture incoming e-mails	DNSSEC, Radware carrier solution
14	Sniffer Attacks	capture the sensitive information at the Ethernet frame point by the attackers	ARP and RTT based detection platform and encrypt network transmission data
15	Amplification attacks	Produce large response by persuading the distributed network device in a cloud environment	Need to setup high performance improvised operating system, load balancing, reduce the network connection rate
16	Smurf attack	Using ICMP echo request packet to produce Denial of service attack	To stop sending ICMP packets to the IP broadcast address, configure the operating systems in the PaaS layer, Ingress filtering
17	DDoS attack	Attackers generate large number of request to the cloud server for compromising data availability.	Install Intrusion detection system in all the virtual and physical machines.
18	XML signature attack	SOAP message comprises security header with a signature element which addresses additional message parts which is processed in TLS layer. hacker may possible to change the SOAP message and signature value in XML document	Adopt the WS-Security policy and preserve a digital certificate for XML script to protect against XML Signature attack

Table 1

IDS	Types	Advantages	disadvantages
Methods	HIDS	• HIDS is able to confirm, if an attack is thriving or not. • It can monitors all users activities	• Deploying HIDS is difficult.
	NIDS	• Easy to deploy, no need to change existing infrastructure. • Easily detect the attacks.	• This type of IDS only gives an alert of the attack. • Not possible to monitor all the users activities in a network.
	Hypervisor based IDS	• Hypervisor based IDS consists of Virtual Machines and Hypervisors. User can monitor and analyses the communication between them.	• It is difficult to understand the system structure, because newly invented IDS method for cloud users.
	DIDS	• Both NIDS and HIDS characteristics are used and gain the benefits of them.	• Distributed Intrusion Detection System works on centralized cloud environment, so it is difficult to manage the servers due to overloading.

	Network behavior analysis IDS	• Network behavior analysis IDS is well suited for DDoS Attack and it detects new and unpredicted vulnerabilities. • It is advanced method for Detecting intrusions like unexpected traffic flows, certain kind of malware programs, etc., • Less dependent on operating system specific mechanisms.	• The major disadvantage of this method is high false alarm rate. • Except existing behavioral pattern, the system not able to detect new threats.
	Intrusion prevention systems	• It prevents threats from attacks. • HIPS Prevents host (system) level attacks. • NIPS Prevents attacks from the group of computers are connected together.	• Intrusion prevention system accuracy is lower than Intrusion detection systems.
Techniques	Pattern based	• Intrusion can be recognized by matching existing data collections (patterns). • Intrusion detection is more accurate when attack is already known. • With the help of detailed log file, easy to track the system. • Computational cost is reduced.	• Poor performance for unknown attacks. • Cannot detect newly updated threats, if database is obsolete.
	Anomaly based	• Not necessary to have an updated database for identifying intrusions. • Once system is installed then automatically it monitors the network activity, so minimum level of maintenance is sufficient.	• False positive can become more difficult with anomaly based techniques. • Discovering the limitations between abnormal and normal behavior is too complex.

Table 2: Intrusion detection systems comparative table

4. Conclusion

Cloud computing backbone is distributed platform on the other side expect large number of security measures and subsequent weaknesses in a system. This paper provides comparative study on various security attacks in the Cloud environment, impact of DDoS attacks and intrusion detection systems. DDoS attack is most challenging one for the users to access cloud resources. This comparative study assists to build secure cloud infrastructure and protect legitimate users from those suspicious attacks. Future work focused to high level security measures by considering the use of minimum resources and reduced performance degradation.

5. References

1. Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, “Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems”, ACM Transactions on Computational Logic, Vol. 2, No. 3, 2006.
2. M. Durairaj, P. Kannan, “A Novel Approach for Elastic Application Partitioning in Mobile Cloud”, IEEE - ICAET-4th International Conference on Advances In Engineering & Technology, India, 2014.
3. M. Durairaj, P. Kannan, “A study on Virtualization Techniques and Challenges in Cloud Computing”, International Journal of Scientific &Technology Research, Volume 1, Issue 1, 2014.
4. Amirreza Zarrabi, Alireza Zarrabi, “Internet Intrusion Detection System Service in a Cloud”, IJCSI, Vol. 9, Issue 5, No, 2, September, 2012.
5. B.Sumitra, C.R.Pethuru, M.Misbahuddin, “A survey of cloud authentication attacks and solution approaches”, International journal of innovative research in computer and communication engineering, vol.2, issue 10, October 2014
6. Ajey Singh, Dr. Maneesh Shrivastava, “Overview of attacks on cloud computing”, International journal of engineering and innovative technology, vol.1, issue 4, April 2012.
7. Sanchika Gupta, Padam Kumar, “Taxonomy of cloud security”, International journal of computer science, engineering and applications, vol.3, No.5, October 2013.

8. Junho Choi, Chang Choi,Byeongkyu Ko, Dongjin Choi, and Pankoo Kim, "Detecting web based DDoS attack using mapreduce operations in cloud computing environment", Journal of internet services and information security, vol.3, No.3/4, 2013.
9. Abdul Nasir Khan, Kalim Qureshi, and Sumair Khan, "An intelligent approach of sniffer detection", The international arab journal of information technology, vol.9, No.1, January 2012.
10. Niraj Suresh Katkamwar, Atharva Girish Puranik and Purva Deshpande, "Securing cloud servers against flooding based DDoS attacks", International journal of application or innovation in engineering and management, vol.1, issue 3, November 2012.
11. 11. H. Wang, C. Jin and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop- Count Filtering, " IEEE/ACM Transactions on Networking, vol. 15, no. I, pp. 40-53, Feb. 2007.
12. M. Gonzalez, M. Anwar, and J. B. D. Joshi, "A trust-based approach against IP- spoofing attacks, " 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 63-70, Jul. 2011.
13. D. Gollmann, "Securing Web Applications", Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002.
14. Richa Sondhiya, Maneesh Shreevastav, Mahendra Mishra, "To improve security in cloud computing with intrusion detection system using neural network", International journal of soft computing and engineering, vol.3, issue-2, may, 2013.
15. Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, Joaquim Celestino Junior, "An intrusion detection and prevention system in cloud computing: A systematic review", Journal of network and computer applications, June, 2013.
16. Soumya Mathew, Ann Preetha, "Securing cloud from attacks based on intrusion detection system", International journal of advanced research in computer science and communication engineering, vol.1, issue 10, December 2012.
17. Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, Muttukrishnan Rajarajan, " A survey of intrusion detection techniques in cloud", Journal of network and computer applications, June, 2013.