ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

Cloud Security Problems and Encounters from DDOS Attacks Using Intrusion Recognition System

[1]Dr BJD KALYANI, Assistant Professor, Department of Computer Science and Engineering, Priyadarshini Institute of Science and Technology for Women, Khammam, India.kjd_kalyani@yahoo.co.in
[2]Y venkateswara Reddy, Associate professor, Dept of ECE, Mallareddy institute of technology, Maisammaguda, Dulapally, Secunderabad, Telangana 500100
[3]K saikumar, JRF, Dept of ECE, KoneruLakshmaiah Educational Foundation, Green Fields, Vaddeswaram, Andhra Pradesh 522502, saikumarkayam4@gmail.com

Abstract:
Currently, a distributed denial of service (DDoS) assault scenario affects the Internet community. IDSs are becoming an essential component of systems and network security. This article presents research on current DDoS assaults and a comparison of the main cloud-based DDoS defensive technologies. The approach, deployment layer, benchmark datasets, tools, and performance indicators for cloud DDoS solutions are all demonstrated. The goal of DDoS detection and protection for cloud infrastructure using learning algorithms is to prevent the limitations of existing solutions for practical use. In order to stop zero-day attacks, this methodology employs anomaly detection to find unusual patterns in the data. A considerable enhancement is made to the service availability and quality of cloud apps to safeguard the genuine users from DDoS assaults.

Keywords: Cloud Computing, DDoS, DDOS, Security Issues and Research Challenges

1.0 INTRODUCTION

Cloud computing has a significant impact on nearly every industry. A few of the primary benefits of utilizing cloud infrastructure include its low cost, limitless storage capacity, device variety, scalability, backup and recovery, energy efficiency, rapid deployment, and agility. Cloud computing has had a major impact on the way businesses operate today. Since its introduction, this new technology has forced organisations of all types to adapt. Experts in the field believe that cloud infrastructure will continue to assist enterprises of all sizes in the next few years. [1]. When a company is trying to figure out whether or not cloud infrastructure is the perfect fit for them, security is the determining aspect. As DDoS assaults have become easier to carry out in recent years, there has been an increase in the number of attacks. [2]. A DDoS assault occurs simultaneously with numerous systems trying to access the same server. Re-throwing an application even after a server response is received is a widespread condition. [3]. As a result, a DDoS detection system is a critical part of creating a company's statement of principles and procedures for ensuring data security. DDoS assaults in the cloud can be detected via ICMP flooding, HTTP flooding, and TCP flooding, among other techniques[4]. The purpose of this study is to detect DDoS attacks in an OpenStack-based private cloud. The most accurate and precise classifier model was chosen among a number of models. The network traffic from the cloud is recorded and analyzed dynamically to discover anomalies. It is at this point that cloud administrators are informed of the system that is responsible for launching the attack. Next, the cloud administrator has the option of adding a firewall rule to include the system's ip address in its protection.

Applications:

The applications of cloud computing are as follows

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

- It provides secure data storage center.
- Cloud computing solutions eliminate the problem for advanced hardware on consumers, which is also efficient in decreasing the hardware expenditures.
- Cloud computing can be achieved through the sharing of resources between various systems.
- The Cloud allows for an almost infinite number of internet connections for clients.

Scope of the Study

Focusing on intrusion detection and prevention systems, this survey gives a survey on fog and cloud computing, and proposes how businesses might apply these technologies in their own systems. The benefits and drawbacks of various technologies are thoroughly analysed. To better understand potential cyber dangers, a study of network topologies is also conducted. On the basis of this research, it is possible to see how private and public cloud computing and intrusion detection/prevention can work together in a way that is both cost-effective and effective.

2.0 Literature Review

In [5], An Intrusion Detection System (IDS) programme based on Snort is provided by the authors to help detect DDoS attacks. Specifically, a system is proposed to notify the network administrator of an assault on any resource, together with details on how and where it occurred. The attacker is also put on hold until the network administrator implements a backup strategy. [6]. By identifying DDoS attacks at an early stage and adjusting various settings, the suggested solution helps to reduce the impact of DDoS attacks. Cloud computing SDN-based cloud security against DDoS assaults is discussed in [7] by the authors [7]. It also emphasises the necessity of SDN security in protecting itself from the threats. DDoS attacks in cloud computing are also covered in this work. In [8], This paper discusses how to construct a cloud architecture. In addition, he stresses the significance of spotting DDoS attacks at the network layer. In order to detect DDoS assaults in SDN, this research provides machine and deep learning methods such as Decision tree, Nave Bayes, DNN, and KNN. Then, these algorithms are tested for their detection rates and efficiency. Cloud-based network intrusion detection systems (NIDS) are proposed in [9]. In the NIDS module, Snort and a signature-apriori technique are used. It creates new rules based on the packets it detects. Snort's performance is boosted by the addition of these new rules to the configuration file. To detect known attacks and their derivatives in Cloud, it monitors network traffic to ensure minimal false positive rates while maintaining an acceptable computing cost. [10].

3.0 INTRUSION DETECTION SYSTEM FOR DDOS

A DDoS attack prevents a legitimate user from using a service because it overwhelms the network with traffic. The defences focus on detection, identification, and filtration approaches to combat DDoS attacks. Using an Intrusion Detection System (IDS) like SNORT is one of the most effective mechanisms for detecting and preventing DDoS. An IDS monitors the system and network for any malicious activity and reports to the administrator to take necessary action against it. Virtual machines are used to run the IDS. It is possible to install the IDS system on a user's physical PC as well. Techniques like wavelet, spectral analysis, statistical methods, and machine learning can be used to detect DDoS attacks. Using IP traceback, attackers can be directly traced.Traditional IDS that were used on the network were single threaded. When dealing with the dynamic and distributed nature of the cloud

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

environment, these types of systems were rendered inefficient As a result, DIDS was chosen as the best IDS for a cloud environment. IDS has emerged as one of the most effective ways to defend against DDoS attacks.

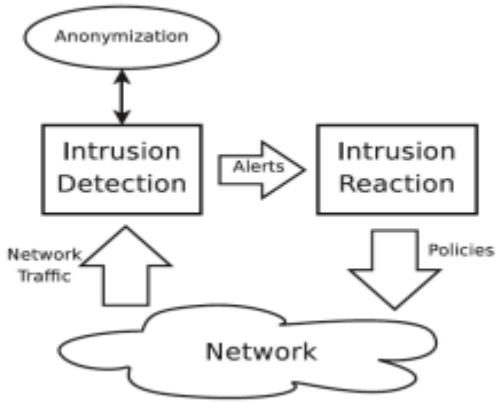

Figure 1: Framework for intrusion detection system is represented

It is thus a passive attack that can take over the resources of the victim and use them as zombies in a DDoS attack. Cloud users' resources can be accessed and controlled by an attacker if the system is breached. A firewall, signature and anomaly-based intrusion detection system is employed to prevent such attacks.

Intrusion Reaction system: The exchange of information and the tracking of the assault resources are triggered by alert signals. The IP infrastructure described above is required for the design described above. An Intrusion Detection System Framework.

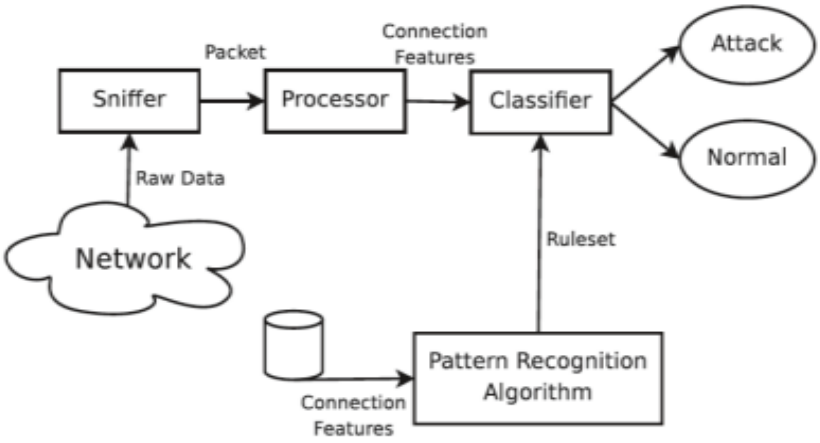

Figure 2: Framework for Intrusion Detection system

Research challenges in cloud computing

However, cloud computing has swiftly emerged. A lot of the cloud computing research is still in its infancy. Many concerns remain unresolved and new difficulties are developing in every industry on a daily basis. The following are a few cloud computing research difficulties.

- Service level agreement (SLA)
- Cloud data management and security
- Data Encryption
- Virtual machines migration
- Access controls
- Multi-tenancy
- Reliability and availability of services.

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

- Service level agreement (SLA)

A single application can be duplicated across several servers on a first-come, first-served basis. While SLAs are sometimes used as a form of insurance against potential legal concerns, they provide only a limited level of confidence to other customers. Several critical challenges, such as data security, downtime, and pricing structures, are

Threats to security in cloud computing

In the world of Cloud Computing, security is the primary concern. As a result of previous research, cloud security concerns have been categorized depending on their service model. Various levels of cloud security are required, including the network, host, and application levels. There are several types of security lapses that can occur at this level, and they are as follows.

Cross Site Scripting attacks: Malicious code is injected into web content in order to gain control of a user's machine or expose confidential information to the attacker, both of which are possible outcomes from this attack.

Man in the Middle attack: An intruder enters into a discussion between a sender and receiver and makes them believe that only they are participating.

Network level Security

Problems associated with networks are:

DNS attacks: Translating a domain name into an IP address is the job of a DNS server. It's much easier to recall a domain name. However, it is possible for a user to be redirected to another malicious cloud while calling a server by its web domain.

Sniffer attacks: It's an application programme that intercepts network packets and reads the data they contain if they aren't encrypted.

Issue of Reused IP addresses: This user's IP address is given to another user when they leave a network by not clearing DNS caches immediately after changing one's IP address in DNS, this could put the prior user's security at risk. Because of this, there is a potential that the data of the prior user will be available to the user database.

4.0 RESULTS AND DISCUSSIONS

Cloud security remains a challenge to this day due to DDoS attacks. Complex and aggressive DDoS attacks are difficult to handle since the botmaster owns unsecured nodes that are used to target cloud services, as demonstrated in Figure 3 This exploit wreaks havoc on cloud systems by actively inserting malicious packets into the cloud. DDoS attackers are increasingly employing advanced techniques to bring down and disrupt cloud services. The DDoS targets include surprisingly political institutions, financial companies, defense and military departments. Major websites like Facebook and eBay have been subject to DDoS attacks that interrupt service and cause financial loss by blocking genuine users from accessing the sites. Without even realizing it, bots can take control of cloud-based workstations and launch DDoS attacks against vital servers. It is possible to launch a powerful DDoS assault without the requirement for technical knowledge or consequences thanks to a readily available DDoS attack technique.

DDoS Tools:

Trinoo, Tribe flood network, TFN2K, Stacheldraht, Mstream, Shaft, Trinity, Knight, Low orbit canon, High orbit canon, and Slowloris are just a few of the well-known DDoS tools

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

that can be found on the internet nowadays. the DDoS attack tool classifications together with specific protocols and operating layers.

Table 1: DDoS tools

DDoSTools	Protocol	Layer
Trinoo	UDP	Transport
Tribe FloodNetwork TribeFlood Network 2000 ,Stacheldraht,Shaft	UDP, ICMP,SMURFandTCPSYN	Network andTransport
Mstream	TCPACK	Transport
Trinity	TCPrandomflag,TCPRST,TCP established andTCPfragment	Transport
Knight	UDP, SYN andurgent pointerflood	Transport
Low Orbit IonCannon	TCP,UDP,HTTP	Application andTransport
High OrbitIon Cannon,Slowloris	HTTP	Application

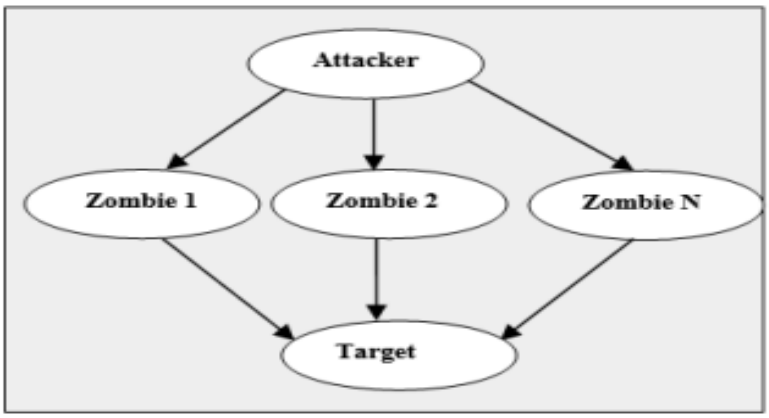

Figure 3: DDoS attack scenario

Proposed Model:

The network topology of the cloud model being studied must be taken into account when designing an attack scenario. The first step is to choose if the cloud model will be public, private, or a hybrid of the three. It is determined by the network model that the software/hardware requirements and operating platform are selected. DDoS tools numerous, and each tool's properties are widely described in the literature. As part of this stage, you must decide how many virtual nodes will participate in the attack and how long it will last. The strength of the attack is determined by the attacking parameters. Cloud DDoS attacks can be detected and prevented by capturing real-time traces from the attack scenario, according to the researchers.

When compared to traditional DDOS attacks, low-rate DDOS attacks have an average traffic flow that is substantially lower and looks practically normal traffic, making detection and prevention challenging. Because of this, it is imperative that a more effective cloud security solution be developed. This method uses the Hidden Markov model to observe traffic flow

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

features in the network, and the features seen are applied to train a random classifier to identify disordered traffic flow in the network.

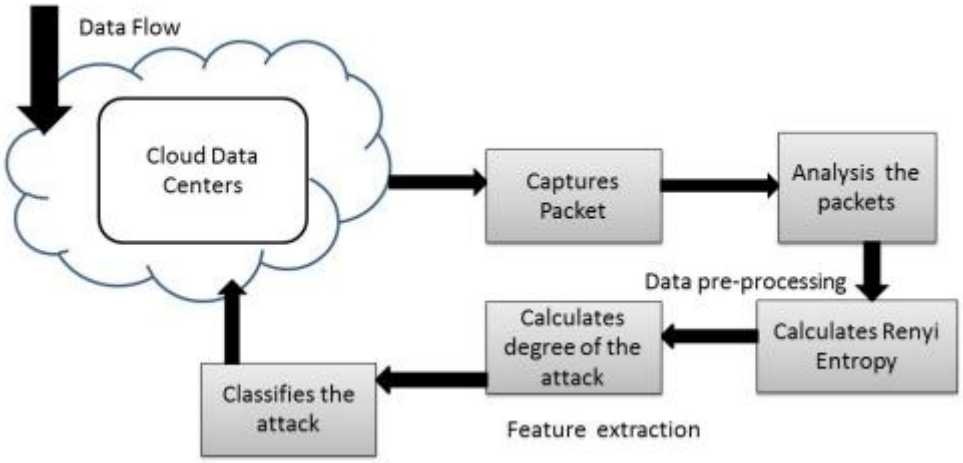

Figure 4: Proposed Block Diagram

Table 2: DDoSdetectiontechniques

Techniqueused	Layer	Dataset	Tools	PerformanceMetrics
ForensicAnalysis	Network	CNSMS	NA	NA
Confidence-basedfiltering		MAWIWorkingGroupTrafficArchive	Attack tools,net-filter,C++	False Positive Rate, FalseNegativeRateandProcessTime
RankCorrelation		Simulated	ns2	NA
CollaborativeIntrusion Detection		NA	NA	NA
MultistageAnomalyDetection		NA	NA	NA
DistributedIntrusionDetection		NA	NA	NA
SecuringCloudServers		Simulated	ns2	DetectionRateandFalsePositiveRate
IntrusionDetectionSystem	Network/Transport	Simulated	CloudSimulatorandJava	ComputationTimeandPacketsLost
DetectingIntrusions		Virtual	NA	NA
Statistical-basedfiltering		RealTime	Netwag,Jpcap	Accuracy,Detectionaccuracy,FalseAlarmRateandProcessingTime

DDoS assaults are common in cloud security, and the application of advanced tools poses a significant threat to cloud providers. DDoS attacks can be devastating. DDoS is a difficult challenge to solve, even with the aid of security measures.

Conclusion:

The possibility to securely preserve data is a key benefit of the cloud. As a result of its 'unlimited storage' feature, the cloud has become increasingly important. One other brand-

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

new area of expertise is the OpenStack cloud. There are other features that may be added to cloud setups, like the ability to manage many users and dashboards, and the ability to create your own topology. However, OpenStack's current firewall did not particularly address DDoS threats. As a result, OpenStack needed both a DDoS detection module and a firewall to provide adequate protection. A notification to the network administrator in the event of a DDoS assault would be useful as well. This experiment provides an overview of DDoS attacks, including bandwidth flooding and connection flooding, detection systems, and research issues and challenges. Also included in this report is a comparison of current DDoS detection technologies and a way to notify the administration of the IP addresses responsible for the attack.

Future scope

The whole IT industry is predicting the automation process. We've offered an overview of how it will be and the primary security challenges that will be confronted in the future with our imaginations. We expect our research to shed light on the design issues in cloud computing and pave the way for future research in this area, as automation in cloud computing is still an ideal process requiring further clarification and study.The research can be extended to discover how different DDoS assaults can overload the controller in the cloud and thus cause issues with the OpenStack-based private cloud. DDoS assaults can be detected using a larger range of algorithms than previously stated. In order to better detect various types of DDoS attacks, optimized algorithms in the Hadoop architecture can be utilized.

REFERENCES

1. Mukkamala, Srinivas, Guadalupe Janoski, and Andrew Sung. "Intrusion detection using neural networks and Support vector machines." Neural Networks, 2002. IJCNN'02. Proceedings of the 2002 International Joint Conference on. Vol. 2. IEEE, 2002.
2. Barki, Lohit, et al. "Detection of distributed denial of service attacks in software-defined networks." Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016.
3. Bikram Khadka, Chandana Withana, AbeerAlsadoon, Amr Elchouemi, 2015. Distributed Denial of Service attack on Cloud Detection and Prevention. School of Computing and Mathematics, Charles Sturt University, Sydney, Australia Hewlett Packard. 2015 International Conference (pp. 1-5). IEEE.
4. Qiao Yan, F. Richard Yu, Qingxiang Gong, Jianqiang Li, 2015. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. 2015 IEEE Communications Surveys & Tutorials (pp. 2-4). IEEE.
5. Narayan D G, Mohammed Moin Mulla, LohitBarki, Amrit Shidling, NisharaniMeti, 2016, September. Detection of Distributed Denial of Service Attacks in Software Defined Networks. 2016 Intl. Conference on Advances in Computing, Communications, and Informatics (pp. 1-3) (ICACCI).
6. Chirag Modi,Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, MuttukrishnanRajarajan, Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing, Procedia Technology, Volume 6,2012,Pages 905-912

ISSN- 2394-5125 VOL 07, ISSUE 12, 2020

7. S. Umarani, D. Sharmila," Predicting Application Layer DDoS Attacks Using Machine Learning Algorithms" World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:10, 2014.
8. P. S. Sheela and M. Choudhary, "Deploying an OpenStack cloud computing framework for a university campus," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, 2017, pp. 819-824.
9. DimitriosGkounis," Cross-domain DoS link-coding attack detection and mitigation using SDN principles" Master Thesis MA-2013-18 October 14, 2013, to April 13, 2014.
10. Wang, Bing, et al. "DDoS attack protection in the era of cloud computing and software-defined networking." Computer Networks 81 (2015): 308-319.