# DETECTING DDOS ATTACK USING INTRUSION DETECTION SYSTEM

Ezzureen Faznien Ibrahim
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
50250 Kuala Lumpur
kaitozuren95@gmail.com

Shahrinaz Ismail
University Kuala Lumpur
Malaysian Institute of Information Technology 50250 Kuala Lumpur
shahrinaz@unikl.edu.my

***Abstract*—Cloud Computing is the delivery of computing services that serves storage, databases, networking, software, analytics and more over the internet. The cloud user should concern about the security of the cloud service. This is because cloud computing services are delivery by a third party who owns the infrastructure. Cloud computing is emerged as the modern technology which developed in last few years and considered as the big thing in the years to come. This paper introduces the existing issues in cloud computing such as security, privacy and reliability. This research focuses to provide some guidelines to secure the data in cloud computing. Malware attacks can occur in cloud computing due to lack of security systems. Our result indicate that user did not aware of security data in cloud computing and also the benefit of using cloud computing.**

***Index Terms*—About; cloud computing; ddos attack; intrusion detection system.**

## I. INTRODUCTION

Cloud provider typically implement security system, but involvement of a different party could be needed to improve the security levels. Security is a significant concern driving decision making in the cloud computing space. Either the security standards are published by provider or the buyer requires the use of objective security standards, the issue and challenge of the security is best addressed at the outset and explicitly documented in the cloud services.

Advantages prevention from malware attack like DDoS in cloud computing are to secure the data. Solutions offered by a reliable cloud computing service will detect DDoS attacks and provide effective responses to ensure 24/7 availability. It also can offer solutions that protect users' credentials from being stolen. Besides, without a secure platform, hackers may eavesdrop on out transactions, manipulate data and return falsified information that harms clients of cloud computing.

Cloud computing security is basic of cloud technologies which automated security management, disaster recovery, redundant system and also making it safer with critical data cloud solutions. Lastly this research is to know about malware attack and how IDS can prevent this attack.

## II. RESEARCH OBJECTIVES

This research focuses to identify Distribution Denial of Services (DDoS) attack in cloud computing using Intrusion Detection System (IDS).

- To identify DDoS attack using Intrusion Detection Systems in cloud computing
- To study the importance of preventing cloud computing from being attack.

### *A. Problem statement*

The popularity of cloud computing is increasing day by day but there are some challenges that are faced by it because of the challenges in cloud is security. Security is one of the major issues which is reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market (Subashini et al., 2011). DDoS attacks are major security risks in cloud computing where resources are shared by many users. Although cloud computing is an emerging technology, the recent increased use of cloud services required current insights into necessary security requirement and it is solutions.

Furthermore, an analysis of cloud computing security issues describe how to identify characteristics of DDoS attack using an Intrusion Detection System (IDS) tool based on Snort to detect DDoS. In secure information management set of policies and security requirements are derived from multi-user organizations. The cloud federation issues are resolved by single on, authentication and authorization.

### *2.3 Comparison among the Existing Solutions*

Intrusion Detection System IDS refer to a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

Subashini et al. (2011) suggested Software as a Service. SaaS is software deployed over the internet and/or is deployed to run behind a firewall in local area network or personal computer. The key characteristics include Network-based access to, and management of, commercially available software and managing activities from central locations rather than at each customer's site, enabling customers to access application remotely via the web.

According to Chonka at.el. (2010), Service-oriented trace back architecture (SOTA) is web security service application that is product-neutral. Its main objective is to apply a SOA approach to trace back methodology. This is in order to identify a forged message identify, since one of the main objective of X-DoS and DX-DoS is to hide the attacker's true identity.

Carlin et al. (2015) confirmed that IDS designed for cloud computing can be classified into for main categories. Host-based IDS (HIDS) monitors and analyses log files, security access and user login information to detect intrusive behavior. Network-based IDS (NIDS) monitors IP and transport layer headers with behavior being compared with previously observed behavior in real time. Hypervisor-based IDS (HyIDS) allows users to monitor and analyses communication between VMs, within the hypervisor based virtual network and between the hypervisor and VMs. Distributed IDS (DDIS) consists of a number of IDSs, HIDS and NIDS, placed across a large network.

As a conclusion, many method can be used to prevent when the malware attack the cloud computing. Whether it is software or hardware, it also can help to secure the data in cloud computing.

## III. LITERATURE ANALYSIS ON PROBLEM STATEMENT DOMAIN

The security is the biggest problem of this system, because the services of cloud computing is based on sharing (Singh & Shrivastava, 2012). According to Kuyoro (2010), usually cloud computing services are delivered by a third party provider who owns the infrastructure. It is supported by Arockiam & Monikandan (2013), it is more reliable and flexible to users to store and retrieve their data at anytime and anywhere.

The findings by Rajak & Verma (2012) showed that, a cloud computing environment data protection as the most important security issue. In an observation-based study by Carlin et al., (2015), the findings have shown the exploitation of compromised virtual machines to execute large-scale Distribution Denial of Service (DDoS) attacks. One of the efficient methods for detecting DDoS is to use the Intrusion Detection System (IDS), in order to assure usable cloud computing services (Lonea et al., 2012).

In placing more emphasis, (Subashini et al., 2011) claimed that security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. This is supported by Darwish et al. (2014), especially true today as distributed denial-of-service (DDoS) attacks constitute one of the largest threats faced by Internet users and cloud computing services.

DDoS attacks are major security risks in a cloud computing environment, where resources are shared by many users. In addition, DDoS is an attack that consumes all the cloud resources may have making it unavailable to other general users (Khadka et al., 2015). He also identifies characteristics of DDoS attack and provides an Intrusion Detection System (IDS) tool based on Snort to detect DDoS.

Based on article 'Survey on DDoS Attack in Cloud Environment' by Agrawal & Bhatt (2015), DDoS instead of using attackers own IP it will use some compromised machine (bot machine) which will flood the targeting server in synchronized way. Moreover, DoS attack is triggered to make unavailable the targeted system to its intended users by flooding the targeted system with malicious traffic using a single node (Prabadevi et al., 2014).

Many research problems are yet to be identified in cloud computing. DDoS attacks are currently a major threat and work against the availability of cloud services. With each developed defence mechanism against DDoS attacks, an improved attack appears (Darwish et al., 2014). Therefore it is very necessary to provide Detection and Prevention mechanism for the attack which targets the availability. There is lot of work going around providing cloud an effective way to defeat DDoS attack (Agrawal & Bhatt, 2015).unit tesla). Refer to the equation as "Equation (X)" where X is the equation number.

## IV. LITERATURE ANALYSIS ON THE DOMAIN OF THE PROPOSED TECHNOLOGY

Cloud computing is Internet based infrastructure where shared resources, software and information are provided to computers and other devices. However, there are many issues and challenges in cloud computing. DDoS is one of the identifying cloud security issues and it can be detecting by Intrusion and Prevention System (IDS). This is supported by Achbarou et al. (2017), when such a suspicious event is detected, IDS sends an alert message to a person or monitoring console to trigger some actions for preventing these attacks.

According to Kumar & Sharma (2015), Distributed denial-of service (DDoS) attacks pose a serious threat to network security. Intrusion detection system is proposed based on knowledge multithreaded system (Samani et al., 2016). Intrusion detection system plays an important role in the security and perseverance of active defence system against intruder (Navaz et al., 2013). To solve the security issues we need IDS, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection (Sharma, 2012).

Intrusion detection (ID) is the art of detecting inappropriate, incorrect, or anomalous activity and also evaluates suspicious activity that occurs in corporate network (Murthal et al., 2011). In such case, the administration of IDS in cloud becomes the responsibility of cloud provider. Their research found that, IDS basically generate an alert in the form of a report and notification upon the detection of an intrusion. Based on article Achbarou et al. (2017), after effective treatment of IDS alerts watched proposed move to a monitoring service by third parties, who in turn informs the cloud directly to users about their system under attack.

Cloud computing security is still considered the major issue in the cloud computing environment. The popularity of Cloud Computing is increasing day by day but there are some challenges that are faced by it because one of the challenges in cloud is security. DDoS attacks have been placed first on the list of cloud attacks (Kumar & Sharma, 2013). In developing solutions to cloud computing security issues it may be helpful to identify the problems and how to mitigate its. One of the solutions on defences Distributes Denial of Service Attack (DDoS) is by using Intrusion Detection System (IDS) technique. However, some solutions could not detect nor perfectly mitigate all the possible attacks. In all cases, and as always in the security field, no solution is perfect (Bonguet et al., 2017).

## V. Conclusion

Cloud computing is a new way of delivery computing resource, and it is not a new technology. Security awareness is important for each user that uses the cloud computing services. Every user must know about CIA; confidentiality, integrity and availability to keep all information or data from outsider. Authorization should keep secret all password or data from unauthorized to make less attacker to attack the network. Since many of people are using cloud computing but still have lack of awareness in preventing cloud computing from being attack. So in this report, we are doing some research on the importance of preventing cloud computing from being attack.

## References

Achbarou, O., Kiram, M. A., & Bouanani, S. E. (2017). Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems. International Journal of Interactive Multimedia and Artificial Intelligence, 4(3), 61. doi:10.9781/ijimai.2017.439

Ajey Singh, & Dr. Maneesh Shrivastava. (2012). Overview of Attack on Cloud Computing. International Journal of Engineering and Innovative Technology (IJEIT), 1(4), 321-323.

Bonguet, A., & Bellaiche, M. (2017). A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet, 9(4), 43. doi:10.3390/fi9030043

Carlin, A., Hammoudeh, M., & Aldabbas, O. (2015). Defence for Distributed Denial of Service Attacks in Cloud Computing. Procedia Computer Science, 73, 490-497. doi:10.1016/j.procs.2015.12.037

Chonka, A., Xiang, Y., Zhou, W., & Bonti, A. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34(4), 1097-1107. doi:10.1016/j.jnca.2010.06.004

Darwish, M., Ouda, A., & Capretz, L. F. (2014). Formal Analysis of an Authentication Protocol against External Cloud-Based Denial-of-Service (DoS) Attack. International Journal for Information Security Research, 4(1), 400-407. doi:10.20533/ijisr.2042.4639.2014.0046

Dr. L. Arockiam, & S. Monikandan. (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering, 2(8).

Dr. S. Saravana Kumar, R. Senthil Kumar, R. Arun Prasad, & S. Thiraviam. (2015). Detecting and Preventing DDoS Attacks in Cloud. International Journal of Innovative Research in Computer and Communication Engineering, 3(3), 1877-1884.

Khadka, B., Withana, C., Alsadoon, A., & Elchouemi, A. (2015). Distributed Denial of Service attack on cloud: Detection and prevention. 2015 International Conference and Workshop on Computing and Communication (IEMCON). doi:10.1109/iemcon.2015.7344496

Kirtesh Agrawal, & Nikita Bhatt. (2015). Survey on DDoS Attack in Cloud Environment. International Journal of Innovative and Emerging Research in Engineering, 2(3), 18-22.

Kumar, N., & Sharma, S. (2013). Study of intrusion detection system for DDoS attacks in cloud computing. 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN). doi:10.1109/wocn.2013.6616255

Kuyoro, Shade O, Ibikunle Frank, & Awodele Oludele. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 3(5), 247 - 255.

Lonea, A. M., Popescu, D. E., & Tianfield, H. (2012). Detecting DDoS Attacks in Cloud Computing Environment. International Journal of Computers Communications & Control, 8(1), 70. doi:10.15837/ijccc.2013.1.170

Mishti D. Samani, Miren Karamta, Jitendra Bhatia, & M.B. Potdar. (2016). Intrusion Detection System for DoS Attack in Cloud.

Prabadevi, B., & Jeyanthi, N. (2014). Distributed Denial of service attacks and its effects on Cloud environment- a survey. The 2014 International Symposium on Networks, Computers and Communications. doi:10.1109/sncc.2014.6866508

S.SyedNavaz, A., Sangeetha, V., & Prabhadevi, C. (2013). Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud. International Journal of Computer Applications, 62(15), 42-47. doi:10.5120/10160-5084

Sharma, P. (2012). A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. International Journal of Computer Applications, 41(21), 16-21. doi:10.5120/5824-8064

Shobha Rajak, & Ashok Verma. (2012). Secure Data Storage in the Cloud usingDigital Signature Mechanism.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. doi:10.1016/j.jnca.2010.07.006