Analysis of Attacks on Private Cloud Computing Services that Implicate Denial of Services (DoS)

MOSIUR RAHAMAN[1], BIBISUMAIYA CHAPPU[1], NIZIRWAN ANWAR[2], PANJI KUNCORO HADI[3]
[1]Asia University, Taiwan
[2]Esa Unggul University, Jakarta, Indonesia
[3]PGRI University, Madiun, Indonesia

ABSTRACT It is well established that the field of cloud computing is immensely gaging importance and is constantly evolving. Cloud computing is employed by the vast majority of organizations because of the overall increase in e-commerce and internet trade. Private Cloud Computing allows the user to use the resources (networks, servers, storage, applications, and services) that exist in a network cloud (Internet), so it can be shared and used together in any place. This makes interest for big companies to store data on the cloud service, Although the services and characteristics of Private Cloud Computing benefits and an attractive solution to the problem of Information Technology , Private Cloud Computing is not risk free or completely secure as well as can lead for data leakage , threat from insiders, and not close kemngkinan of DOS (Denial of Service). This study aims to determine the impact analisisdan DOS (Denial Of Service) to the server service Private Cloud Computing. The methodology used in conducting this research is using Model Forensics (The Forensic Process Model). The results of the analysis carried out will get digital evidence, such as IP Address, Packet data, time stamp, which indicates the occurrence of DOS (Denial Of Service).

KEYWORDS Cloud, Digital, DoS, Forensics, Investigation

I. INTRODUCTION

One of the major technical developments in information technology could be cloud computing [1]. A simple framework for users to access cloud resources and services using the Internet is provided by the revolutionary method known as cloud computing [2].Cloud computing is an application which is accessible from any location at any time and benefiting us in considerably lower cost. SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment. Organizations including educational institutions, hospitals, and banks have started embracing cloud services over the past few years, that are big cloud companies like Microsoft, Google, IBM, and Amazon [3].The use of cloud computing is becoming increasingly popular today now, whether for storage, networking, or computing, as the name implies. Based on a survey on cloud computing in 2019 [4], of the 786 enterprises that were respondents, 94 percent ($\approx$ 739 enterprises) of them use the cloud [5] [6]. In this analysis, Right Scale segments and examines enterprises according to their stages of cloud adoption using its Cloud Maturity Model [7]. Additionally, it has been seen recently that researchers are utilizing cloud computing and software defined networks (SDNs) [8]. The SMB cloud spending increased dramatically from 38% in 2021 to 53% in 2022, amounting to up to $1.2 million annually, according to Flexera's 2022 State of the Cloud Report. The four distinct levels of cloud maturity are identified by the Cloud Maturity Model. The four stages of cloud adoption by enterprises, from least to most experienced, are: Organizations that have not yet deployed apps onto the cloud but are creating cloud strategy and plans are known as watchers. Learners are new to cloud computing and are working on proofs-of-concept or initial cloud projects. Beginners want to gain experience with the cloud in order to determine future projects. Intermediate users have several cloud-deployed applications or projects already. They are concentrating on enhancing and growing the way they utilize cloud resources. Advanced organizations heavily rely on cloud infrastructure and want to reduce cloud costs while still maximizing cloud operations. As the number of users increases, so does the number of attacks. Based on a report provided by NetScout in February 2020, they found that in the second half of 2019, DDoS attacks were carried out 8.4 million times, about 23,000 times in one day or 16 times every minute. The number of such attacks increased by 16 percent from the global number in the second half of 2018 [2], [9], [10]. These resources can be provided by private, public, or hybrid clouds. Cloud Computing technology or cloud computing allows users to use resources (networks, servers, storage, applications, and services) that exist in a cloud network (Internet) so that they can be shared and used

together. Cloud Computing applies the method of accessing data from anywhere [11], using a file or device, and using the Internet as a place to store data, applications and others. Cloud Computing can be interpreted as accessing computer facilities together via the Internet from various locations [12] [13], [14] Cloud computing has become a trend [15], [16] at this time for companies. A survey conducted by Symantec together with Rez Research with corporate correspondents in 29 countries, including Indonesia, revealed that knowledge about cloud computing among corporations is increasing. In Indonesia, according to the survey, 100% of organizations have at least discussed or discussed cloud computing. This means there is a spike of up to 80% from before. More and more consumers move their data to the server.

The technological world where we currently live in is inherent to cyber-attacks that are continually developing and the tries to attack surface are rapidly rising. Although the services and characteristics of Private Cloud Computing provide attractive advantages and solutions to Information Technology problems, Private Cloud Computing is not risk-free or completely secure. It is crucial to anticipate Artificial Intelligence (AI) technology, that is a pleasant and potent current technology against cyber-threats as this technology is proficient of recognizing and performing on the cyber-based assault against the private credit data and password insights [17], [18].There are several types of threats in this private cloud computing technology, for example, Malicious Insiders, Data Breach, Insider threats, Data Loss, and DOS (Denial of Service) [19] [20] [21].

II. LITERATURE REVIEW

This study built a cloud computing server and tested it by carrying out a DOS (Denial Of Service) attack to prove the security of cloud computing services [22], [23]. Cloud computing [24] is an information technology computing service that includes hardware, software, and application services that can be obtained via the Internet. The service must be adapted to the needs of the user, and the service usage fee is charged according to the number of resources that have been used on a per month or per-minute basis [25].

The area of digital forensics known as network forensics focuses on the observation and examination of computer network traffic in order to acquire data, establish facts, or locate commands. The term network forensics is taken from terminology related to criminology. Network forensics is an activity of searching for data related to crime in a computer network environment [25] [26]. Considering traffic comes from several sources, it is challenging to identify and protect [27].

Cloud forensics is a branch of forensic science, and cloud forensics has a unique challenge where the digital forensic investigation process is usually carried out offline where the evidence collected has a form and can be held by investigators for analysis. The situation is different from cloud computing which does not have a physical form, directly, so in handling cases related to criminal activities that occur in cloud computing, special steps are needed [28].

DOS (Denial of Service) is an attack that is specifically an attempt by the attacker to prevent legitimate users from using network services. Denial of Service attacks primarily aims to disable a computer or network. DoS assaults have recently attacked well-known cloud-based organizations including RackSpace, Amazon EC2, Microsoft, and Sony [29]. There are several motives of attackers in carrying out Denial of Service, namely: sub-cultural status, to gain access, revenge, political reasons, and economic reasons [30] DoS aims to block genuine users from accessing servers. This can significantly affect any online activity and have an adverse long-term effect. Targeted attack networks have a far bigger number of devices [31]. In a cloud system, there are several DoS attack versions with varying objectives, requirements of the task, and scales [32].DOS assaults might raise application demand, necessitating the addition of more compute power to the additional capacity [33].

Thousands of packets are transmitted to one target in a DOS assault to slow down all of its services from numerous computers attacking it at the same time [34]. However, it is possible to lessen the vulnerabilities and anomalies of a computer by keeping all the software and regulations [35].

In addition to that a DoS protection system based on fog has been presented by [8]. The purpose of an attack like this results in the Private Cloud Computing server being overwhelmed with serving requests sent and ending up stopping an activity or stopping itself because it is unable to serve requests. Sometimes an attack carried out in this way can damage or shut down the system as a whole. The system under attack can become malfunctions (hang, crash), malfunction, or decrease in performance so that it can't work or run as it should. Several types of DOS attacks (Denial of Service) Ping of Death, SYN Attack, Land Target, Smurf Intrusion, and UDP (User Datagram Protocol) Flood are a few examples of attacks. Despite the fact that centralized control is the main benefit of SDN, a Denial of Service DoS assault can still lead it to fail [8].

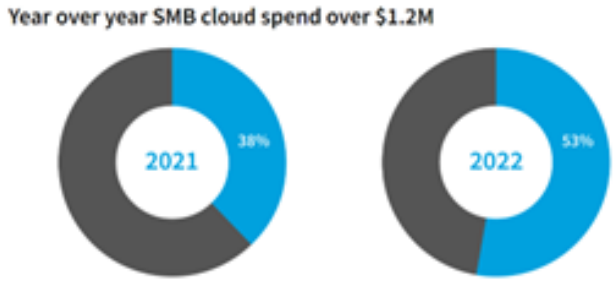
For the purpose of DDOS attack detection, [1], [36] designed and implemented the ensemble technique. Naive Bayes, decision trees, SVMs, and K-NN were utilized as basis models in the ensemble, which relies on popular vote.

Depending on the specific the analysis of attack traffic, research provided by [37] utilized the K-nearest neighbor (K-NN) method to identify DDOS assaults. This method's drawback is that it operates in offline mode and has a high falsepositive rate. According to a research by [38], DOS assaults may be detected using a method based on the C4.5 algorithm, which creates decision trees.

III. METHODOLOGY

According to Flexera's 2022 State of the Cloud Report, SMB cloud spending climbed significantly from 38% in 2021 to 53% in 2022, totaling up to $1.2 million yearly.

The yearly State of the Cloud Survey was done by Flexera in January 2019. The poll inquired about the adoption of



cloud services among technical professionals from a wide range of enterprises. The 786 responses (Enterprises = 456 and SMB = 330) represent enterprises of various sizes across several industries and range from technical executives to managers and practitioners. Respondents are enterprises from a variety of industries, and they include both users (21%) and non-users (79%) of Flexera's RightScale Cloud Management System.

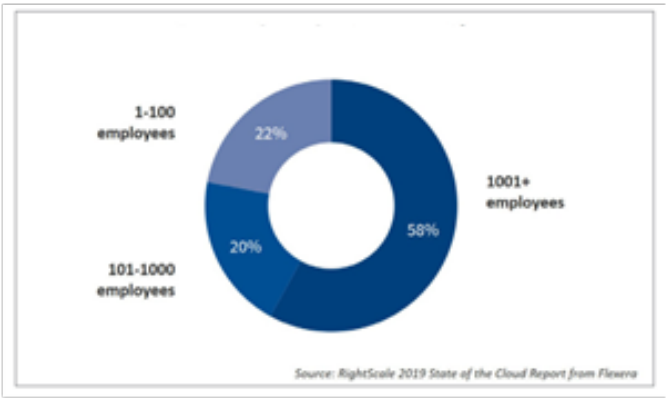


FIGURE 1: Respondent Demographics by Company Size [7]

The investigation used in this study refers to the stages of the forensic process model (Figure 1,2,3,4.), this method is carried out by analyzing all the evidence found, but for this research, the evidence to be analyzed is only on the Private

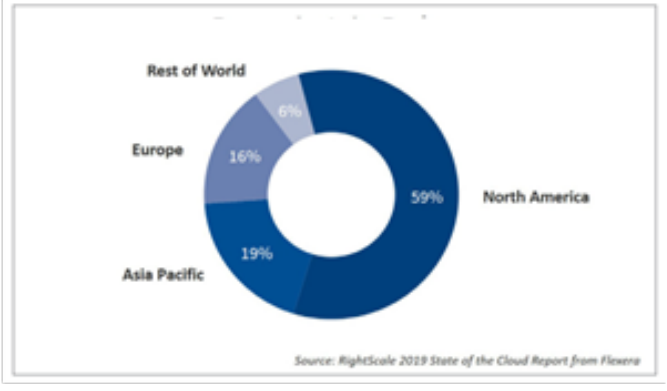


FIGURE 2: Respondent Demographics by Region [7]

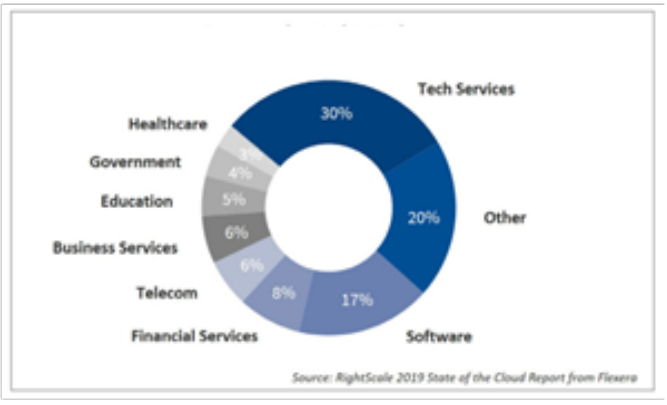


FIGURE 3: Respondent Demographics by Industry [7]

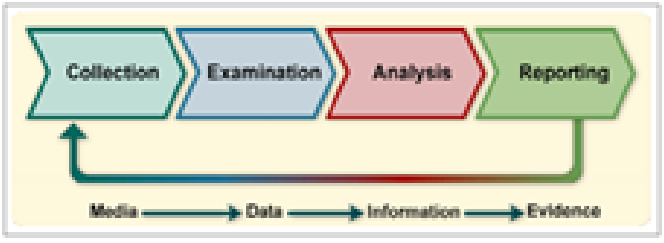


FIGURE 4: 4-Phase Forensic Process Model [39]

Cloud Computing server. The stages of this methodology include:

1) Data Collection (Collection) stage, namely collecting evidence at the crime scene such as:
   - IP Address
   - Operating system used by the attacker
   - Data packets sent
   - The time used in carrying out attacks that have been connected to the Private Cloud Computing service so that it can be known.
2) Examination Stage The Inspection stage is to check the system on the Private Cloud Computing service.
3) Stage of Analysis (Analysis) The analysis stage carried out is to examine the attempted DOS attack (Denial Of Service) to check the digital files or data related to the attack experiment, such as checking the IP address, sending data packets and time.
4) Reporting Stage The report stage, after obtaining digital evidence from the above examination and analysis process in accordance with the investigation, then the data regarding the digital evidence is entered into a technical report which will later strengthen the case being researched or investigated.

IV. RESULTS AND DISCUSSION

Based on the case scenario, the steps carried out in this research are analyzing the Private Cloud Computing server. Data Collection Phase (Collection), this data collection stage collects digital evidence related to crime data.

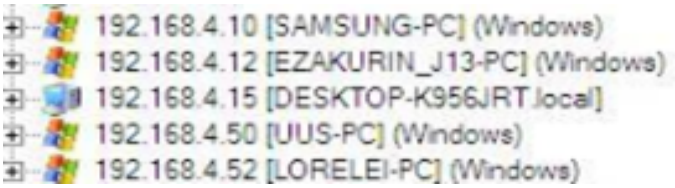


FIGURE 5: Display of a network miner running on a Private Cloud Computing server

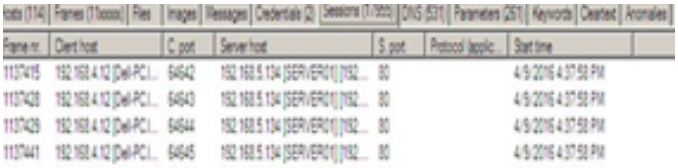


FIGURE 6: Session menu display on network miners

Referring to Figure 5. is the result of the scanning process carried out on the server using the Network Miner Tools to find out every activity that is running. The results of the scan get several IP addresses, the operating system used, the name of the PC.

Referring to Figure 6., it can be seen that there is an ongoing activity; it is recorded that the IP Address 192.168.4.52 with the name LORELEI-PC is recorded to be sending so many data packets that it continues to run. This raises the suspicion that a DOS (Denial Of Service) attack is taking place. Later it will have an impact on the server, which will be down or not functioning properly. Stage of Examination (Examination), the data examined is digital data related to the experimental data of DOS (Denial Of Service) attacks.

Referring to Figure 7, which shows that there has been a DOS (Denial Of Service) attack on the private cloud computing server, the network miner noted that 16,167 data packets had been sent continuously, so the impact of the attack ran out of bandwidth and made malfunctions or stopped the system. so it can not provide the service as it should.

Figure 8, shows that there has been an attack activity leading to the private cloud computing server service. It can be seen by the upstream and downstream activities recorded by the traffic cour router. This results in a decrease in internet access. Stage of analysis (Analysis), the analysis process is carried out on the digital evidence that has been obtained in

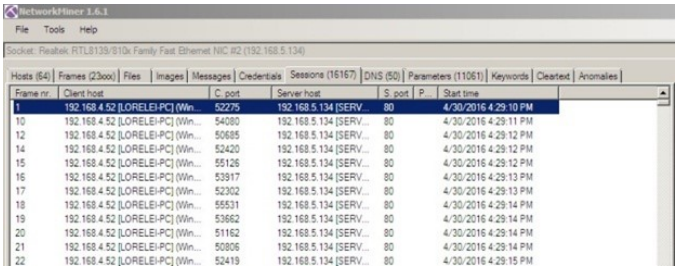


FIGURE 7: Session menu display on network miners

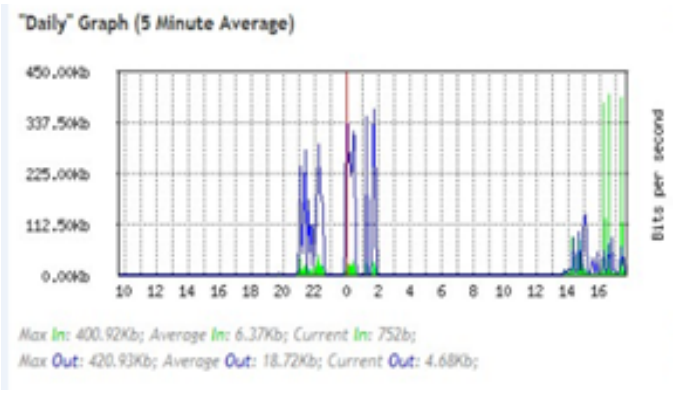


FIGURE 8: Traffic on the core router

FIGURE 9: Hosts attack

order to support the investigation to obtain 4W1H data (Who, When, Where, Why, and How).

Who

Referring to Figure 9, the results obtained IP Address 192.168.4.52 with the name LORELEI-PC and using the Windows operating system, it was recorded that sending data packets of 20,861 packets (2,267,618 Bytes) continued to run.

When

Referring to Figure 10. shows the time of the DOS attack (Denial Of Service). The attack took place on 04/30/2016 at 04:29:10 PM.

Where (Where)

The attacker launches a DOS (Denial Of Service) attack by using an open port on the Private Cloud Computing server as happened port 80 is used to send data packets.

Reporting stage (Reporting)

Digital evidence obtained in the data collection process,

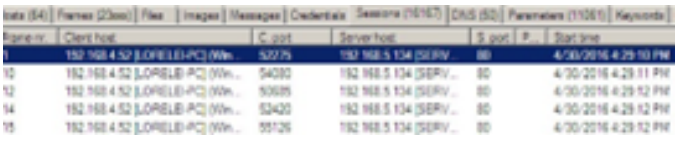


FIGURE 10: explains when it happened.

examination, and analysis process obtained data that was in accordance with the needs of the investigation, then the data regarding the digital evidence was entered into a technical report.

V. CONCLUSION AND SUGGESTION

Based on the results of research and testing that has been carried out using the Forensic Process Model Method, the following conclusions can be drawn:Identification of the occurrence of a DOS (Denial Of Service) attack is a spike in traffic so that with a spike in traffic, the usability or availability of the network service that leads to the Private Cloud Computing service is disrupted.The surge in traffic was caused by IP Address 192.168.4.52 sending data packets outside the norm, sending data packets by normal clients was usually below 400 packets, seeing packet delivery from IP Address 192.168.4.52 data packets received amounted to 12,860 packets. This can be identified as a DOS (Denial Of Service) attack.The quality of internet access to the Private Cloud Computing Service becomes slow or does not function properly when a DOS (Denial Of Service) attack occurs. The device's Private Cloud Computing Service becomes malfunctions.The results of this study found that the IP Address 192.168.4.52 using the Windows operating system at 04:29:10 PM and April 30, 2016, sent 20,861 packets (2,267,816 Bytes) of data packets.

This decrease in bandwidth indicates that the system still has weaknesses, for it is necessary to investigate further how to cover these weaknesses, such as adding patches that can prevent DOS (Denial Of Service) attacks. The monitoring process should not only use Network Miner as a tool to detect intruders so that every activity in Private Cloud Computing can be monitored, thereby reducing the risk of attacker attacks.

REFERENCES

[1] A. A. Alqarni, "Majority vote-based ensemble approach for distributed denial of service attack detection in cloud computing," Journal of Cyber Security and Mobility, pp. 265–278, 2022.

[2] R. Shakeri, M. A. Al-Garadi, A. Badawy, A. Mohamed, T. Khattab, A. K. Al-Ali, K. A. Harras, and M. Guizani, "Design challenges of multi-uav systems in cyber-physical applications: A comprehensive survey and future directions," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3340–3385, 2019.

[3] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," Future Generation Computer Systems, vol. 79, pp. 849–861, 2018.

[4] L. Alhenaki, A. Alwatban, B. Alamri, and N. Alarifi, "A survey on the security of cloud computing," in 2019 2nd international conference on computer applications & information security (ICCAIS). IEEE, 2019, pp. 1–7.

[5] M. Alfaridzi, "Ddos attacks detection in cloud computing," 2018.

[6] C. I. Machine, "Netscout threat intelligence report," in 15th Annual Worldwide Infrastructure Security Report (WISR), no. 4, 2020, pp. 1–29.

[7] R. Flexera, "State of the cloud report from flexera," 2019.

[8] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (ddos) attacks in sdn and cloud computing environments," IEEE Access, vol. 7, pp. 80 813–80 828, 2019.

[9] M. S. E. Shahabadi and et al., "A combination of clustering-based under-sampling with ensemble methods for solving imbalanced class problem in intelligent systems," Technological Forecasting and Social Change, vol. 169, p. 120796, 2021.

[10] S. R. Sahoo and et al., "Security issues and challenges in online social networks (osns) based on user perspective," Computer and cyber security, pp. 591–606, 2018.

[11] B. B. Gupta, Modern Principles, Practices, and Algorithms for Cloud Security. IGI Global, 2019.

[12] P. Suryateja, "Threats and vulnerabilities of cloud computing: a review," International Journal of Computer Sciences and Engineering, vol. 6, no. 3, pp. 297–302, 2018.

[13] M. N. Salimath and J. Sheetlani, "The vulnerabilities of cloud computing: Security threats."

[14] R. Jiao and et al., "Adaptive feature selection and construction for day-ahead load forecasting use deep learning method," IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4019–4029, 2021.

[15] S. Larson, "The basics of digital forensics: The primer for getting started in digital forensics." J. Digit. Forensics Secur. Law, vol. 9, no. 1, pp. 83–85, 2014.

[16] B. B. Gupta, A. Gaurav, and D. Peraković, "A big data and deep learning based approach for ddos detection in cloud computing environment," in 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE). IEEE, 2021, pp. 287–290.

[17] K. Memon, S. Khuhro, N. Pirzada, M. Panhwar, M. Mohd, K. Soothar, and N. Ain, "Analyzing distributed denial of service attacks in cloud computing towards the pakistan information technol-ogy industry," Indian Journal of Science and Technology, vol. 13, no. 29, pp. 2062–2072, 2020.

[18] M. Hammad and et al., "Deep learning models for arrhythmia detection in iot healthcare applications," Computers and Electrical Engineering, vol. 100, p. 108011, 2022.

[19] Z. Chen, J. Wang, Y. Yang, G. Yang, L. Wen, and L. Chen, "Research on key technology of enterprise private cloud anti-leakage," in 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS). IEEE, 2019, pp. 829–834.

[20] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1–35, 2014.

[21] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200–222, 2016.

[22] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[23] B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed denial of service attack in iot networks using supervised learning classifiers," Computers & Electrical Engineering, vol. 98, p. 107726, 2022.

[24] J. Wang and et al., "Pcnncec: Efficient and privacy-preserving convolutional neural network inference based on cloud-edge-client collaboration," IEEE Transactions on Network Science and Engineering, 2022.

[25] T. Wedge, "The basics of digital forensics," Computers and Security, vol. 31, no. 6, p. 800, 2012.

[26] R. Li, J. H. Fan, and X. B. Wang, "Technique of constructing cloud computing platform based on ubuntu enterprise cloud," in Advanced Materials Research, vol. 482. Trans Tech Publ, 2012, pp. 713–716.

[27] A. Bonguet and M. Bellaiche, "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing," Future Internet, vol. 9, no. 3, p. 43, 2017.

[28] G. Grispos, T. Storer, and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," International Journal of Digital Crime and Forensics (IJDCF), vol. 4, no. 2, pp. 28–48, 2012.

[29] P. Nelson, "Cybercriminals moving into cloud big time, report says," Network world, 2015.

[30] Z. Hui, "A design of distributed collaborative intrusion detection model," in 2011 6th International Conference on Computer Science & Education (ICCSE). IEEE, 2011, pp. 99–101.

[31] S. Dong, K. Abbas, and R. Jain, "A survey on distributed denial of service (ddos) attacks in sdn and cloud computing environments," IEEE Access, vol. 7, pp. 80 813–80 828, 2019.

[32] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, and R. Buyya, "Combating ddos attacks in the cloud: requirements, trends, and future directions," IEEE Cloud Computing, vol. 4, no. 1, pp. 22–32, 2017.

[33] N. Z. Bawany, J. A. Shamsi, and K. Salah, "Ddos attack detection and mitigation using sdn: methods, practices, and solutions," Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441, 2017.

[34] A. K. Soliman, C. Salama, and H. K. Mohamed, "Detecting dns reflection amplification ddos attack originating from the cloud," in 2018 13th International Conference on Computer Engineering and Systems (ICCES). IEEE, 2018, pp. 145–150.

[35] A. Amjad, T. Alyas, U. Farooq, and M. A. Tariq, "Detection and mitigation of ddos attack in cloud computing using machine learning algorithm," EAI Endorsed Transactions on Scalable Information Systems, vol. 6, no. 23, pp. e7–e7, 2019.

[36] B. B. Gupta, P. Agrawal, A. Mishra, and M. Pattanshetti, "On estimating strength of a ddos attack using polynomial regression model," in International Conference on Advances in Computing and Communications. Springer, 2011, pp. 244–249.

[37] F. Xiao, J. Ma, X. Huang, and R. Wang, "Ddos attack detection based on knn in software defined networks," Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), vol. 35, no. 1, pp. 84–8, 2015.

[38] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "Ddos attack detection using machine learning techniques in cloud computing environments," in 2017 3rd international conference of cloud computing technologies and applications (CloudTech). IEEE, 2017, pp. 1–7.

[39] F. Marturana, "Device classification in digital forensics triage," in Faculty of Science Department of Mathematical Sciences, University of Stellenbosch, IEEE International Conference on Communications Workshops (ICC), 2014, pp. 676–681.