International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.32, August 2020 – www.ijais.org

Mitigating DDoS Attacks in Cloud Network using Fog and SDN: A Conceptual Security Framework

K.A. Sadiq
Dept. of Computer Science
Kwara State Polytechnic, Ilorin, Nigeria

A.F. Thompson
Cyber Security Science Dept.
Federal University of Technology, Akure, Nigeria

O.A. Ayeni
Cyber Security Science Dept.
Federal University of Technology, Akure, Nigeria

ABSTRACT
In recent years, Cloud computing has changed the entire Information Technology (IT) domain due to bi-overlay focus points as against the traditional computer networks, i.e., capital expenditure (CapEx) and operational (OpEx) reduction. Both Cloud users'(CS) data and business reasons are stored in remote data centers and accessed through the network, typically the internet. The geographic distribution of Cloud data centers poses a risk to Cloud security. Consequently, a Distributed Denial of Service (DDoS) attacks remains the most prominent threats to Cloud data availability, confidentiality, and integrity. This paper explores Fog computing and Software-defined Networking (SDN) to mitigate Cloud networks against DDoS attacks. Fog computing center intermediate node between the CS and the data center, "Fog computing is proposed as an additional firewall to complement the security of the Cloud networks due to its closeness to the ground, and internet of things IoT devices and also ensures better security, Quality of Service (QoS), low latency, real-time data process, location awareness, and mobility support." Additionally, SDN that decouples the data plan (hardware) from the control plan (software) is employed to provide a global view of the Cloud network, and better management of the entire security architecture. The research presents DDoS security challenges and conceptual description of mitigating it with Fog computing and SDN.

Keywords
Cloud Computing, Fog computing, Software-defined network SDN, DDoS

1. INTRODUCTION
Cloud computing provides organizations with benefits by reducing CapEx and OpEx to a reasonable level [1]. Unfortunately, as the Cloud adoption rate increases, the Cloud becomes a point of attraction for cyber-criminals [1][2]. Among all the cyber-attacks recently, DDoS poses a concern for both industries and academia. The DDoS attacks prevent legitimate CS from accessing the Cloud resources by over-flooding the server with illegal requests thereby, making Cloud resources unavailable. A DDoS also takes advantage of CU software vulnerabilities to install malicious software called malware that makes the victims captive and act like "Zombie" to perform illicit acts [2]. The attacking nature of DDoS is not static, up-to-date approaches to mitigate its effects becomes necessary. New technological paradigms such as Fog computing and SDN are proposed by researchers to strengthen Cloud infrastructure [3]. Fog computing center intermediary node between the Cloud data-centers and the CS helps solve security challenges by serving as an additional firewall to the data centers, thereby filtering all ingress and egress packets in real-time and block the compromised packets close to its source [3]. The Fog computing also enhances the latency challenge encountered in Cloud networks, by bringing minimal computational procedure, and data storage close to the edge node where the data was created or needed [5]. Additionally, SDN that decouples the data plan (hardware) from the control plan (software) is employed to provide a global view of the Cloud network, and better management of the entire security architecture. [4][6][8][12]. As stated in [13], the SDN programmability nature is a feature this research uses to develop appropriate packet classifier and packet flow decisions to enhance data availability, integrity, and confidentiality in Cloud infrastructure. This paper's main contribution is to provide a conceptual framework of how these two paradigms improve security in Cloud networks. The rest of this paper is as follows: Section 2 introduces the benefits, challenges of Cloud computing, Section 3 gives an overview of DDoS attacks, Section 4 presents Fog and SDN roles in Cloud network, Section 5 views an account of related past works, Section 6 presents the motivation and research method and Section 7, 8, and 9 presents the result, conclusion, and references respectively.

2. CLOUD COMPUTING BENEFITS AND CHALLENGES
The deployment of different Cloud service models reduces the cost of doing business. The Cloud service models available to CS are Infrastructure-as-a-service (IaaS) which makes, CS outsource IT hardware and reduces the CapEx and OpEx on the part of CS. Software-as-a-service (SaaS) makes CS use software applications over the Internet via subscription or free of charge for limited access. Lastly, Platform-as-a-service (PaaS) makes software developers and vendors develop and host their applications with ease. Cloud computing distinguish from the traditional client/server network with the below five distinct characteristics:

1. ***Broad Network Access***: CS can access the Cloud network from multiple locations simultaneously, e.g., home and office using various types of customer devices, such as phones, personal computers, tablets, smart televisions, etc.

2. ***Rapid Elasticity*****:** CS can adjust workload variations by automatically upscale and downscale services without CS awareness.

3. ***Resource Pooling*****:** Multiple CS through a multi-tenant model can use the same physical infrastructure and maintain a high security and hardware utilization level.

4. ***On-demand self-service*****:** CS can perform all the actions needed to set up a Cloud service on their own, e.g., going through an IT department. The CS request is then handled

automatically without human involvement on the part of the service providers.

5. ***Pay-as-you-use*****:** Cloud networks, unlike traditional Client / Server networks, use Cloud application software that measures and charges each CS based on the service's use.

With all advantages, cloud computing faces numerous challenges in terms of security, high latency, stringent service level agreements (SLA), support for mobility and real-time application, and a single point of failure. Security issues such as Denial of Service (DoS) and (DDoS) pose threats to Cloud data availability, integrity, and confidentiality. The single point of Cloud network failure that exists between the CS and data center architecture layout also stands to benefit cyber-criminals from making Cloud service unavailable and unreliable [13].

3. DDoS ATTACKS IN CLOUD NETWORK

The DDoS attacks prevent legitimate CS from accessing the Cloud resources by over-flooding the server with illegal requests thereby, making Cloud resources unavailable. A DDoS also takes advantage of CU software vulnerabilities to install its malicious software called malware that makes the victims captive and act like "Zombie" to perform illicit acts [2]. The attackers are usually motivated by different forms of incentives, i.e., revenge, ideological belief, financial, and economic gains, cyber-warfare, and intellectual contest [14]. DDoS attackers mostly target either the Network/Transport layer or the Application layer. The Network/Transport layer launch attacks use the Transmission Control Protocol TCP, User Datagram Packets UDP, Internet Control Message Protocol ICMP, and Domain Name Service DNS to perform IP spoof [14]. The attacks category includes flooding attacks, protocol exploitation, reflection-based attacks, and amplification-based attacks [14] [15]. The Application-level flooding attacks target specific characteristics of applications such as hypertext transfer protocol HTTP and session initiation protocol SIP [14]. Detecting DDoS attacks is difficult because attackers mostly use spoofed (fake) IP addresses to send packets and make it difficult to detect or trace-back [15]. The DDoS attacks are capable of rendering the Cloud services unavailable or degrade its performance due to spike packet requests. Different methods like intrusion detection, anomaly detection using numerous machine learning algorithms have been proposed in the past [2]. Most techniques bring an additional computational burden to the Cloud server, making it unable to process large requests in real-time [22]. Also, the lack of up-to-date dataset made it difficult for these methods to mitigate recent DDoS attacks since the attacking nature is not static [15]. Fog computing is a promising technique to mitigate such attack since the packets need to pass through the Fog server before it gets to the data-centers, the Fog server stands as an additional firewall to filter these illicit packets requests. Figure 1 below shows a DDoS attack scenario, where legitimate CUs are controlled by an attacker to send unsolicited packets to the server.

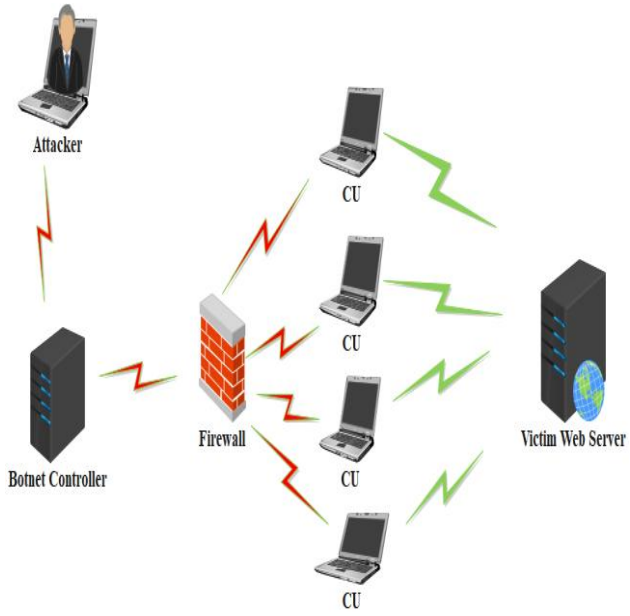

Fig 1: DDoS Attack Scenario

4. FOG COMPUTING AND SDN ROLES IN CLOUD NETWORKS

To address the challenges of Cloud network CISCO introduces Fog computing in 2012 [25]. Fog computing center intermediate node between the CS and the data centers, therefore some little computation, storage, processing, et.c can be done within the Fog server otherwise, are forwarded to the Cloud data centers [25]. Fog computing is not a replacement for Cloud computing, rather complements the Cloud services. Figure 2 shows the Cloud and Fog architecture. Fog

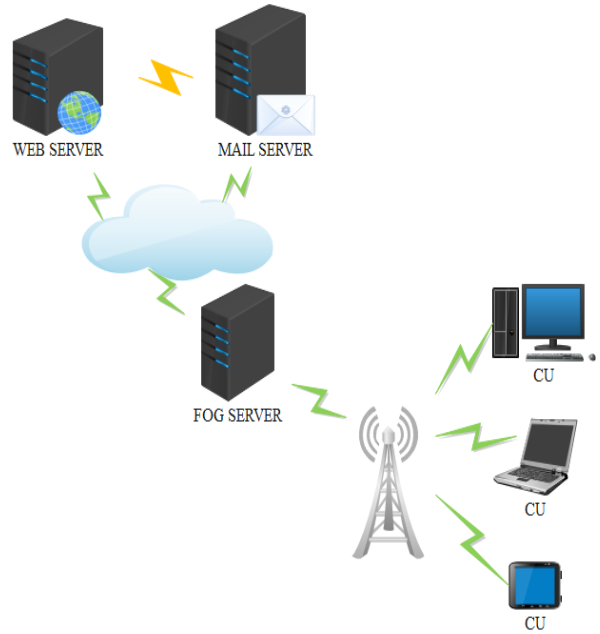

Fig 2: Cloud and Fog Computing Architecture

computing faces security challenges due it mobility supports and less computational ability with thousands of IoT devices characterized by power challenge and less security to connect to the Fog server [13]. The Fog server ensures a better security feature by detecting and blocking DDoS close to the

attack source. Additionally, to provide better security monitoring and global knowledge of the entire network, SDN is introduced. SDN decouples the data plane (hardware) from the control plane (software) thereby, increasing the network management. SDN networks have capabilities such as centralized control, flow abstraction, dynamic updating of forwarding rules, and software-based traffic analysis [26].

5. RELATED WORK

Research in [8] shows that every time a new packet arrives at the SDN OpenFlow switch, the destination packet header in the flow table is checked before actions are taken. If a match is found, the packet will be forwarded to its destination following the instructions in the flow table; otherwise, it will be sent to the SDN controller for further decision-making, i.e., accept or discard the packet. The work proposes a flow collector as a new module within the SDN controller. The flow collector is responsible for applying statistical methods to evaluate the unidentified packet, i.e., normal or malicious. Some performance matrices, such as detection rate management, false alarm, are considered to validate the system. [9] explores the collaborative approach of attack detection and containment unique to SDN. The researchers proposed a system of sensory monitors distributed over a network and an attack correlation with the Open Virtual Switch (OVS) SDN controllers. The monitor is sensitive and lightweight with the ability to detect network traffic anomalies rapidly. To comply or reject the suspicion, an attack correlator alerted by the monitor collects more evidence with a controller's aid to verify the attack signature. The controller coordinates further measures to update the normal traffic profile to prevent future false alerts or to mitigate the effects of an attack. Global Environment for Network Innovation (GENI) has been tested. [10] explains how Cloud computing properties help DDoS attacks expand, some features of SDN, and the challenges it faces in mitigating DDoS attacks. The problems listed include a single failure point, unauthorized access, malicious applications, etc. The researchers proposed solutions available such as TLS, FortNox, and AVANT-GUARD transport layer security. Future research directions such as the prevention of DDoS are recommended on mobile networks, DDoS fault-tolerant, and multiple location defense method. [2] noted that the significant attribute of a DDoS attack is spoofing the IP address that hides the attackers' identity and IP spoofing frustrate packet traceback of the attack. The work proposes fingerprinting a host-based operating system (OS), which uses passive and active approach methods to compare the incoming packet operating system from its database. The passive monitoring collects and analyzes the incoming packet's TCP / IP header functions using the P0f tool. The OS's fingerprinting is accomplished by comparing the analyzed header information with the known OS database of P0f to determine its actual OS. Using Nmap device, specially designed probe packet is sent to the received packet's IP source in an active state. If the spoofed IP address is active, it will return a response that Nmap captures from its database and uses it to identify its OS. Comparison is made of the observed OS during both passive and active probes; if a match exists, it means the packet is legitimate; otherwise, it is spoofed. [23] proposes a lightweight scheme, based on rules to efficiently identify packets sent as legitimate, or malicious, to a network switch. All incoming OpenFlow switch port packets are inserted in the flow buffer that initiates the flow table search to find a rule that fits the packet message area, e.g.iP / TCP header, UDP, etc. If the match occurs, it will only pass the packet to its desired destination; otherwise, it will send a *packet_in* message to the OpenFlow controller requesting the switch to provide associated data and check if the system is under DDoS attacks by setting the *hard_timeou*t and idl*e_timeout* to 60 and 10 seconds respectively. The controller maintains records of incoming packets, numbers of packets per flow, the size of packets per flow, and each entry in the flow table, all of which are used to measure the average packet threshold. If the packets are not equal to the average threshold, then the network is deemed under DDoS attack, the *hard_timeou*t and idl*e_timeout* to 60 and 10 seconds are implemented. When the flow is higher or equal to the packet threshold, the network is deemed normal, and the *hard_timeou*t and idl*e_timeout* parameter of 600 and 100 are specified. If the legitimate packet request is high, the False alarm rate can trigger. [11] proposes a Secure Controller SeCo algorithm to mitigate the DoS attack in the SDN controller. Four functions are used in the algorithm. First, threshold counters to differentiate between regular and DoS packets. Second, multiple counter functions help monitor each part of the data plane so that the packet sent to the controller is known. Third, the DoS function module helps detect and locate when an attack is initiated to stop the controller from processing fake packets. Finally, the DoS Defense function instructs the data plane to drop packets from the affected port or disconnect the controller's connection and the data plane. The simulation was performed with Mininet, POX tools, and performance comparison was carried out with and without the SeCo algorithm. SeCo uses 57%, while without SeCo uses 90% of CPU resources.

6. RESEARCH MOTIVATION AND METHOD

This study aims to analyze how SDNs is used in the Fog network to ensure security, flexibility, and centralized network management. Because of the decoupling nature of SDN or the separation of software (control plane) and hardware layers (data plane), much of network management is achievable. The challenge is to justify how SDN-administered Fog network deployment is more inclined towards security against DDoS attacks than conventional Cloud network deployment. Providing mitigation against DDoS attacks comes with enormous technical challenges, which includes;

1. Identification is difficult because the attack imitates a legitimate packet or use the Botnet controller to instruct the "Zombies" CU.
2. The potential for packet misclassification is high, and DDoS packets classified as a legitimate packet will lead to False Positives. Also, packets maybe are classified as DDoS, which may lead to False Negatives.
3. DDoS also uses tactics of IP spoof to initiate their attacks, thereby making it very difficult to trace-back attacks.

Providing adequate measures to address these challenges while ensuring data availability, integrity, and confidentiality requires thorough research in this area.

7. PROPOSED METHOD

The research seeks to achieve service availability in the Cloud network using Fog computing and SDN. The following are the three steps needed for better security of Cloud Network

Step 1: The research analyzes each packet received in the Fog computing network via its TCP / IP header to detect

IP spoof.

Step 2: It uses a classifier to distinguishes between normal and malicious packets while ensuring high accuracy and less computational complexity.

Step 3: Insert the design in 2 into the flow control rules and mechanisms to absorb or discard normal and malicious packets before they overwhelm the computing power of the SDN controller.

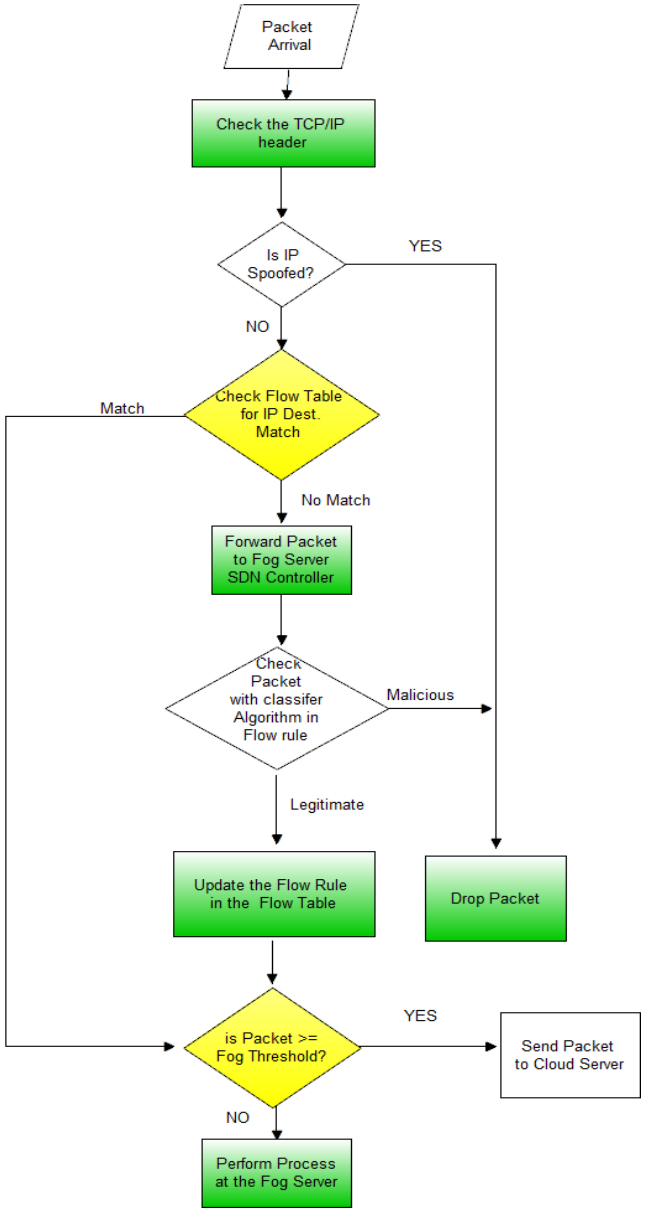

Fig 3: Fog and SDN Security Workflow

8. RESULT

When the packet arrives at the data plane (i.e., from CU 1, CU 2, or CU 3), it checks the window size and time to live TTL for any anomalies. If the arrived packet's destination address is available in the Data plane flow table (I.e., CU 2 to CU 3), the packet will be forwarded to the appropriate destination; otherwise, it will be sent to SDN Controller inside the Fog server. The SDN controller, through its DDoS classifier algorithm, checks the packet received and performs the filtering process. If it's legitimate, the flow rule in the data plane will be updated to accommodate the packet and send it to the appropriate destination; otherwise, it is dropped. All legitimate packets are checked and must be less than the Fog server threshold before it can be processed; this is to ensure QoS; otherwise, the packet is sent to the Cloud server. Figure 4 shows the architectural workflow of Fog and SDN managed Cloud network.

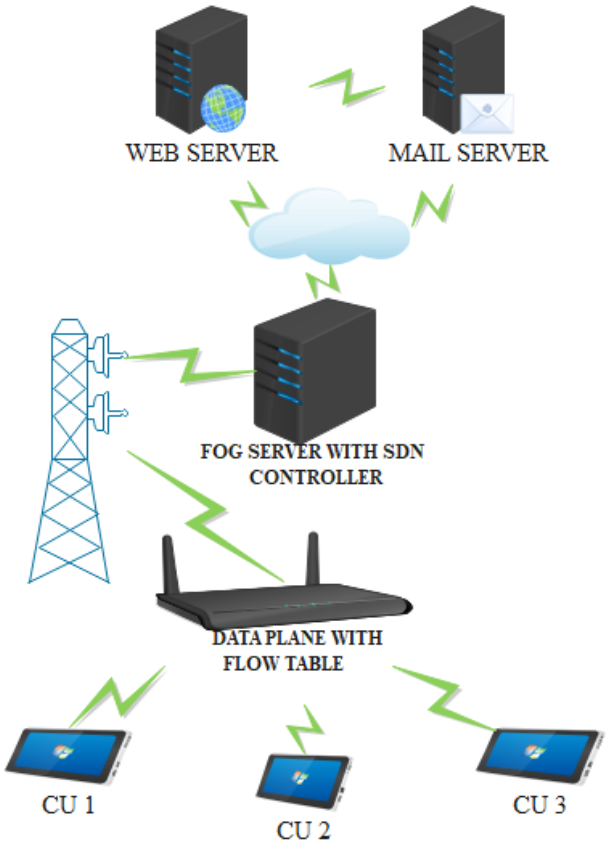

Figure 4: Architectural Layout Fog and SDN Security Framework

9. CONCLUSION

The security issue of the Cloud is the main focus of this work. DDoS is considered as the most prominent security threat to Cloud data availability, integrity, and confidentiality. This paper combines Fog computing and SDN as a single mitigation technique to achieve better results. It also considers IP spoof as a great technique to carry out DDoS. The IP spoof detection is carried out near the source of the attacker in this research, this will boost attack trace-back.

10. REFERENCES

[1] Chandrasekaran, K., 2015. Essentials Of Cloud Computing. London: Chapman & Hall, pp.14-17

[2] Osanaiye, O. A. (2015). Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. 2015 18th International Conference on Intelligence in Next Generation Networks, 139–141. https://doi.org/10.1109/icin.2015.7073820

[3] Buyya, R., & Srirama, S. N. (2019). Fog and Edge Computing: Principles and Paradigms (Wiley Series on Parallel and Distributed Computing) (1st ed.). Newyork, United States of America: Wiley.

[4] Osanaiye, O., Choo, K.-K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in Cloud: Review and conceptual Cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, *67*, 147–165. https://doi.org/10.1016/j.jnca.2016.01.001

[5] Zhou, L., Guo, H., & Deng, G. (2019). A fog computing based approach to DDoS mitigation in IIoT systems. *Computers & Security*, *85*, 51–62. https://doi.org/10.1016/j.cose.2019.04.017

[6] Ahmed, M. E., & Kim, H. (2017). DDoS Attack Mitigation in Internet of Things Using Software Defined Networking. 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), 271–276. https://doi.org/10.1109/bigdataservice.2017.41 admin. (2017, December 25). Fog Computing and Internet of Things. Retrieved from http://www.techplayon.com/fog-computing-and-internet-of-things/

[7] Morgan, H. (2016, December 21). Census outage marked boom year for global DDoS attacks.Retrieved from https://www.csoonline.com/article/3152724/census-outage.html

[8] Dharma, N. I. G., Muthohar, M. F., Prayuda, J. D. A., Priagung, K., & Choi, D. (2015). Time-based DDoS detection and mitigation for SDN controller. 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 550–553. https://doi.org/10.1109/apnoms.2015.7275389

[9] Chin, T., Mountrouidou, X., Li, X., & Xiong, K. (2015). An SDN-supported collaborative approach for DDoS flooding detection and containment. MILCOM 2015 - 2015 IEEE Military Communications Conference, 1–6. https://doi.org/10.1109/milcom.2015.7357519

[10] Yan, Q., & Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with Cloud computing. IEEE Communications Magazine, 53(4), 52–59. https://doi.org/10.1109/mcom.2015.7081075

[11] Wang, S., Chavez, K. G., & Kandeepan, S. (2017). SECO: SDN sEcure COntroller algorithm for detecting and defending denial of service attacks. 2017 5th International Conference on Information and Communication Technology (ICoIC7), 1–6. https://doi.org/10.1109/icoict.2017.8074692

[12] Khakimov, A., Ateya, A. A., Muthanna, A., Gudkova, I., Markova, E., & Koucheryavy, A. (2018). IoT-fog based system structure with SDN enabled. Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS '18, 1–6. https://doi.org/10.1145/3231053.3231129

[13] Javaid, U., Siang, A. K., Aman, M. N., & Sikdar, B. (2018). Mitigating loT Device based DDoS Attacks using Blockchain. Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock'18, 71–76. https://doi.org/10.1145/3211933.3211946

[14] Bhushan, K., & Gupta, B. B. (2018). Detecting DDoS Attack using Software Defined Network (SDN) in Cloud Computing Environment. 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN), 872–877. https://doi.org/10.1109/spin.2018.8474062

[15] Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. *Future Generation Computer Systems*, *88*, 16–27. https://doi.org/10.1016/j.future.2018.05.008

[16] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156

[17] Latah, M., & Toker, L. (2018). A novel intelligent approach for detecting DoS flooding attacks in software-defined networks. International Journal of Advances in Intelligent Informatics, 4(1), 11–20. https://doi.org/10.26555/ijain.v4i1.138

[18] Wani, A., & Revathi, S. (2020). DDoS Detection and Alleviation in IoT using SDN (SDIoT-DDoS-DA). Journal of The Institution of Engineers (India): Series B, 101(2), 117–128. https://doi.org/10.1007/s40031-020-00442-z

[19] Yu, J., Kim, E., Kim, H., & Huh, J. H. (2020). Design of a Framework to Detect Device Spoofing Attacks Using Network Characteristics. IEEE Consumer Electronics Magazine, 9(2), 34–40. https://doi.org/10.1109/mce.2019.2953737

[20] Singh, R., Tanwar, S., & Sharma, T. P. (2019). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy, 3(3), 1–13. https://doi.org/10.1002/spy2.96

[21] Singh, R., Tanwar, S., & Sharma, T. P. (2019). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy, 3(3), 1–13. https://doi.org/10.1002/spy2.96

[22] Priyadarshini, R., Kumar Barik, R., & Dubey, H. (2020). Fog-SDN: A light mitigation scheme for DDoS attack in fog computing framework. International Journal of Communication Systems, 33(9), 1–13. https://doi.org/10.1002/dac.4389

[23] Gkountis, C., Taha, M., Lloret, J., & Kambourakis, G. (2017). Lightweight algorithm for protecting SDN controller against DDoS attacks. 2017 10th IFIP Wireless and Mobile Networking Conference (WMNC), 1–6. https://doi.org/10.1109/wmnc.2017.8248858

[24] A.Ayeni, A., Faruk, N., & A. Sadiq, K. (2014). Energy-Efficient Planning Tool for WCDMA Heterogeneous Network Deployment. *International Journal of Applied Information Systems*, *6*(8), 30–36. https://doi.org/10.5120/ijais14-451101

[25] Tomovic, S., Yoshigoe, K., Maljevic, I., & Radusinovic, I. (2016). Software-Defined Fog Network Architecture for IoT. *Wireless Personal Communications*, *92*(1), 181–196. https://doi.org/10.1007/s11277-016-3845-0

[26] Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*, 1–8. https://doi.org/10.15439/2014f503

[27] admin. (2017, December 25). Fog Computing and Internet of Things. Retrieved from http://www.techplayon.com/fog-computing-and-internet-of-things/

[28] Deepali, & Bhushan, K. (2017). DDoS attack mitigation and resource provisioning in Cloud using fog computing. 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 308-313. doi:10.1109/smarttechcon.2017.8358387

[29] Yang, L., & Zhao, H. (2018). DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method. *2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN)*, 174-178. doi:10.1109/i-span.2018.00036

[30] Arif, M., Wang, G., Wang, T., & Peng, T. (2018). SDN-Based Secure VANETs Communication with Fog Computing.*Security, Privacy, and Anonymity in Computation, Communication, and Storage*, 46–59. https://doi.org/10.1007/978-3-030-05345-1_4