A New Frame work for DDoS Attack Detection and Mitigation.

DR. S. SELVAM
Department of Artificial intelligence
Nadar Mahajana Sangam S.Vellaichamy Nadar college,
Nagamalai Madurai-19, Tamilnadu INDIA

Abstract: Cloud computing seems to be further advancement among many different recent technologies that allow users to create services on-demand. Cloud computing has achieved benefits as a result of its self-service capability as well as on demand services. This offers significant adaptability to its users, as they simply pay for the services they require, rather than worrying about the expense of equipment or software support. The major benefit of utilizing the cloud based environment in organization is to enhance the data maintenance scheme in easy way as well as improve the integrity of service to avoid manual flaws over maintenance. However, the remote cloud based data maintenance and evaluation leads certain security related threats, especially with Distributed Denial of Service (DDoS) Attacks. These attacks are caused by intruders or hackers to attempt to hack the data presented into the server end or traverse between client and server end. The attacker obtains the data and modifies it according to their convenience without the knowledge of data owner. These kinds of attacks are most dangerous and the confidentiality of the data is totally disturbed due to such threats. This paper is intended to design a novel deep learning strategy called Modified Learning based Cloud Attack Detection (MLCAD), in which it adapts the features from the conventional security handling scheme called Intelligent Attack Identification Strategy (IAIS). This proposed MLCAD approach identifies the DDoS attack over cloud environment by means of analyzing the authorization and authentication logics of the respective user, examine the Internet Protocol (IP) Address mentioned in the relevant request as well as the metadata acquired from the user end. These provisions made the proposed approach MLCAD to act better to identify the DDoS attack in an efficient manner with full significance. The resulting section of this paper provides the proper graphical proofs to prove the integrity and performance of the proposed approach in clear manner.

Keywords: Cloud Computing, Deep Learning, Attack Detection, MLCAD, Intelligent Attack Identification Strategy, IAIS, DDoS, Data Security

Received: April 17, 2024. Revised: December 4, 2024. Accepted: January 11, 2025. Published: March 5, 2025.

1. Introduction

Cloud computing is a type of Internet-based computing that offers memory, networking and business applications. This has a significant influence on the business industry by equating storage systems to the Internet. Even though the approach is analogous to virtualized servers in that it enables users to share and access computational resources. Cloud computing enables use of massive cluster networks of servers, in which those are powered by low-cost client personal computer technology with specialized interconnections. In general, cloud computing involves clients or users uploading data to the cloud. This reduces hardware and maintenance costs automatically, but availability of data becomes more unsecure and susceptible in the cloud. From the user's perspective, the primary worry in a cloud computing systems is security, which must be addressed meticulously in order for consumers to securely exchange their information over the cloud. [1][2].

Distributed Denial of Service (DDoS) attacks are a common method of attack in which attackers effectively disable database access capabilities for legitimate cloud computing customers. In a Distributed Denial of Service attack, the attacker or hacker transmits superfluous erroneous information in order to gain access to the cloud server for confirmation requests including an incorrect specific address. Because the server must wait before closing the connection, the website or networking will be unable to detect the information about the identity of the intruder requesting identification permission. Once the accessible server disconnects the link, the attacker or hacker sends a large number of confirmation requests with an erroneous number of addresses. As a result, the authentication process and server wait time will resume, improving the reliability or cloud server congested. When an attacker uses a

faked IP address, a distributed denial of service attack is challenging to notice. Typically, hackers employ faked Internet Protocol addresses to ensure that the hacked system stays undetected, allowing them to exploit it for a variety of attacks. However, if the assault's source is known in advance, it is feasible to prevent and halt the attack. In this research paper, the Distributed Denial of Service threats against network-based cloud server components in a cloud assisted network environment will also be discussed.

The cloud computing server environment has different variations such as: Public Cloud Computing Services, Private Cloud Computing Services, Cloud based Community Model and Hybrid Cloud Computing Services.

(i) Public Cloud Computing Services: The cloud computing service provider serves as a capability of resources in the public cloud server environment for various organizations over the global Internet on a compensation basis, with the assurance of resources segmentation for distinct organizations [2]. The public cloud computing technology is an information technology architecture in which on-demand computational infrastructural facilities are provided by a third party service provider as well as shared among numerous businesses over the public Internet. The public cloud makes computer resources available for purchase by anybody. Typically, several users share access to a public cloud. The public cloud enables consumers to exchange resources and infrastructure while safeguarding each customer's information privacy. The public cloud server environment structure is entirely virtualized, enabling the use of pooled resources that meet. The public cloud server environment is described as online services that are made accessible via the open network by third party service providers to anybody who wishes to utilize or acquire them. That users can be provided for free of charge or on a pay-per-use basis, letting users to spend only for the Computational resources, space or frequency band they utilize.

(ii) Private Cloud Computing Services: Private cloud network is wholly owned by an organization and can be operated by that organization or by another company on-site or remotely situated. All computing resources are deployed in front of a corporate firewall. Private cloud computing is a computing architecture that provides a dedicated environment for a single corporate organization. As with other forms of cloud computing systems, private cloud computing extends virtualization enabled computational power through the use of physical components housed on-premises or at a company's datacenter.

Cloud computing is a broad phrasing that encompasses a variety of categories, kinds, and architecture models. Public cloud computing refers to cloud computing that is supplied via the internet and utilized by several businesses. Private cloud computing refers to cloud technology that is exclusively dedicated to your company. Private clouds are often more expensive than traditional clouds due to the hardware and maintenance requirements. Not only will you require hardware, but also an operating system and software programme licensing.

(iii) Cloud based Community Model: The structure of a community cloud is always owned and operated by several organizations on a basis of equality. In computing, a community based cloud model is a collaborative operation in which the technology is utilized by different companies that share reasonable issues (privacy, regulation, authority and so forth), either administered domestically or through a third party service provider and whether stored inside or outside. Community based Cloud models safeguard user information in just the same manner that other cloud services do, by duplicating it in many secure places to safeguard it from unexpected occurrences. Cloud computing utilises alternative network to ensure that the information is always accessible whenever and wherever users need to use it.

(iv) Hybrid Cloud Computing Services: A hybrid cloud is a combination of some of the above-mentioned cloud technologies. A hybrid cloud computing environment is one that combines on-premises technology, private cloud computing services and a public cloud computing services such as Amazon-Web-Services or Microsoft-Azure, with

coordination between the multiple infrastructures. Hybrid cloud computing model enables businesses to operate their most important applications on again and their lesser crucial assets on a third-party cloud computing provider in public manner. This strategy enables companies to take use of the advantages of the both private and public cloud computing architectures.

1.1 Cloud Computing Environment's Service Patterns

The following are the service patterns generally utilized over the cloud computing platforms, in which they are illustrated in detail below.

(i) Software-as-a-Service (SaaS): It provides a digital interface that allows user to share their applications remotely through the world-wide-web pathway.
(ii) Platform-as-a-Service (PaaS): It offers intellectual courses that include database, internet services, computer languages and system software.
(iii) Infrastructure-as-a-Service (IaaS): It provides a highly effective framework for physical and the virtual resource enabled services.
(iv) Network-as-a-Service (NaaS): It analyses entire network data traffic statistics for consumers in order to deliver improved network connection.

1.2 Distributed Denial of Service Attack

This exploit is used to deny legitimate users access to cloud resources. In DDOS, the attacker attempts to overwhelm the network with numerous message requests, therefore reducing the user's bandwidth. Additionally, it impairs the access services to a certain system. The accompanying figure, Fig-1, illustrates the aforementioned notion.

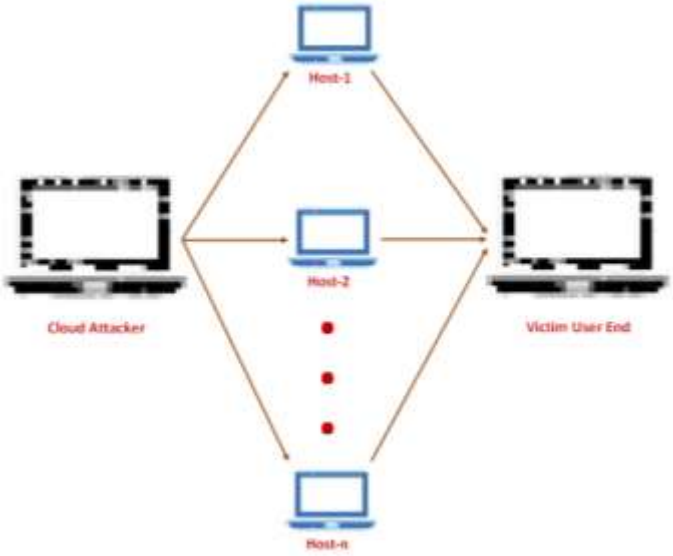

Fig.1 Portrayal of Distributed Denial-of-Service Attack

(i) Cloud Computing and Distributed Denial of Service Attacks

Cloud computing is a type of on-demand utility processing in which resources are made available on a "pay-as-you-go" basis. More precisely, a cloud service provider is a provider of infrastructure as a service (IaaS) that operates virtual computers on demand. Thus, a cloud service provider is also a cloud client if the service provider has configured the web interface as a virtual machine within the cloud infrastructure provided by the cloud provider [3]. DDOS assaults are becoming increasingly successful in recent years on cloud computing, where attackers may completely disrupt the pay-as-you-go business paradigm. By sending numerous message requests to the servers, it has a direct effect on service downtime.

1.3 DDOS Attack Methods

The following are the different types of attacks triggered over the cloud computing platform, in which these attacks are illustrated in detail below.

(i) Smurf-Attack: In the Smurf attack, the attacker broadcasts a large volume of duplicated Internet-Control-Message-

Protocol (ICMP) traffic to a large number of Internet Protocol (IP) broadcast destinations [3].

(ii) Synchronization (SYN) Flood-Attack: In this sort of attack, the server is unable to process requests due to the user to gain access queue being overloaded [3][4].

(iii) UDP Flood Attack: A User Datagram Protocol (UDP) flood attack leverages the majority of PCs on the network's UDP character generator and echo capabilities. The attacker connects the characters creation on one system to the echoing services on some other machine using User Datagram Protocol network packets.

1.4 Available Distributed Denial of Service Attack Defense Techniques

Numerous researchers have said that while there are now no safety precautions accessible to defend against DDOS attacks, there are a variety of security measures that a host or group of computers may do to strengthen the security of a system and its adjacent set of connections [5]. Several distributed defense frameworks are listed below that can assist in providing resistance against DDOS attacks:

(i) Router Filtering: When confronted with a DDOS assault, it is critical to filter all data packets leaving and entering the system in order to provide essential protection. Many people believe that routers that employ access control lists (ACLs) to filter out undesirable traffic provide an additional layer of security against distributed denial of service (DDOS) assaults [6].

(ii) Rendered immobile IP Broadcast: By immobilizing IP broadcast, source machines are rendered incapable of being utilized as amplifiers in Smurf attacks and ICMP floods. To protect against this assault, all nearby networks must disable IP broadcast.

(iii) Performing Intrusion Detection: By performing intrusion detection, the host computer and network are safeguarded from becoming both a source of attack and a victim of attack. It is a piece of software or hardware that keeps an eye on the actions of a network or system. If any anomalous behavior is identified, a report is automatically created and sent to a central controller [7].

(iv) Securing Unused Services: Securing unutilized services will also assist in defending against an assault. For instance, if a computer has 30 ports, the hacker can utilize them to spread the assault, but if only 2 or 3 terminals are accessible, the victim's attack will be limited [8].

2. Related Study

Khadijeh et al., 2019 [9] proposed a paper related to the IoT which is revolutionizing the way that we live our everyday lives by empowering the gadgets that surround us to make choices and carry out our daily duties and errands. A difficult job is to keep an IoT system secure from hacks and other malign activity. These attacks, which have caused significant security risks to all networks, even IoT devices with low resources, include DoS as well as DDoS assaults. Developing a thorough detection technique that successfully protects against DDoS assaults and can offer a 100 percent identification of DDoS attacks in IoT seems to be a key objective for the future of IoT, since security has always been a fundamental element for allowing most IoT applications The creation of such a technique requires familiarity with existing DDoS attack detection mechanisms in the Internet of Things (IoT). When it comes to detecting DDoS assaults on IoT networks, there are a number of new machine learning (ML) methods that have been created along with their benefits and drawbacks. There is also a comparison of the results of various methods.

Ui-Jun-Baek et al., 2019 [10] proposed a paper related to the crypto currency industry has expanded quickly since Satoshi-Nakamoto created Bitcoin, the very first crypto currency to use Blockchain technology. In addition to this increase in vulnerabilities and assaults, the Bitcoin ecosystem faces numerous challenges, both at the network and service levels where it is used, according to the results of the study. DDoS attacks will be examined and detected based on the assumption that network-level data for Bitcoin and DDoS assaults at the service level are linked. A correlation is found between

network-level data as well as service-level DDoS assaults on Bitcoin, as measured by the metrics provided throughout the experiment. Finally, we recommend that the suggested approach be used on other block-chains.

Shahzeb-Haider et al., 2019 [11] proposed a paper suggesting that SDNs separates the control plane from forwarding logic, many believe they represent the networking technology of the future. SDNs also meet the growing demand for networks that are both faster and more efficient. In spite of this, the development of SDNs poses new security risks to the centralized architecture, such as DDoS attacks. As a result, detecting large-scale sophisticated DDoS attacks quickly is critical for implementing effective responses. For effective DDoS detection in SDNs, this article proposes a DL-based CNN ensemble solution. With the most recent Flow-based dataset, the performance of the proposed framework is examined (ISCX 2017). As shown by the suggested framework's empirical findings, 99.48 percent of attacks may be detected in the shortest time possible while remaining computationally difficult.

Sabeel et al., 2019 [12] proposed a paper suggesting by looking for patterns in unusual network traffic, Deep Learning (DL) may help identify network assaults. An earlier study found great success using dynamic analysis to identify known profiles, or attack patterns that may be used to train DL-based algorithms. However, the effectiveness of these defenses against unknown or constantly changing assaults has not been well studied. We need to know how DL-based techniques perform in such situations and how far they may deviate from existing training models since cyber-attacks on network based resources have become more sophisticated. For binary prediction on unknown DoS as well as DDoS assaults, we compare the performance of the two widely suggested DL-based techniques: DNN and LSTM. When the models have been trained on the benchmarks CICIDS2017 dataset, a new test dataset is generated and tested on the models in a simulated environment. The TPR for DNN and LSTM increases by 99.8% as well as 99.9% after retraining its models on the dataset containing additional unknown threats, respectively.

Subham-Kumar et al., 2019 [13] proposed a paper related to one of the most damaging assaults include DoS as well as DDoS, which may knock down a few of the largest and most well known web domains and Internet infrastructures. In 2018, attacks reached a high of 1.5 Terabytes each second, rising in size each year. Command-and-Control servers of botnets employ Domain Generation Algorithms to upload malware to certain domains, which the bots then contact to receive it. As a result, it's impossible to manually identify and sink-hole domains when there are thousands of them generated using algorithms. Today's virus writers use sophisticated methods to create domain names that are strikingly similar to well-known brand names. DDoS assaults may be stopped in their tracks if these algorithms and their associated servers are identified and stopped before they can do any damage. As a result, the assault is rendered null and void. The goal of this research [13] is to use machine learning as well as deep learning methods to create effective models that can identify malware or bots.

3. Methodologies

The suggested approach called Modified Learning based Cloud Attack Detection (MLCAD) focuses on Distributed Denial-of-Service (DDoS) attacks, which are a major problem now-a-days throughout the globe. This attack damages the cloud system's services and resources extremely rapidly. A methodology for controlling DDoS attacks is provided in this study is utilizing to preserve the needs and integrity of cloud computing platform. As previously stated, this attack caused a significant slowdown in cloud services, affecting user data as a result. A denial-of-service attack slows down network traffic by flooding the server with messages. This allows the attacker to target online services or web applications more easily. We're working out how to deal with DDoS attacks and how to keep our data safe while the system seems to be under assault using our suggested paradigm. DDoS protection cloud aids in the management and prevention of DDoS attacks, ensuring that

other network services are not adversely impacted. Different methods are used by the DDoS monitoring panel to keep tabs on activities occurring in the cloud. Most important in this design is the DDoS shield protecting user data, which may be used if the DDoS monitoring panel identifies any data loss activity and this model also keeps network traffic information log data in the DDoS prevention cloud such that the attack can be easily identified if any network latency is found as well as the idea is clearly shown in the following figure, Fig-2.

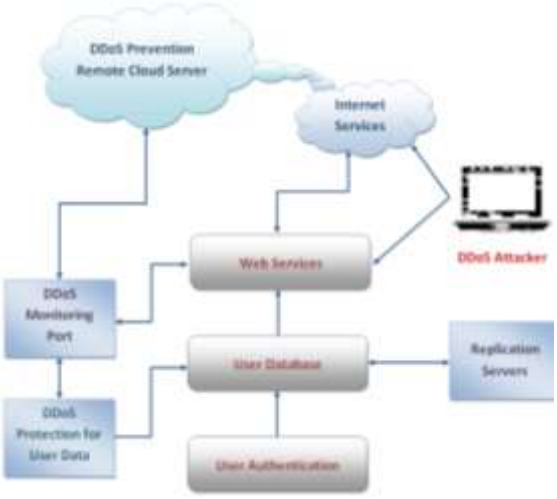

Fig.2 Model for Countering Distributed Denial-of-Service Attacks on the Cloud

3.1 Blocks of the Proposed Model with Functionalities

(i) Cloud Assisted DDoS Protection: Protecting cloud computing services against DDoS attacks are made easier using DDoS protection cloud. The data logs and network traffic generated by online services are stored in the cloud. DDoS prevention cloud immediately sends a request to the monitoring panel for the necessary action if it detects any clues such as network delay, excessive messages over cloud, ping request duration out, or a server response with a network outage, which indicate a DDoS attack.

(ii) DDoS Monitoring System: A DDoS monitoring system can detect the type of denial of service attacks that slows down a network, whether it's because of slow internet speed or because the network is overloaded with IP ping request messages, among other things. This panel enables us to keep a close eye on the assault while also taking decisive action against it. It may also be used to ban illegal IPs that cause network delay or stop idle services that might have disastrous consequences for the services. To remove the root of the problem, it provides network-wide filtering. We need NaaS to keep track of network traffic so that we may keep network traffic records. Finally, it protects user data, which is at jeopardy when a DDoS assault hits the network.

(iii) Protection against DDoS Attacks on Cloud User Data: This model's main piece is the DDoS shielding for user data, which protects that data from an assault. Because users are unable to access the data while under a DDoS assault, they are unable to log in to online services or check into the data. We also include a data replication mechanism in this shield, so that the replication servers may act as a backup for customers' data.

(iv) Internet: The control of DDoS attack requires a high-speed network since it typically targets sluggish Internet services as an easy DDoS attack target.

(v) Web enabled Services: This is the web service or web app's connection module.

(vi) User Database: Users may access their accounts and other data in the user database by logging in.

(vii) User Login: Users may login using an authenticated user id as well as password and create new accounts here, which is offered by online services or web applications.

(viii) DDoS Attacker: The DDoS attacker disables the services for the users using a variety of methods. To conduct a successful denial-of-service (DDoS) assault, the assailant targets data and critical information while also slowing down services.

(ix) Replication Servers: Replication servers are available to protect user data from DDoS attacks. For medium-sized backups, our model recommends at least three servers, although additional servers may be added if necessary. When the system is being attacked by DDoS, these servers rapidly offer a data backup.

4. Results and Discussion

This paper introduced a new deep learning model called Modified Learning based Cloud Attack Detection (MLCAD), in which it is derived from the conventional DDoS attack detection scheme called Intelligent Attack Identification Strategy (IAIS). The proposed approach MLCAD utilizes the concept of deep learning and identifies the DDoS attacks on cloud environment by cross-validating the IP address of the data packets along with user authentication credentials. The conventional Intelligent Attack Identification Strategy provides a way to identify the cloud environment based DDoS attacks based on Internet Protocol address alone, but this proposed MLCAD scheme identifies the attack based on user novelty as well as the deep learning scheme maintains the present monitored or analyzed records into the server end for further validation. The data acquired from the source or user end need to be validated according to the concern of authentication check, IP validation as well as the training model comparisons. If the received data and node crosses all these validations in proper manner, the system allows the data or user to proceed further otherwise it blocks the data to proceed further. The following are the key metrics of the proposed learning based DDoS identification scheme.

(i) This approach will assist identify distributed denial of service (DDoS) attacks more quickly.

(ii) By using this approach, it will be simple to keep track of unauthorized IP addresses.

(iii) The DDoS assault will be detected and the excessive network requests will be controlled by the DDoS monitoring panel.

(iv) This approach makes it simple to immobilize unnoticed service requests, ensuring that no user data is destroyed.

(v) Replication servers will provide users with a copy of their backup data.

The following figure, Fig-3 illustrates the perception of proposed approach data handling efficiency in order to transfer it into the server end from client end without any interference, in which it is cross-validated with the conventional DDoS attack detection scheme called IAIS and prove the proposed approach efficiency in clear manner.

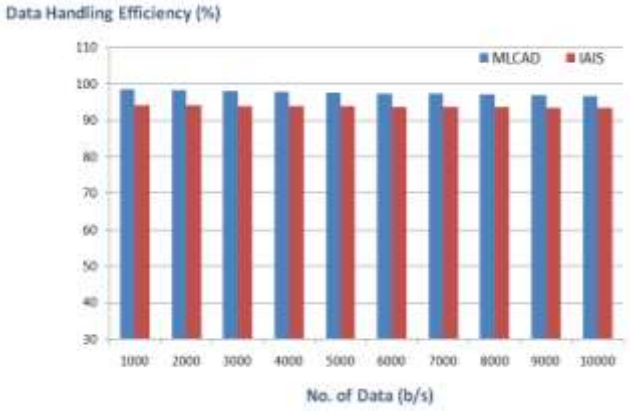

Fig.3 Data Handling Efficiency

The following figure, Fig-4 illustrates the perception of proposed approach attack detection efficiency, in which it is cross-validated with the conventional DDoS attack detection scheme called IAIS and provide the graphical proof to prove the efficiency of the MLCAD scheme.

Fig.4 Attack Detection Efficiency

The following figure, Fig-5 illustrates the perception of proposed approach timing efficiency, in which it is cross-validated with the conventional DDoS attack detection scheme IAIS timing efficiency and provide the graphical proof to prove the time efficiency of the MLCAD scheme in clear way.

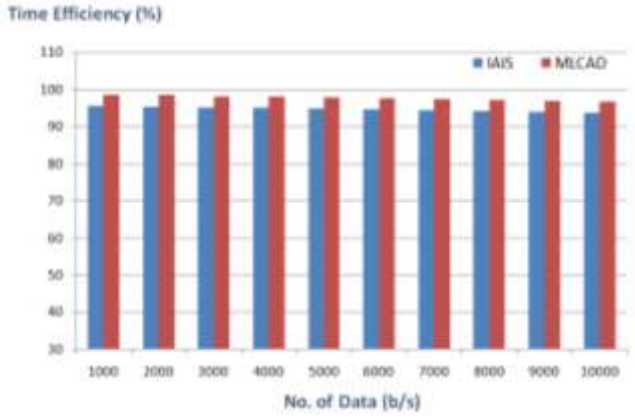

Fig.5 Time Efficiency of MLCAD and IAIS

5. Conclusion

In this paper we introduced a novel deep learning scheme called Modified Learning based Cloud Attack Detection (MLCAD) based on the conventional DDoS attack detection scheme called IAIS. As we all know, cyber security is the most essential problem in the globe today. At the moment, DDoS attacks are a very prevalent type of assault, and as a result, people are concerned about the security of their data and resources. The suggested architecture includes the capability to cope with distributed denial of service attacks on cloud computing via a DDoS protection cloud. Due to the fact that DDoS attacks cause catastrophic damage to network capacity and customer information in a very short period of time, our suggested model will assist in rectifying DDoS attacks and preserving the maximum amount of network resources possible. For future development, we intend to add more characteristics in this architecture in order to improve its usefulness.

References

[1] Ramya R. and Kesavaraj G., "A Survey on Denial of Service Attack in Cloud Computing Environment," International Journal of Advanced Research in Education & Technology (IJARET) vol. 2, no. 3, pp. 131-133, 2015.

[2] Somani G., Gaur M. S., Sanghi D., Conti M. and Buyya R., "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications vol. 107, pp. 30-48, 2017.

[3] Mehta R., "Distributed Denial of service Attacks on Cloud Environment," International Journal of Advanced Research in Computer Science vol. 8, no. 5, pp. 2204-2206, 2017.

[4] Bonguet A. and Bellaiche M., "A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing," Future Internet vol. 9, no. 3, pp. 1-19, 2017.

[5] Bhosale K. S., Nenova M. and Iliev G., "The distributed denial of service attacks (DDoS) prevention mechanisms on application layer," 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), pp. 136-139, 2017.

[6] Wang C., Zheng J. and Li X., "Research on DDoS Attacks Detection Based on RDF-SVM," 10th International Conference on Intelligent Computation Technology and Automation (ICICTA), pp. 161-165, 2017.

[7] Dong S., Abbas K. and Jain R., "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," IEEE Access vol. 7, pp. 80813-80828, 2019.

[8] Wu D., Li J., Das S. K., Wu J., Ji Y. and Li Z., "A Novel Distributed Denial-of-Service Attack Detection Scheme for Software Defined Networking Environments," 2018 IEEE International Conference on Communications (ICC), pp. 1-6, 2018.

[9] Khadijeh Wehbi, Liang Hong, Tulha Al-salah and Adeel A Bhutta, "A Survey on Machine Learning Based Detection on DDoS Attacks for IoT Systems", IEEE, 2019.

[10] Ui-Jun Baek, Se-Hyun Ji, Jee Tae Park, Min-Seob Lee, Jun-Sang Park and Myung-Sup Kim, "DDoS Attack Detection on Bitcoin Ecosystem using Deep-Learning", 20th Asia-Pacific Network Operations and Management Symposium, 2019.

[11] Shahzeb Haider, Adnan Akhunzada, Ghufran Ahmed and Mohsin Raza, "Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs", UK/ China Emerging Technologies, 2019.

[12] Ulya Sabeel, Shahram Shah Heydari, Harsh Mohanka, Yasmine Bendhaou, Khalid Elgazzar and Khalil El-Khatib, "Evaluation of Deep Learning in Detecting Unknown Network

Attacks", International Conference on Smart Applications, Communications and Networking, 2019.

[13] Subham Kumar and Ashutosh Bhatia, "Detecting Domain Generation Algorithms to prevent DDoS attacks using Deep Learning", IEEE International Conference on Advanced Networks and Telecommunications Systems, 2019.