**How to Cite**:
Madan, S., Anita, A., & Ali, A. (2022). DDoS attacks in cloud environment. *International Journal of Health Sciences*, *6*(S4), 5836–5847. https://doi.org/10.53730/ijhs.v6nS4.9457

# DDoS attacks in cloud environment

**Shefali Madan**
Associate Professor, Echelon Institute of Technology, Faridabad
Corresponding author email: shefalimadan@gmail.com

**Anita**
Associate Professor, Echelon Institute of Technology, Faridabad
Email: eranitachauhan@gmail.com

**Ashif Ali**
Assistant Professor, Echelon Institute of Technology, Faridabad
Email: ashifali76@gmail.com

***Abstract*---**Network communication is gaining day by day in different ways. Cloud is one of the most recent and latest environments in communication. Whereas this environment is a facilitator for the user to access his/her information from anywhere as and when required. But this technological enhancement is also opening the door for new attacks. In this paper, we have conducted an extensive study on the Distributed Denial of Service Attack (DDoS) as well as the techniques which are used up till now for detection as well as prevention of those attacks. We also have thoroughly presented the details of some very frequent techniques and in the end, we have also discussed some research gaps. This study will facilitate the new research in this era to find out the research problems and provide the optimal solutions for those problems.

***Keywords*---**DDoS, HTTP flood molest, cloud security worries, cloud computing, ping death, slow loris, SYN flood assaults.

## Introduction

Infrastructure as a service, software as a service, and platform as a service are three key cloud computing services made possible by the Internet [1]. Increased cloud storage of data and information has prompted cloud security worries about the protection of data and information. A side from ICMP flood, Ping of Death, Slow Loris, and SYN flood assaults [2] and [3], HTTP flood molest, protocol vulnerability exploitation, and malformed packet attacks, [2], distributed attacks have also resulted. It is up to the attacker to determine how easy it is to exploit a system and how well-versed he or she is in that particular attack technique. A DDoS attack is an attempt to disrupt and deny access to services or network

*Manuscript submitted: 27 March 2022, Manuscript revised: 18 May 2022, Accepted for publication: 9 June 2022*

resources. During anattack, the targeted website is flooded with unwanted, illegitimate traffic from several computers.

Distributed assaults on the cloud may be discovered, stopped, and mitigated by previous studies. These strategies rely heavily on the two primary detection mechanisms of signature or abnormalities. If they're clever enough, they'll be able to learn new attacks based on predetermined guidelines. Intrusion detection methods that use classical methods are discussed in the next section. In addition, it provides examples of different cloud computing-based detection approaches. There is an underlying goal of comparing the different detection systems and highlighting their strengths and weaknesses. In addition to the review, the article will demonstrate the success or failure of individual strategies developed by specific researchers in the detection of cloud-based DDoS assaults. For each approach, the measures used to evaluate its performance will be presented. These strategies employ a variety of data sets and technologies that will be highlighted throughout the study. Thus, it is easy to determine if an approach is effective or has the possibility for improvement.

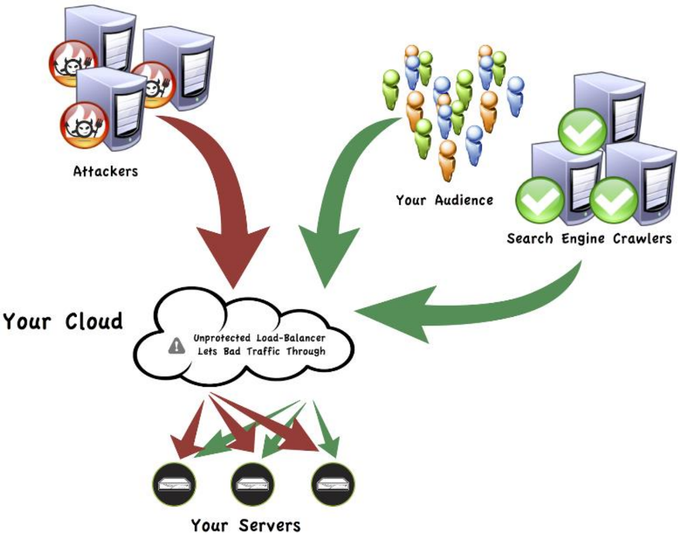


Fig. 1 Cloud-Server Architecture

According to Cloud Security Alliance, DDoS is one of the top nine threats to cloud computing environment 13 . Out of many attacks in clod envi- ronment 14% are DoS attacks. Many popular websites like yahoo were affected by DDoS in early 2000. Website of grc.com was hit by huge DDoS in May, 2001.

## Cloud

Cloud computing provides the platform, resources, and high availability and web applications on demand. The computing framework has shifted the whole viewpoint of businesses and industries far from the concept of deploying the daily work base of their applications/services by providing on-demand and charging you for your use. In the IT industry, cloud computing has become more popular due to the availability and quality of services for the customer. On-demand computing, resource spooling, and quality of service are all embodied by the National Institute of Standards and Technology (NIST). Based on the diagram in Fig.1.1, services may be divided into three broad categories: platform services, software services, and infrastructure services [1] and [4]. Services such as operating system, software, middleware, virtual server, and storage space are provided via SaaS. Vendors in the cloud provide this service, which may be accessible through a web application. Create, remove, and query permissions may be granted to users at their request. User-level services, rather than infrastructure and platform services, are the primary emphasis of this product line [5]. User-level applications are virtualized; therefore cloud service providers have full control over the user-level application. Also, the program is likely to have constraints on the modification that may be done. Although the program is customizable to some level, users are free to alter it to suit their needs. Outlook, Google Drive, and Salesforce are just a few examples of this kind of software.

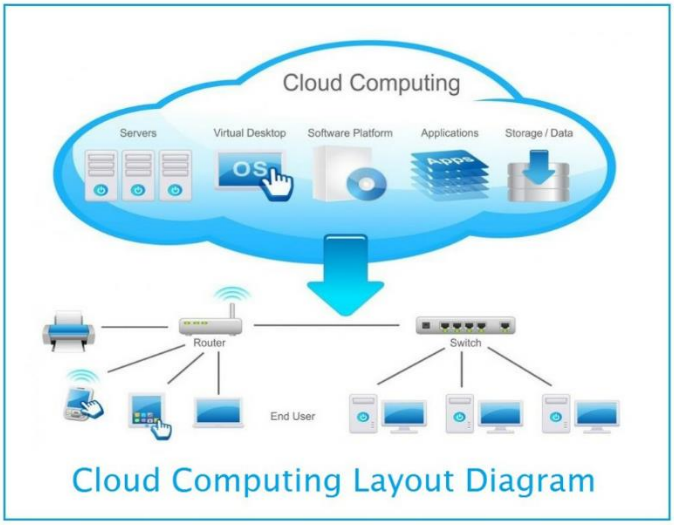


Fig 1.1: Cloud Services

Fig 1.1 for “Cloud Services” The implementation of PaaS enables businesses to build and install cloud applications without having to own the corresponding infrastructure themselves. Users may manage their application and data using PaaS capabilities that include advancement services, integration, and testing. The service provider is in charge of everything else. In a PaaS, the cloud service provider holds the data. When it comes to the working platform and development platform, cloud users are often responsible for everything above them. Additional applications that may be needed in the future will be the responsibility of the user.

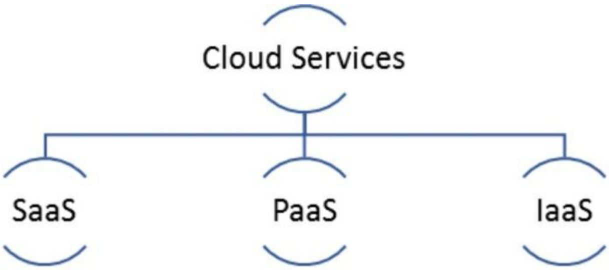


Fig. 1.2 Cloud Services

**AWS Services Used**

1. *AWS WAF:-*AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of security rules. With AWS WAF, you pay only for what you use. The pricing is based on how many rules you deploy and how many web requests your application receives. There are no upfront commitments.
2. AWS GuardDuty:-Amazon GuardDuty is priced based on the quantity of AWS CloudTrail Events analyzed and the volume of Amazon VPC Flow Log and DNS Log data analyzed. There is no additional charge to enable these log sources for GuardDuty analysis.
3. *AWS Shield:-* AWS Shield is a service that provides protection against DDoS attacks for web applications on AWS. There are two types of AWS Shield, Standard and Advanced, with Standard being free and Advanced being paid version.

This includes software component updates and online application monitoring, among other responsibilities. Despite immediate access, the database may be shared with the customer if necessary. Google apps and Salesforce apps are two examples of useful programs. Core infrastructure, such as computing power, storage, a network, and an operating platform, are all provided by IaaS. The allotted resources may then be used to build one's surroundings. Cloud clients may use the hardware provided by IaaS, such as a server. The server will be hosted on the provider's side, and the users will have full access. Servers may be configured to run any software that cloud users need. Because the cloud service provider is unable to deliver multitenancy, the services are more costly. [2]. Because of this, customers will be able to pay the costs of the system. It's becoming more commonplace to use IaaS, and there are a variety of platforms available.

**DDoS**

DDoS assaults are a subset of denial of service (DoS) attacks that are distributed. A botnet is a collection of linked internet devices that are used to overload a target website with bogus traffic in a DDoS attack.
A DDoS attack is an attempt to disrupt and deny access to services or network resources. During an attack, the targeted website is flooded with unwanted, illegitimate traffic from several computers. DDoS attacks, unlike other types of cyberattacks, do not aim to penetrate your network's defenses. Instead, a DDoS

assault seeks to prevent genuine people from accessing your website or servers. There are many different ways in which DDoS may be utilized, such as a smokescreen for other malicious actions and for taking down the target's protection equipment. DDoS attacks that target the whole internet user population are quite apparent. Hacktivists, cyber vandals, extortionists, and anybody else who wants to make a point or advocate a cause utilize it often. DDoS attacks may take days, weeks, or even months for a website or company to recover from, regardless of how many times they occur. As a result, DDoS attacks on online organizations may be devastating. DoS assaults may destroy a company's income, faith in customers, cost millions in compensation, and harm its brand, just to name a few consequences.

### Cloud-based DDoS attack

Twitter, Amazon, Github, and others have been affected by DDoS assaults on Dyn [9] DNS infrastructure, which is operated by the company. To resolve DNS and other third-party CSPs, AWS uses various service providers. There was an issue with hostname resolution as a result of the assaults, resulting in sporadic connection. When Mirai, a malicious virus that infiltrated an unprotected IoT system, got a command from a central server, it launched a flood assault on the device. As a result, internet service providers (ISP) reported poor service as millions of botnets were using network capacity. Assailants are now focusing their efforts on the gaming industry, which is open 24 hours a day, seven days a week, and has high bandwidth and a large number of online transactions. DDoS assaults on Xbox and Reddit disrupted service for real users [11]. With DNS reflection patterns and overload, Feedly [12] also survived an assault by a DDoS swarm. DDoS assaults resulting in service interruptions are the result of this ransomware attack. Some are shown in Table 2.1.

Attacks requesting large quantities of money from SaaS-based firms were also common. DDoS flood attacks using a UDP protocol vulnerability have been reported on the biggest cloud provider, Amazon [13], as well [14].

Table 2.1: Cause of Attacks

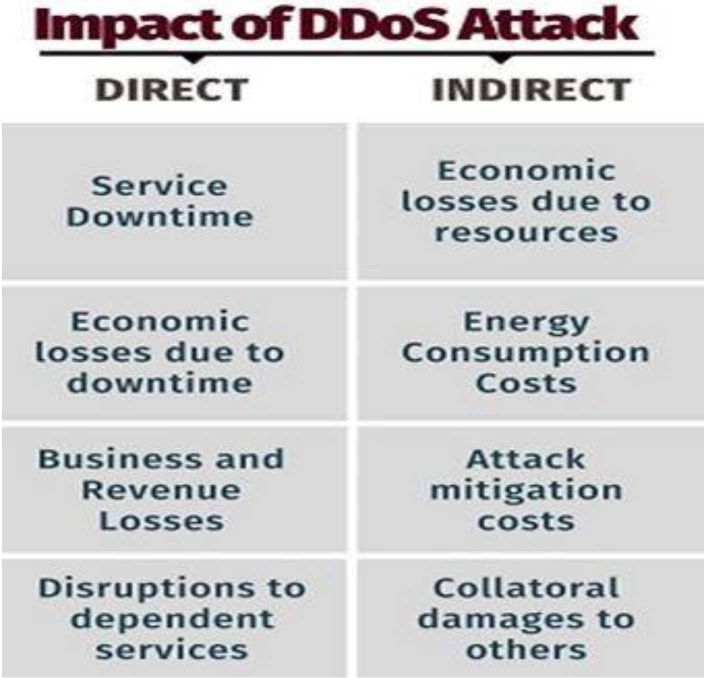
| # | Target | Cause of Attack | Year |
|---|---|---|---|
| 1 | Dyn [9] | DNS Flood | Oct 2016 |
| 2 | News Site and Xbox Live Reddit [11] | DDoS | Dec 2015 |
| 3 | Feedly News [12] | Application Overload and DNS Reflection attack | Nov 2014 |
| 4 | Amazon Cloud Services [13] | UDP Flood | Jul 2014 |
| 5 | Microsoft Cloud Services [14] | UDP Flood | Feb 2014 |
| 6 | US Banking Websites [15] | ICMP/UDP with HTTPS attacks | Apr 2013 |

DDoS flood packets were sent by taking advantage of a vulnerability in the virtual machine. DDoS assaults and cryptocurrency mining were shown in a botnet built by Bishop Fox at the black hat conference [14] and [20]. UDP/ICMP and HTTPS DDoS assaults were used to infiltrate banking websites [15]. More than 70Gbps of bandwidth and 30 million packets are used in DDoS assaults.

**The attacks are explained in detail**

1. ICMP Floods: An Internet Control Message Protocol (ICMP) flood DDoS attack, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).
2. DNS Amplification: Using various amplification techniques, perpetrators can "inflate" the size of these UDP packets, making the attack so potent as to bring down even the most robust Internet infrastructure. DNS amplification, like other amplification attacks, is a type of reflection attack.
3. Volume Based Attacks: Attacks utilize a huge quantity of traffic which saturating the total bandwidth of the Target.
4. Application Layer Attacks: Protection and Preventive Measures An Application Layer attack (DDoS attack) exploits system vulnerabilities and loopholes to attack the application resulting in complete malfunction.

Loss of profitability is another effect. Numerous organizations and associations utilize their system, online assets and openly accessible services to help their essential business. Any interruption to the accessibility of these important assets brings about lost profitability.



Impact of DDoS Attack

| DIRECT | INDIRECT |
|---|---|
| Service Downtime | Economic losses due to resources |
| Economic losses due to downtime | Energy Consumption Costs |
| Business and Revenue Losses | Attack mitigation costs |
| Disruptions to dependent services | Collatoral damages to others |

Fig. 2 Direct and Indirect DDoS Attack diagram

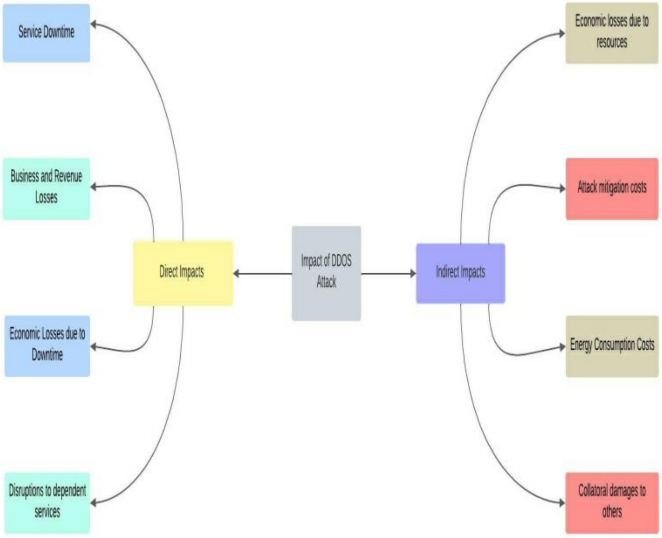

Service Downtime
Business and Revenue Losses
Economic Losses due to Downtime
Disruptions to dependent services
Direct Impacts
Impact of DDOS Attack
Indirect Impacts
Economic losses due to resources
Attack mitigation costs
Energy Consumption Costs
Collatoral damages to others

Fig. 3 Process of DDOS Attack

## Cloud-Based DDoS Solutions

DDoS attacks have risen to prominence as the most damaging kind of cyberattack on cloud computing infrastructure. To guarantee that genuine customers get a high-quality service, cloud security must be maintained Among the most important characteristics of the cloud is its capacity to provide high levels of security while still allowing for ease of use. DDoS assaults must be analyzed to ensure a safe cloud environment. Table 3.1 discusses in depth the different "DDoS solutions in the cloud computing context." "Cloud DDoS Detection Rule-based engines" in a cloud computing environment detect the application layer attack. For speeding up the processing and eliminating errors, the MapReduce framework is employed. In comparison to SNORT, this pattern detection method performs better and takes less time to process [16].

Table 3.1:Different "DDoS solutions in the cloud computing context

| Authors | Techniques | Advantages | Disadvantages |
|---|---|---|---|
| Choi 2014 [16] | Signature | Error is low<br>Fast, processing time | High response time |
| Cha and Kim 2011 [17] | Signature | Error is low,<br>Fast processing time | High response time |
| Navaz 2013 [18] | Entropy | Error is low,<br>Fast processing time | Efficiency reduces if the attack distribution varies. |
| Chouhan 2012 [19] | Hop count | Error is low,<br>Fast processing time | Difficult maintenance of a legitimate database |

| | | | |
|---|---|---|---|
| Chouhan 2012 [19] | Network | Detects collaborative attacks | Difficult maintenance of a legitimate database |

DDoS assaults in the cloud may be detected using a method called multistage anomaly detection [17]. In the monitoring phase, the attack patterns are compared to the rule base to determine whether misuse has occurred. Based on the volume, anomaly detection is used for in- depth analysis and Bayesian classification to identify assaults. For the identification of large anomalies that lead to DDoS assaults, unsupervised learning is used in targeted anomaly detection.

Genuine users can pass via the router with the help of an entropy-based approach [18]. When the threshold value is below a certain level, the confirmation algorithm sends an alert to the cloud service provider (CSP). Gathering information on ports and IP addresses is used to determine the entropy threshold. Customers are alerted to and blocked from transmitting packets at a high rate by the cloud service provider (CSP). In the cloud, faked sources can be detected via hop count detection [19]. The IP packet's originating IP and TTL are used to identify it. The packet is considered valid if the source IP and the related TTL are located in the database. At the gateway router, the attack packets are discarded with minimal computational overhead. An attack analyzer is part of the network-based detection [20], which includes the network controller and a profile server.

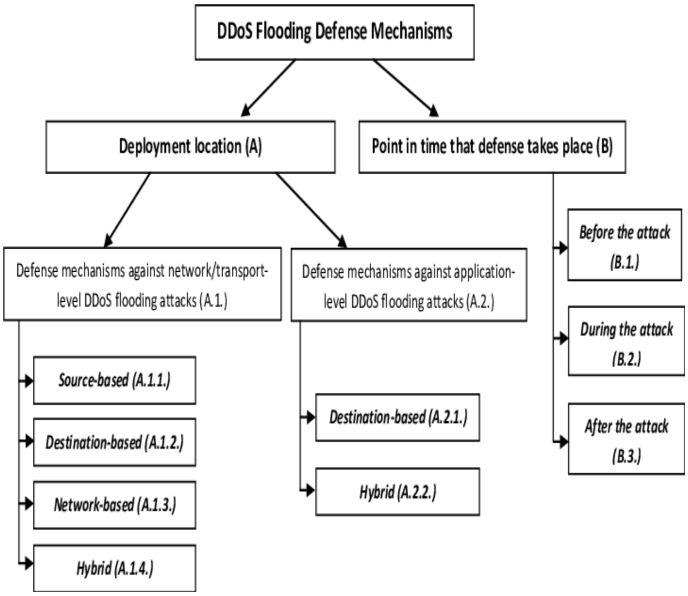

DDoS Flooding Defense Mechanisms
Deployment location (A)
Point in time that defense takes place (B)
Defense mechanisms against network/transport-level DDoS flooding attacks (A.1.)
Defense mechanisms against application-level DDoS flooding attacks (A.2.)
Source-based (A.1.1.)
Destination-based (A.1.2.)
Network-based (A.1.3.)
Hybrid (A.1.4.)
Destination-based (A.2.1.)
Hybrid (A.2.2.)
Before the attack (B.1.)
During the attack (B.2.)
After the attack (B.3.)

Fig. 4 Flowchart of DDoS Solution Mechanism

The analyzer determines the most effective defenses, and the network controller implements them. The profile server contains all of the virtual machine's security flaws in a cloud-based system. DDoS attack origins may be located via attack graph modeling. Users' typical profile is maintained by collecting information from their packet header using confidence-based filtering [21]. The incoming packet's correlation parameter is assessed. The packet is accepted if the value is within the acceptable range; else, it is rejected. Statistics filtering [22] keeps the regular profile with information such as hop count and TTL value gathered from the header. If the inbound source IP address can be found in a valid database, the IP address is regarded as genuine; otherwise, the IP address is considered spoofing. Divergence metrics are applied to the non-spoof IP address, and the likelihood of observation is calculated. The IP address of the source is banned if there is any variance.

Attack Mitigation :DDoS mitigation is a set of network management techniques and/or tools, for resisting or mitigating the impact of distributed denial-of-service (DDoS) attacks on networks attached to the Internet, by protecting the target, and relay networks. DDoS attacks are a constant threat to businesses and organizations, by delaying service performance, or by shutting down a website entirely

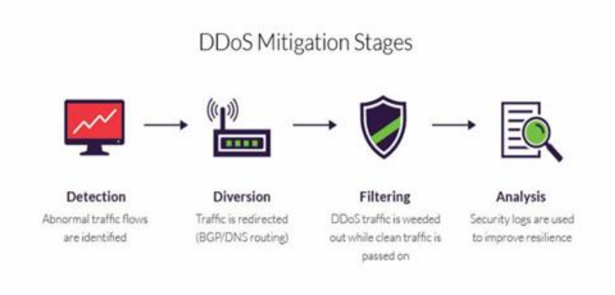

DDoS Mitigation Stages
Detection
Abnormal traffic flows are identified
Diversion
Traffic is redirected (BGP/DNS routing)
Filtering
DDoS traffic is weeded out while clean traffic is passed on
Analysis
Security logs are used to improve resilience

Fig. 5 DDos Mitigation Stages

## Conclusion and Further Scope

Cloud data must be protected from any sort of cyberattack. The challenge of securing the cloud is daunting, but it is necessary. Assaults in the cloud are known as "Distributed Denial of Service (DDoS) attacks." The techniques used to counter DDoS attacks are heavily influenced by tried-and-true methods, as this paper has demonstrated. DDoS assaults may be detected and prevented using several techniques, although none have been shown to be completely foolproof.

For a DDoS assault to be detected or prevented, the attacker's motive must be established. There are seven reasons given by reference [40] for DDoS assaults, namely: intellectual challenge, vengeance, ideological belief, sluggish network performance, financial and commercial gain, service unavailability, and cyber warfare. An assault might be motivated by a single factor or a combination of factors. Researchers in the future will have to devise ways for not only detecting an attack but also intelligently identifying the attacker's tactics and traffic rates. In addition, the techniques should be able to determine the validity of the attacker's origins, as well. It is possible to further improve the performance of the IDS using several of the previously suggested and implemented ways. Instead of focusing on one location, the method might strive toward having several sites of attack detection and repair. Distributed attack analysis points can be added to the approaches to increase detection and inference speed by relaying attack descriptions to a central location. As a result, all aspects of an assault might be identified without compromising system performance.

## References

1. Yang, L.; Shami, A. A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams. IEEE Internet ThingsMag. 2021, 4, 96–101.
2. Qaddoura, R.; Al-Zoubi, A.M.; Almomani, I.; Faris, H. A Multi-Stage Classification Approach for IoT Intrusion Detection Basedon Clustering with Oversampling. Appl. Sci. 2021, 11, 3022.
3. Shi, W.C.; Sun, H.M. DeepBot: A time-based botnet detection with deep learning. Soft. Comput. 2020, 24, 16605–16616.
4. Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. In Proceedingsof the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30September 2018; pp. 118–122.
5. McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet Detection in the Internet of Things using Deep Learning Approaches. InProceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
6. Stiawan, D.; Suryani, M.E.; Susanto; Idris, M.Y.; Aldalaien, M.N.; Alsharif, N.; Budiarto, R. Ping Flood Attack Pattern RecognitionUsing a K-Means Algorithm in an Internet of Things (IoT) Network. IEEE Access 2021, 9, 116475–116484.
7. Al-Haija, Q.A.; Smadi, A.A.; Allehyani, M.F. Meticulously Intelligent Identification System for Smart Grid Network Stability toOptimize Risk Management. Energies 2021, 14, 6935.
8. Chandra, B.E.; Karthikeyan, E. Sigmis: A feature selection algorithm using the correlation-based method. J. Algorithms Comput. Technol. 2012, 6, 385–394.
9. Singh, D.; Birmohan, S. Investigating the impact of data normalization on classification performance. Appl. Soft Comput. 2020,97, 105524.
10. Al-Haija, Q.A.; Alsulami, A.A. High-Performance Classification Model to Identify Ransomware Payments for HeterogeneousBitcoin Networks. Electronics 2021.
11. Abu Al-Haija, Q.; Krichen, M.; Abu Elhaija, W. Machine-Learning-Based Darknet Traffic Detection System for IoT Applications.Electronics 2022, 11, 556.
12. Stamp, M. A survey of machine learning algorithms and their application in information security. In Guide to Vulnerability Analysisfor Computer Networks and Systems; Springer: Cham, Switzerland, 2018; pp. 33–55.
13. Timˇcenko, V.; Gajin, S. Ensemble classifiers for supervised anomaly-based network intrusion detection. In Proceedings of the2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania,7–9 September 2017; pp. 13–19.
14. Gaikwad, D.P.; Thool, R.C. Intrusion detection system using bagging with partial decision tree based classifier. Procedia Comput. Sci.2015, 49, 92–98.
15. Al-Haija, Q.A.; Ishtaiwi, A. Multiclass Classification of Firewall Log Files Using Shallow Neural Network for Network SecurityApplications. In Soft Computing for Security Applications. Advances in Intelligent Systems and

Computing; Ranganathan, G.,Fernando, X., Shi, F., El-Allioui, Y., Eds.; Springer: Singapore, 2022; Volume 1397.

16. Aygun, R.C.; Yavuz, A.G. Network anomaly detection with stochastically improved autoencoder based models. In Proceedingsof the 4th International Conference on Cyber Security and Cloud Computing, New York, NY, USA, June 2017; pp. 193–198.
17. Kumar, A.; Lim, T.J. EDIMA: Early detection of IoT malware network activity using machine learning techniques. In Proceedingsof the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 289–294.
18. Ioannou, C.; Vassiliou, V. Classifying Security Attacks in IoT Networks Using Supervised Learning. In Proceedings of the 201915th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May2019; pp. 652–658.
19. Gao, X.; Shan, C.; Hu, C.; Niu, Z.; Liu, Z. An Adaptive Ensemble Machine Learning Model for Intrusion Detection. IEEE Access2019, 7, 82512–82521.
20. Abu Al-Haija, Q.; Sabatto, S.Z. An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoTCommunication Networks. Electronics 2020, 9, 2152.
21. Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet detection via power consumption modeling. Smart Health 2020, 15, 100103.
22. Ashraf, J.; Keshk, M.; Moustafa, N.; Abdel-Basset, M.; Khurshid, H.; Bakhshi, A.D.; Mostafa, R.R. IoTBoT-IDS: A novel statisticallearning-enabled botnet detection framework for protecting networks of smart cities. Sustain. Cities Soc. 2021, 72, 103041.
23. Abu Al-Haija, Q.; al-Badawi, A.; Bojja, G.R. Boost-Defence for resilient IoT networks: A head-to-toe approach. Expert Syst. 2022,39, e12934.
24. B.S.K. Devi and T. Subbulakshmi, “A Comparative Analysis of Security Methods for DDoS attacks in the Cloud Computing Environment”, Indian Journal of Science and Technology, vol. 9, no. 34, pp. 1-7, 2016.
25. M. Sebastian, Major DDoS attack on Dyn disrupts AWS Twitter Spotify and more, October 2016.
26. A. Kumar et al., “Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-Sampled Packet Traffic Analysis”, 2019.
27. J. Choi, C. Choi, B. Ko and P. Kim, “A Method of DDoS Attack Detection using HTTP Packet Pattern and Rule Engine in Cloud Computing Environment”, Soft Computing, vol. 18, no. 9, pp. 1697-1703, 2014.
28. A.S. Navaz, V. Sangeetha and C. Prabhadevi, “Entropy-based Anomaly Detection System to Prevent DDoS Attacks in Cloud”, International Journal of Computer Applications, vol. 62, no. 14, 2013.
29. V. Chouhan and S.K. Peddoju, “Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing”, International Journal of Computer Science and Electrical Engineering, vol. 1, no. 1, pp. 38-42, 2012.
30. W. Dou, Q. Chen and J. Chen, “A confidence-based filtering method for DDoS attack defense in cloud environment”, Future Generation. Systems., vol. 29, no. 7, pp. 1838-1850, 2013.
31. P. Shamsolmoali and M. Zareapoor, “Statistical-based filtering system against DDOS Attacks in cloud computing”, Proceedings of the International Conference on Advances in Computing Communications and Informatics, pp. 1234-1239, 2014.

32. F.A. Guenane, B. Jaafar, M. Nogueira, and G. Pujolle, “Autonomous architecture for managing firewalling cloud-based service”, Proceedings of the International Conference and Workshop on the Network of the Future, pp. 1-5, 2014.
33. Kshirsagar, Deepak, and Sandeep Kumar. "A feature reduction based reflected and exploited DDoS attacks detection system." Journal of Ambient Intelligence and Humanized Computing 13, no. 1 (2022): 393-405.
34. Kautish, Sandeep, A. Reyana, and Ankit Vidyarthi. "SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment." IEEE Transactions on Industrial Informatics (2022).
35. Gaur, Vimal, and Rajneesh Kumar. "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices." Arabian Journal for Science and Engineering 47, no. 2 (2022): 1353-1374.
36. Aziz, Israa T., Ihsan H. Abdulqadder, and Thakwan A. Jawad. "Distributed Denial of Service Attacks on Cloud Computing Environment." Cihan University-Erbil Scientific Journal 6, no. 1 (2022): 47-52.
37. Raich, Anagha, and Vijay Gadicha. "Overview of passive attacks in cloud environment." In AIP Conference Proceedings, vol. 2424, no. 1, p. 030004. AIP Publishing LLC, 2022.
38. Chaudhary, Deepali, Kriti Bhushan, and Brij B. Gupta. "Survey on DDoS attacks and defense mechanisms in cloud and fog computing." International Journal of E-Services and Mobile Applications (IJESMA) 10, no. 3 (2018): 61-83.
39. Aydın, Hakan, Zeynep Orman, and Muhammed Ali Aydın. "A Long Short-Term Memory (LSTM)-Based Distributed Denial of Service (DDoS) Detection and Defense System Design in Public Cloud Network Environment." Computers & Security (2022): 102725.
40. Agrawal, Ankit, Rajiv Singh, Manju Khari, S. Vimal, and Sangsoon Lim. "Autoencoder for Design of Mitigation Model for DDOS Attacks via M-DBNN." Wireless Communications and Mobile Computing 2022 (2022).
41. Nyandra, M., Suryasa, W. (2018). Holistic approach to help sexual dysfunction. *Eurasian Journal of Analytical Chemistry*, *13*(3), pp. 207–212.
42. Suryasa, W. (2019). Historical Religion Dynamics: Phenomenon in Bali Island. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(6), 1679-1685.
43. Wijayanti, N. (2021). Factors related to behavior the community in disposing of garbage. *International Journal of Health & Medical Sciences*, *4*(1), 74-79. https://doi.org/10.31295/ijhms.v4n1.1226