JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Detection of DDoS/DoS Attack Methodologies in Cloud Computing Network: A Survey

Tariq Mehboob[1], Irshad Ahmad Sumra[2*], and Iram Shahzadi[1]

[1]Department of Information Technology, Lahore Garrison University Lahore, 54000, Pakistan.
[2]Department of Computer Science, Lahore Garrison University Lahore, 54000, Pakistan.
[*]Corresponding Author: Tariq Mehboob. Email: ranatariqm@gmail.com

Received: February 21, 2024 **Accepted:** September 28, 2024

Abstract: The concept of cloud computing has been proposed for many years, and the first cloud computing service was launched in the 21st century. Cloud computing uses the Internet or the cloud to provide computing services such as servers, storage, databases, networks, software, analytics, and intelligence. The three types of cloud computing include IAAS, PAAS, and SAAS. CIA, which stands for Trust, Integrity, and Availability, is the foundation of information security. While DDoS/DoS destroys availability, network unavailability and network inadequacy affect reliability. DoS and distributed DoS (DDoS) attacks have become more sophisticated and cannot be stopped by traditional protection tools in cloud computing. Machine learning and neural networks are subcategories of software computing techniques that can be used for network analysis to detect patterns in the occurrence of DDoS/DoS attacks. With the rise of cloud computing, the threat of attacks has also increased. Attackers are also using new technologies to attack the cloud to disrupt services. These attacks can cause serious damage to cloud service providers and their customers. DDoS/DoS attacks attempt to prevent loss of revenue, reputation, and trust. By using cloud computing technology, cloud service providers can ensure that their services are secure and reliable, thereby enhancing confident and proud customer experience.

Keywords: IAAS; PAAS; SAAS; Public; Private; Hybrid; Community; Integrity; Confidentiality; Availability.

1. Introduction

The rapidly up gradation of technology is driving the world of technology towards most secure security resources, multiple companies are using cloud for securing their data but cloud needs to secure with multiple ways too. Due to rapid change in recent world, lots of security challenges are getting developed with rapidly developing technology, that need to cover up with latest best suitable sources that can overcome these challenges and make the data secure and durable. Cloud is word, utilized as a substitution of web. While cloud computing is kind of web-based computing. Multi the world "Cloud" is really utilized as the substitution of web while the computing connected to the preparing of the educated charge utilizing assets. So, the cloud issues in regards to security are connected with cloud security e.g. outpouring of information, information insecurity, sharing of information that isn't permitted and inside DDoS/DoS attacks [1].Basic security con- side rate on aspects that are linked with cloud security, data availability, integrity of the data, data management and other attacks. In case the user remains unable to access the services, it is assumed that the users are under the threat of these rapidly increasing security challenges [2].Cloud computing is a key to access multiple sources relating to storage, networking service etc. Cloud computing also save time and results in efficient and effective way of solution finding for the organizations having particular demand [3]. Cloud Computing works through depending on internet and its much necessary to secure the data and available sources.

Section 2 shows Security Goals, Section 3 represents importance of Availability, Section 4 represent Impact of DoS/DDoS attack, Section 5 shows DDoS attack in cloud computing, Section 6 represents

Literature Review, Section 7 shows Security Methods in Cloud Computing, Section 8 represents DoS/DDoS detection methodologies, Section 9 is about on Comparative Analysis Of Different Methodologies, Section 10 is Conclusion.

2. Security Goals

The CIA set of three of data security was made to give a reference line standard to surveying and applying proof security regardless of the central framework and association [4]. The three center objectives have unique necessities and procedures inside each other. The following Figure 1 shows security goals.

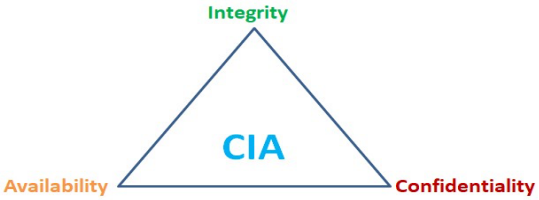

Figure 1. Security Goals

Confidentiality: Certifies that information or any material plan is gotten to by just an approved individual. Client Id's and keys, get to control records ACL and technique established asylum are a portion of the strategies through which confidentiality is accomplished [5].

Integrity: It depicts the unwavering quality ensures that the information or data framework can be solid. Affirms that it is altered by just approved people and remains in its one of a kind state when at reprieve. Actualities encryption and slashing systems are entering forms in giving integrity [6].

Availability: Facts and preparing information frameworks are accessible when obligatory. Equipment conservation, programming repairing/advancement and system improvement make certain availability.

3. Importance of Availability

Availability is a crucial aspect of cloud computing that refers to the ability of a cloud service or resource to be accessible and operational when needed. It is of paramount importance for several reasons.

- **A.** Business Continuity: Availability ensures that critical applications and services hosted in the cloud are accessible to users at all times. It helps maintain business continuity by minimizing downtime and ensuring uninterrupted operations. Organizations heavily rely on the cloud for mission-critical tasks, and any disruptions or unavailability can lead to significant financial losses and damage to their reputation [7].
- **B.** Customer Satisfaction: Cloud services often serve a large user base, ranging from individual consumers to enterprises. Availability plays a vital role in ensuring a positive user experience and customer satisfaction [8]. Users expect services to be available on-demand, and any downtime or service interruptions can lead to frustration, dissatisfaction, and potential loss of customers.
- **C.** Scalability and Elasticity: Cloud computing gives the option of getting resources in proportion to the demand for them. The attributes of availability are closely related to scalability and elasticity since it guarantees more resources can be provided for handling a higher workload. If availability is not present, the cloud infrastructure is not prepared to scale and can result in the provision of substandard service or have the service unavailable during usage surge times [9].
- **D.** Disaster recovery: Disaster recovery is one of the most important aspects of cloud computing, as organizations can replicate and restore their data and applications to multiple locations across multiple sites. These recycled materials should be easily accessible and usable in the event of damage or failure of important materials [10]. It helps reduce data loss, manage operations, and achieve faster recovery times.
- **E.** Service Level Agreements (SLAs): Availability is a critical metric defined in service level agreements between cloud service providers and customers. Providers commit to certain availability levels, typically expressed as a percentage of uptime. By guaranteeing high availability, providers instill confidence in customers that their services will be accessible as promised. SLAs often include penalties for failure to meet availability targets, reinforcing the importance of maintaining a highly available cloud infrastructure [11].

F. Cost Optimization: Availability indirectly contributes to cost optimization in cloud computing. Downtime or service disruptions can lead to lost productivity, revenue, and increased support costs. By ensuring high availability, organizations can minimize these costs and maximize the return on investment in cloud services.

4. Impacts of DoS Attack

Denial of Service (DoS) attacks on cloud networks can have many serious consequences. To mitigate the impact of DoS attacks, organizations need to implement security measures such as traffic monitoring, rate limiting, access detection and blocking barriers, and air recycling [12]. Also, having a contingency plan and backup and recovery strategy can help minimize the damage caused by an attack. Here are some things that will happen.

A. Service Disruption: A DoS attacks floods the target system or network with an overwhelming amount of traffic, making it difficult for legitimate users to access resources and services. This results in service disruption, causing downtime and unavailability of critical services hosted in the cloud [13].

B. Loss of Revenue: Cloud-based services are often used by businesses to deliver their products or services to customers. A successful DoS attacks can lead to prolonged service disruption, preventing the organization from generating revenue during the downtime [14]. Additionally, there may be financial penalties or contractual obligations for failing to meet service level agreements (SLAs).

C. Damage to Reputation: Downtime caused by a DoS attacks can significantly impact an organization's reputation [15]. Customers and users may lose trust in the company's ability to provide reliable services, leading to a loss of customers and potential business opportunities. Negative publicity and media coverage can further harm the reputation of the affected organization.

D. Financial Costs: Mitigating the effects of a DoS attacks can be costly. Organizations may need to invest in additional resources such as bandwidth, hardware, or specialized security solutions to handle increased traffic and filter out malicious requests. There may also be costs associated with incident response, investigation, and recovery efforts [16].

E. Customer Dissatisfaction: When services are disrupted due to a DoS attacks, customers and users may experience inconvenience, frustration, and dissatisfaction. This can lead to a loss of customer loyalty, negative reviews, and potential churn as users seek alternative service providers who can offer more reliable services.

F. Operational Disruption: The impact of a DoS attacks can extend beyond service availability. It can cause operational disruptions within an organization, affecting internal systems, communication channels, and productivity. Employees may be unable to access necessary tools or resources, resulting in delays or inefficiencies in their work [17].

G. Secondary Security Risks: A DoS attacks can serve as a distraction or smokescreen for other malicious activities. While defenders are focused on mitigating the DoS attacks, attackers may exploit vulnerabilities, infiltrate systems, or launch additional attacks such as data breaches, theft, or system compromise.

5. DDoS Attack in Cloud Computing

A Distributed Denial of Service (DDoS) attack in the context of cloud computing is a malicious attempt to disrupt the availability of a cloud-based service by overwhelming it with a flood of incoming traffic. In a DDoS attack, multiple compromised computers (often part of a botnet) are used to send a massive volume of traffic to a target system, causing it to become slow, unresponsive, or completely unavailable to legitimate users [18].

Here's how a DDoS attack in cloud computing works:

A. Target Selection: The attacker identifies a target cloud-based service, which could be a website, application, or any other online service hosted on cloud infrastructure.

B. Botnet Formation: The attacker gains control of multiple compromised devices, typically through malware or other malicious methods [19]. These compromised devices are collectively referred to as a "botnet."

C. Traffic Generation: The attacker commands the botnet to send a huge amount of traffic to the target service. This traffic could be in the form of HTTP requests, UDP flood, ICMP echo requests, or any other protocol used by the target service [20].

D. Overwhelming Resources: The massive influx of traffic overwhelms the target cloud service's resources, such as bandwidth, processing power, memory, and network capacity [21]. This results in legitimate users being unable to access the service.

E. Service Disruption: The target cloud service becomes slow, unresponsive, or completely unavailable to users due to the overwhelming traffic load. This disrupts the normal operations of the service.

F. Detection and Mitigation: Cloud service providers typically have various mechanisms in place to detect and mitigate DDoS attacks [22]. These may include traffic filtering, rate limiting, traffic analysis, and pattern recognition to distinguish between legitimate and malicious traffic.

G. Recovery: Once the attack is identified and mitigated, the cloud service can recover and resume normal operations [23]. Depending on the severity of the attack and the measures in place, recovery time may vary.

6. Literature Review

The availability is in the long run, the fundamental custom of the cloud. It speaks to the possibility of anyplace and whenever access to administrations, instruments and information and is the empowering influence of representations of future [24].

This thesis pretends to investigate current and potential future cloud computing trends using existing computing models for clouds. The distribution of cloud services, IaaS, PaaS, SaaS, and deployment models are all included in the virtual study. Promotions, excesses, hardware and software problems, programme failures, and other regular concerns make some interruption a reality due to organizational obstacles that make it difficult to achieve [25].

To deliver a methodical style to the research accessible in this paper, cloud catalog is familiarized to order and relate the offered cloud service contributions. In certain, this thesis emphases on the facilities of a rare main Cloud workers.

Amazon Web Services resolve be used as an improper in numerous instances since this cloud provider exemplifies about 70% of the existing community cloud services souk. It has developed a cloud services lead and a positioning point for further cloud service providers. The inquiry of cloud computing models has exposed that community cloud disposition model is possible to stop leading and save increasing more. Reserved and Hybrid assignment models are going to halt for centuries ahead then their market portion is profitable [26].

Similarly, the interest for cloud computing has naturally driven the creation of novel market solutions, catering to diverse cloud management and delivery paradigms. These models essentially expand the range of available choices, and assignment associations with questions about which cloud computing model to use. This postulation aims at conducting state of mind investigation of available cloud computing models and the possible future cloud computing trends. Affiliate assessment involves cloud administrations conveyance types (SaaS, PaaS, IaaS) and sending kinds (private, open, and half and half) [27].

The best stimulating fence for cloud adoption through distant is called data security. The most important asset for each corporation is data. All the corporations and businesses are focused on security and safety of their data. It is safer felling by companies and firms while saving their data internally because they have full control on it. Importantly the firms and corporations have no guarantee that data is safe and protected from a public cloud. Study discusses an option that data could not be affected by public cloud. This because the public cloud providers have more focus on security and safety of data as com- pared to their customers [28].

Cloud availability process that involves both practical and structural trials. There is swearing resistance of adoption is followed by cloud computing like the other disrupting technologies. Study discusses simulations about the cloud supporters. That is cloud supporters should be ready to overcome the resistance in their firms and business [29] The foremost key to accomplishing accessibility and safety in cloud is thoughtful definitely what that implies. IT segments dependably take a stab at the largest amounts of framework and application. We have distinguished and dissected a few availability and security issues from the clients' perspective in the viewpoint of a structure to perform specialized work

processes in differed distributed computing situations. This investigation has enabled us to recognize regular circumstances where distributed computing floats execute. To expand structure availability and unwavering quality, some cloud-based arrangements have been proposed inaccessible to go to up the net locales they host to honest to goodness guests. The prior state of the distributed computing that is fluffy in a substantial part, in light of the degree of the security dangers and for the all intents and purposes boundless measure of data being distributed [30].

The significant comes when the differences between the real cloud security and the virtual machine security appears. Our search has been directed toward these voids and opposites and the expulsion of tours. The principal purpose of this postulation distributed computing is to manage and securely process the information in cloud. For cloud security issues, one answer might be the structure of distributed computing can develop a way to filter the cloud administration programming, and another may be the extension of remote regulation for correct customer's claims [31].

7. Security Methods in Cloud Computing

Security is an important aspect of cloud computing, and many methods and best practices are used to ensure the protection of data and resources in the cloud environment. Below are some ways to implement security in cloud computing [32].

Cloud service providers typically provide encryption techniques to protect data at rest (stored in the storage system) and in transit (during transmission). This ensures that even if the data is compromised, it remains unreadable without the encryption key. One of the best methods is role-based access control (RBAC), where users are assigned roles with specific permissions. Another method is multi-factor authentication, which adds the use of other forms of personal authentication, such as passwords and access codes sent to the user's mobile phone.

Firewalls: Cloud providers employ firewalls to monitor and control network traffic in and out of their infrastructure. Firewalls are configured to enforce security policies and restrict unauthorized access to resources. They can be con- figured at various levels, such as host-based firewalls on individual virtual machines or network-level firewalls at the perimeter of the cloud infrastructure.

Intrusion Detection and Prevention Systems (IDS/IPS): IDS/IPS tools are used to detect and prevent illegal activities or attacks in cloud environments. These systems monitor network connections, detect patterns, and issue alerts or take critical steps to block suspicious activities.

Security Auditing and Logging: Cloud providers often maintain extensive logging capabilities to track and record various activities within the cloud environment. These logs can be used for security auditing, monitoring, and forensic analysis. Regular auditing of logs helps in identifying potential security issues, detecting anomalies, and ensuring compliance with security policies.

Data backup and disaster recovery: Cloud providers typically provide backup and disaster recovery systems to protect data from loss or failure. Regular backups ensure that data can be recovered in the event of data corruption, deletion errors, or other events. Disaster recovery plans are in place to recover weather conditions and services in the event of a major disaster or explosion.

Regular Updates and Patch Management: Cloud providers apply regular updates and patches to the underlying infrastructure and services to address security vulnerabilities and protect against emerging threats. Keeping the cloud environment up to date with the latest security patches helps mitigate the risk of potential attacks.

Security testing and penetration testing: Cloud providers often conduct security testing and penetration testing to identify vulnerabilities and weaknesses in their systems. These tests simulate real-world situations to evaluate the effectiveness of security controls and identify areas for improvement.

Data Isolation and Virtualization Security: Cloud providers use techniques like virtualization to isolate customer data and resources. Strong isolation ensures that one customer's data remains secure and inaccessible to others. Additionally, virtualization security measures are implemented to protect the hypervisor, virtual machine (VM) images, and related components.

Compliance and Regulatory Measures: Cloud providers adhere to industry-specific compliance standards and regulatory requirements, such as "GDPR, HIPAA, or PCI DSS." They implement security controls and practices to ensure that customer data is handled in accordance with these standards.

8. Comparative Analysis of Different Methodologies

Table 1. Comparative Analysis

Author Name	Objective	Methodology	Data Sets	Accuracy
Himanshi Chaudhry et al.(2022)[54]	To reduce time complexity and detect the attackers by mutual secret key	Hybrid techniques of genetic algorithm and extension of the Diffie-Hellman Algorithm	Network traffic analysis generated data	94.15%
Mythili Boopathi et al. (2022)[55]	The main intent of this research is to detect DDoS/DoS attacks Detection scheme, termed sine cosine anti corona virus optimization (SCACVO)	Sine cosine anti corona virus optimization (SCACVO)-driven Deep maxout network (DMN).	Logs data from log files unprocessed KDD-cup data file.	94.12%
Abdul Raoof Wani et al. (2020)[56]	The objective of this strategy is to classify traffic data whether it is suspicious, normal or unknown	K-means, Decision Tree, SVM, Naïve Bayes, C4.5	Produce dataset from Intrusion Detection System in csv file	K-means: 95.8%, Decision Tree:94.2%, SVM: 97.6% Naïve Bayes: 98.0% C4.5: 98.7%
S. R. Mugunthan (2019)[57]	The proposed HMM-RF for the identifying the low rate-DDDoS/DoS in the cloud data centers utilizes the Hidden Markov model to observe the features of the traffic flow in the network	Hidden Markov model	KDD Cup99 dataset	97.34%
S. Emerald Jenifer Mary et al (2019)[58]	An efficient structure is to identify and avert DDDoS/DoS in cloud condition.	DT, NN, SVM	Multiclass Dataset	DT: 90% NN: 70.8% SVM:80%
Zerina Mašetić et al. (2017)[59]	The aim is to detect potential Denial of Service (DDoS/DoS) attacks in the cloud computing, using Support Vector Machine (SVM) machine learning algorithm	SupportVector Machine (SVM)	Network tra ffic features	96%

Ms. Supriya S. Thakare, et al. (2017)[60]	To find behavior of the DDoS/DoS attacks and intrusive activity using MCA	Multivariate Correlation Analysis (MCA),	KDD Cup99 dataset	89.61%
Chen et al.(2016)[61]	The proposed system can efficiently monitor network activities, find abnormal behaviors, and detect network threats to protect critical infrastructure systems.	K-means clustering, Naïve Bayes	Network traffic data	90%
Swathi Sambangi et al. (2020) [62]	In this paper, the research objective is to study the problem of DDDoS/DoS attack detection in a Cloud environment	multiple regression analysis	CICIDS 2017 dataset	97.86%
Khorshed et al. (2015)[63]	It provides a security centric view of three-layered approach for understanding the technology, gaps and security issues and detect cyber-attacks	Random Forrest	Network Performance dataset	93.19%
M.T. Khorshed et al. (2012)[64]	To identify insider's activities and other DDoS/DoS attacks by using performance data.	C4.5, Decision Tree	Network usage and Performance dataset	93.47%
Amiri et al. (2011)[65]	To detect intrusion with high dimensionality	Least Square SupportVector Machine (LSSVM)	KDD99 Dataset	84.11%

9. Conclusion

In the conclusion of such a paper, researchers typically summarize the key objectives and contributions of their study. They may highlight the specific methodologies or techniques employed to detect DDoS/DoS attacks in cloud computing networks, including any novel approaches or algorithms developed. The effectiveness and efficiency of the pro- posed detection methods are often evaluated and discussed. Additionally, the conclusion may address the limitations or challenges encountered during the research process. This could involve discussing any constraints in data collection, potential vulnerabilities in the proposed detection techniques, or areas for future research and improvement. Furthermore, researchers may present the results of experiments or simulations conducted to validate the effective- ness of their detection methods. The conclusions drawn from these results can be discussed, emphasizing the accuracy, reliability, and scalability of the proposed approaches. It is also common for researchers to discuss the practical implications of their findings. This might involve addressing the potential impact of DDoS/DoS attacks on cloud computing networks and the significance of effectively detecting and mitigating such attacks. Lastly, the conclusion should summarize the overall contributions of the study to

the field of cloud computing security and emphasize the importance of ongoing research and development in this area to enhance the resilience and protection of cloud infra- structures against DDoS/DoS attacks.

References

1. Jansen, W., &Grance, T. (2011). Sp 800-144. Guidelines on security and privacy in public cloud computing.
2. Rittinghouse, J. W., &Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.
3. Padhy, R. P., Patra, M. R., &Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.
4. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.
5. Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 280-288). IEEE.
6. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and com- pliance. " O'Reilly Media, Inc."
7. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and com- pliance. " O'Reilly Media, Inc."
8. Poku, K. (2003). Impact of corporate orientation on information technology adoption in the United States forest products industry (Doctoral dissertation).
9. M. Li, F. Ye, M. Kim, H. Chen and H. Lei, "A Scalable and Elastic Publish/Subscribe Service," 2011 IEEE International Par- allel & Distributed Processing Symposium, Anchorage, AK, USA, 2011, pp. 1254-1265, doi: 10.1109/IPDPS.2011.119.
10. Abualkishik, Abedallah & Alwan, Ali & Gulzar, Yonis. (2020). Disaster Recovery in Cloud Computing Systems: An Over- view. International Journal of Advanced Computer Science and Applications. 11. 702. 10.14569/IJACSA.2020.0110984.
11. Aljoumah, Eman & Al-Mousawi, Fajer & Ahmad, Imtiaz & Al-Shammri, Maha & Al Jady, Zahraa. (2015). SLA in Cloud Computing Architectures: A Comprehensive Study. International Journal of Grid and Distributed Computing. 8. 7-32. 10.14257/ijgdc.2015.8.5.02.
12. Rashmi V. Deshmukh, Kailas K. Devadkar,Understanding DDoS Attack & its Effect in Cloud Environment,Procedia Com- puter Science,Volume 49,2015
13. Bonguet A, Bellaiche M. A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet. 2017; 9(3):43. https://doi.org/10.3390/fi9030043
14. Boopathi, M., Chavan, M., J., J.J. and Kumar, S.N.P. (2022), "An approach for DoS attack detection in cloud computing us- ing sine cosine anti coronavirus optimized deep maxout network", International Journal of Pervasive Computing and Com- munications, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJPCC-05-2022-0197
15. Daffu, Preeti & Kaur, Amanpreet. (2016). Mitigation of DDoS attacks in cloud computing. 1-5. 10.1109/WECON.2016.7993478.
16. Daffu, Preeti & Kaur, Amanpreet. (2016). Mitigation of DDoS attacks in cloud computing. 1-5. 10.1109/WECON.2016.7993478.
17. Bonguet A, Bellaiche M. A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet. 2017; 9(3):43. https://doi.org/10.3390/fi9030043
18. Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya,DDoS attacks in cloud computing: Issues, taxonomy, and future directions,Computer Communications,Volume 107,2017
19. Aziz, Israa T., Ihsan H. Abdulqadder, and Thakwan A. Jawad. "Distributed Denial of Service Attacks on Cloud Computing Environment." Cihan University-Erbil Scientific Journal 6.1 (2022): 47-52.
20. Aziz, Israa T., Ihsan H. Abdulqadder, and Thakwan A. Jawad. "Distributed Denial of Service Attacks on Cloud Computing Environment." Cihan University-Erbil Scientific Journal 6.1 (2022): 47-52.
21. Bonguet, Adrien, and Martine Bellaiche. "A survey of denial-of-service and distributed denial of service attacks and de- fenses in cloud computing." Future Internet 9.3 (2017): 43.
22. Daffu, Preeti & Kaur, Amanpreet. (2016). Mitigation of DDoS attacks in cloud computing. 1-5. 10.1109/WECON.2016.7993478.
23. Srinivasan, Karthik, et al. "A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitiga- tion techniques." Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019. Springer Interna- tional Publishing, 2020.
24. Cvetkovich, G. (2013). Social trust and the management of risk. Routledge.
25. Van Der Burgt, J. Cloud Computing as a sustaining or a disruptive technology.
26. Garfinkel, S., Spafford, G., & Schwartz, A. (2003). Practical UNIX and Internet security. " O'Reilly Media, Inc.".Hernández, S., Fabra, J., Alvarez, P., &Ezpeleta, J. (2013). Using cloud-based resources to improve availability

and reliability in a scien- tific workflow execution framework. In The Fourth International Conference on Cloud Computing, GRIDs, and Virtual- ization, CLOUD COMPUTING (pp. 230-237).
27. Pettis, C. (2001). TechnoBrands: How to create & use" Brand identity" to market, advertise & sell technology products. Universe.
28. Zick, T. (2007). Clouds, Cameras, and Computers: The First Amendment and Networked Public Places. Fla. L. Rev., 59, 1.
29. Huth, A., &Cebula, J. (2011). The basics of cloud computing. United States Computer
30. Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security? University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.
31. Chaudhary, H., Chaudhary, H., & Sharma, A. K. (2022). Optimized genetic algorithm and extended diffie hellman as an effectual approach for DoS-attack detection in cloud. International Journal of Software Engineering and
32. Computer Systems, 8(1), 69–78.
33. Mijić, M. (2014). Predictive Model of Failures in Cloud Computing (Doctoral dissertation, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu).
34. Khalil, Issa M., Abdallah Khreishah, and Muhammad Azeem. "Cloud computing security: A survey." Computers 3.1 (2014): 1-35.
35. Kumar A, Dutta S, Pranav P. "Prevention of DDoS Attack in Cloud Computing using Fuzzy Q – Learning Algorithm. Research Square"; 2022. DOI: 10.21203/rs.3.rs-1536879/v1.
36. Boopathi, M., Chavan, M., J., J.J. and Kumar, S.N.P. (2022), "An approach for DoS attack detection in cloud computing using sine cosine anti corona virus optimized deep maxout network", International Journal of Pervasive 84Computing and Communications, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJPCC-05-2022-0197
37. Mishra, Narendra, R. K. Singh, και S. K. Yadav. 'Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier'. 2022
38. A. Rangapur, T. Kanakam, and A. Jubilson, "DDoSDet: an approach to Detect DDoS attacks using Neural Networks," 2022.Abusitta,
39. E. S. JeyaJothi, J. Anitha, S. Rani, and B. Tiwari, "A com-prehensile review: computational models for obstructive sleep apnea detection in biomedical applications," BioMed Research International, pp. 1–21, 2022
40. Jin, Z.; Zhang, S.; Hu, Y.;Zhang, Y.; Sun, C. Security State Estimation for Cyber-Physical Systems against DoS Attacks via Reinforcement Learning and Game Theory. Actuators 2022, 11, 192. https://doi.org/10.3390/ act11070192
41. Aldhyani, T.H.H.; Al-kahtani, H. Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detec- tion Systems: Cloud Computing Environments. Sensors 2022, 22, 4685.https://doi.org/10.3390/s22134685
42. A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feedforward based deep neural network model," Expert Systems with Applications, vol. 169, no. December 2020, Article ID 114520, 2021.
43. S. Nandi, S. Phadikar, and K. Majumder, "Detection of DDoS attack and classification using a hybrid approach," in Pro- ceedings of the 2020 >ird ISEA Conference on Security and Privacy (ISEA-ISAP) 2020, pp. 41–47, Guwahati, India, March 2020.
44. J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," Elec- tronics, vol. 9, no. 6, p. 916, 2020.
45. Ishtiaq Ahmed, Sheeraz Ahmed, Asif Nawaz, Sadeeq Jan, Zeeshan Najam, Muneeb Saadat , Rehan Ali Khan,Khalid Za- man,"Towards Securing Cloud Computing from DDoS Attacks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 8, 2020.
46. Ahmed, Ali & Ahmed, Huma."A Proposed Model for Controlling Distributed Denial of Service Attack on Cloud Compting." (2019). 1-4. 10.1109/ICEEST48626.2019.8981709.
47. Mugunthan. 'Soft Computing Based Autonomous Low Rate DDoS Attack Detection and Security for Cloud Computing'. Journal of Soft Computing Paradigm 2019.2 (2019): 80–90.
48. Abusitta, A., Bellaiche, M. &Dagenais, M. An SVM-based framework for detecting DoS attacks in virtualized clouds under changing environment. J Cloud Comp 7, 9 (2018).
49. Mahmodi, Ali &Daneshjoo, Parisa &Delara, Changiz. (2018). Using Genetic Algorithm to Improve Bernoulli Naïve Bayes Algorithm in Order to Detect DDoS Attacks in Cloud Computing Platform.
50. El Mir, Iman &Haqiq, Abdelkrim& Kim, Dan. "Collaborative detection and filtering techniques against denial of service attacks in cloud computing", Journal of Theoretical and Applied Information Technology. 95. 6902 -6914. (2017).
51. El Mir, Iman &Haqiq, Abdelkrim& Kim, Dan. (2017). Collaborative detection and filtering techniques against denial

of service attacks in cloud computing.Journal of Theoretical and Applied Information Technology. 95. 6902 -6914.
52. Reddy, Radha &Bouzefrane, Samia. (2014). Analysis and Detection of DoS Attacks in Cloud Computing by Using QSE Algorithm.10.1109/HPCC.2014.183.
53. Prasanna, Lakshmi &Relangi, Kumar & Krishna Satya Varma, Mantena& Varma, Satya. (2015). Improved MCA Based DoS Attack Detection. International Journal of Science Engineering and Advance Technology.
54. R. Karimazad and A. Faraahi, "An anomaly-based method for DDoS attacks detection using rbf neural networks," in Pro- ceedings of the International Conference on Network and Electronics Engineering,2011, pp. 16–18.
55. Boopathi, M., Chavan, M., J., J.J. and Kumar, S.N.P. (2022), "An approach for DoS attack detection in cloud computing using sine cosine anti coronavirus optimized deep maxout network", International Journal of Pervasive Computing and Communications, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/IJPCC-05-2022-0197
56. Abdul Raoof Wani, Q. P. Rana, & Nitin Pandey. (2020). Machine Learning Solutions for Analysis and Detection of DDoS Attacks in Cloud Computing Environment. International Journal of Engineering and Advanced Technology (IJEAT), 9(3), 2205–2209. https://doi.org/10.35940/ijeat.B3402.029320
57. Mugunthan, S. R. (2019). Soft computing based autonomous low rate DDoS attack detection and security for cloud com- puting. Journal of Soft Computing Paradigm, 1(2), 80-90. doi:10.36548/jscp.2019.2.003
58. S. Emerald, S. E. J., & Nalini, C. (2019). The Classification Model for Cloud DDoS Attack. In International Journal of Inno- vative Technology and Exploring Engineering (Vol. 8, Issue 12, pp. 1261–1264). Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication -BEIESP. https://doi.org/10.35940/ijitee.l3909.1081219
59. Zerina, Mašetić, "SYN flood attack detection in cloud computing using support vector machine." TEM Journal 6.4 (2017): 752.
60. Ms. Supriya,Thakare, and Parminder Kaur. "DoS Attack Detection System Based on Multivariate Correlation Analysis." International Journal of Computer Engineering and Application 11.I.
61. Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A cloud computing-based network monitoring and threat detection system for critical infrastructures. Big Data Research, 3, 10-23
62. Sambangi, Swathi &Lakshmeeswari, Gondi. (2020). A Machine Learning Approach for DDoS (Distributed Denial of Ser- vice) Attack Detection Using Multiple Linear Regression. Proceedings. 63. 51. 10.3390/proceedings2020063051.
63. Khorshed, M. T., Sharma, N. A., Kumar, K., Prasad, M., Ali, A. S., & Xiang, Y. (2015, December). Integrating Internet-of- Things with the power of Cloud Computing and the intelligence of Big Data analytics—A three layered approach. In Com- puter Science and Engineering (APWC on CSE), 2015 2nd Asia-Pacific World Congress on (pp. 1-8).
64. M. T. Khorshed, A. B. Shawkat, and S. A. Wasimi, "Classifying different denial-of-service attacks in cloud computing using rule-based learning," Security and Communication Networks, 2012.
65. Amiri, Fatemeh, et al. "Mutual information-based feature selection for intrusion detection systems." Journal of Network and Computer Applications 34.4 (2011): 1184-1199
66. Amiri, Fatemeh, et al. "Mutual information-based feature selection for intrusion detection systems." Journal of Network and Computer Applications 34.4 (2011): 1184-1199
67. Jansen, W., &Grance, T. (2011). Sp 800-144. Guidelines on security and privacy in public cloud computing.
68. Rittinghouse, J. W., &Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.
69. Padhy, R. P., Patra, M. R., &Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2), 136-146.
70. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73
71. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A.,&Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.
72. Y. Shang, "Prevention and detection of DDoS attack in virtual cloud computing environment using Naive Bayes algorithm of machine learning," Xinyang Agriculture and Forestry University, Department of Information Engineering, Xinyang, Henan, 464000, China, (2024).
73. S. Balasubramaniam, C. V. Joe, T. A. Sivakumar, A. Prasanth, K. S. Kumar, V. Kavitha, and R. K. Dhanaraj, "Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing," Department of Futures Studies, University of Kerala, Tiruvananthapuram, Kerala, India, [2023].