International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 10, October 2025
DOI 10.17148/IMRJR.2025.021006

An Enhanced Strong Security Techniques on Mitigation of DDoS attack in Hybrid Cloud Environment: A Critical Review

M. Lakshmi Priya[1], Dr. E. Helen Parimala[2], M. Janaki[3]

Assistant Professor, Department of Computer Science, Bangalore City College, Bangalore, India[1]

Assistant Professor, Department of Computer Science, Gitam Deemed to be University, Bangalore, India[2]

Senior Assistant Professor, Department of BCA, New Horizon College, Bangalore, India[3]

Abstract: Nowadays, cloud computing is rapidly growing across the IT industry, government sector, and various other domains. Security remains one of the biggest challenges in the cloud. Among the most critical threats is the Distributed Denial of Service (DDoS) attack, which can disrupt secure data communication, generate excessive network traffic, and increase response times. A DDoS attack works by sending a massive number of false or malicious requests to a cloud server, resulting in heavy network congestion. This survey paper examines a range of robust security measures, including hybrid cryptography techniques and machine learning algorithms, aimed at addressing security issues and achieving end-to-end protection in hybrid cloud environments. It also highlights key security challenges and outlines future research directions for mitigating DDoS attacks. The goal is to provide a clear understanding of recent mechanisms and advancements in cybersecurity, serving as a valuable reference for both practitioners and researchers.

Keywords: Intrusion Detection System, Enhanced Cryptography Techniques, Deep Learning Model, Fuzzy Logic, Clustering Techniques

I. INTRODUCTION

Cloud computing provides various internet-based services, such as data storage, infrastructure, and applications. It offers easy and cost-effective access to these services on demand [2,4]. However, major challenges in cloud computing include data privacy, security, reliability, and the availability of data when needed. Cloud security is a critical concern for safeguarding and protecting user data against unauthorized access [5,6]. Network security attacks continue to pose risks to security, privacy, and data availability. Among these, Distributed Denial of Service (DDoS) is a malicious attack that disrupts the delivery of cloud services to users. A DDoS attacker generates excessive network traffic by sending unauthorized or false packets, which depletes network performance, increases security threats, and prolongs response times [1,3]. At the same time, it is very difficult to handle a huge amount of big data after fetching from the various users [19-27]. There is no high security for storing this data on the cloud against DDoS attacks. To counter such attacks, cryptography and deep learning models play a vital role in securing cloud services. Cryptographic techniques make it significantly harder for attackers to breach security measures, thereby helping to mitigate DDoS attacks [7,8].

II. LITERATURE REVIEW

Helen Parimala., [9] developed a Smart Mitigating Service (SMS) architecture for DDoS attack prevention, designed to detect vulnerabilities exploited by malicious users and to achieve end-to-end secure cloud services provided by cloud service providers. The proposed system incorporates a malware detection module that conducts Image CAPTCHA, Text CAPTCHA, and Math CAPTCHA tests. Each test allows up to three attempts to solve the challenge, serving as the first verification process. Following this, the Client Puzzle Server checks the user with a jigsaw puzzle test, also allowing three attempts. This serves as the second verification process. Users who successfully pass the second verification step are recognized as legitimate and granted access to the next security level. The Intrusion Detection and Prevention System (IDPS) employs a binary firefly optimization algorithm to filter traffic, distinguishing between legitimate users and attackers. Additionally, a Reverse Proxy Server conceals server details from users, with authentication handled through the Elliptic Curve Cryptography (ECC) algorithm to further enhance cloud security.

Bhardwaj et al., [10] proposed a novel architecture that combines an AutoEncoder (AE) with a Deep Neural Network (DNN) for the detection and mitigation of Distributed Denial of Service (DDoS) attacks. The AutoEncoder, is an unsupervised machine learning technique, encodes and decodes the input data. The encoded output from the AE is then fed into the DNN, which classifies traffic as either normal (non-attack) or DDoS attack traffic. By processing the encoded data, the DNN ensures secure data transmission within the network. Experimental results showed that memory utilization

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 10, October 2025
DOI 10.17148/IMRJR.2025.021006

and CPU performance improved after mitigating DDoS attacks. The mitigation process is achieved through the combined use of the AE technique and the DNN model.

Ankit Agarwal et al., [11] adopted a deep learning–based mechanism for detecting DDoS attacks in cloud storage applications, thereby ensuring secure cloud services. In their approach, a classification algorithm first distinguishes between sensitive and non-sensitive data. Sensitive data is then encrypted using homomorphic encryption, with the key generated in the first stage. In the second stage, the encrypted data is processed using the *Eval* function, and the resulting ciphertext is stored on the cloud server. In the third stage, the processed information is decrypted using the key to recover the original data, which is then forwarded to the cloud service provider. Experimental analysis demonstrated improved performance in the domain of cloud security.

Verma et al., [12] deployed a cloud secure system to resist DDoS attacks and enhance cloud security. The proposed system consists of three modules: the Log Collection Module, the Log Pre-processing Module, and the Attack Detection Module. The Log Collection Module gathers relevant logs from the web server to detect DDoS activity in the network. The Log Pre-processing Module analyzes the collected data, retrieves attributes from the cloud server, and normalizes them within a defined range for further processing. The Attack Detection Module integrates Teacher Learner-Based Optimization (TLBO) clustering to classify incoming requests as either DDoS attacker traffic or legitimate user traffic, while Principal Component Analysis (PCA) reduces the dataset size to minimize time complexity. This reduction in complexity enables more efficient cloud access. Using this architecture, the system effectively detects DDoS attacks.

P.J. Beslin Pajila., [13] introduced a soft computing–based security method for detecting and mitigating DDoS attacks in wireless sensor networks (WSNs). The approach adopts an ANFIS-based (Adaptive Neuro-Fuzzy Inference System) anchor node protection technique to defend against attacks originating from malicious nodes within a cluster. Fuzzy logic is employed at the cluster head to identify and prevent malicious activity. The ANFIS module, deployed at the anchor node, processes data packets received from the cluster head. Metrics such as packet transfer rate and node energy consumption are used to determine whether a node is malicious. If deemed non-malicious, the anchor node forwards packets to the sink. This approach minimizes energy consumption per node and extends the overall network lifetime.

Raj Kumar Batcha et al., [14] developed a hybrid detection system for mitigating DDoS attacks using a Deep Sparse AutoEncoder, an unsupervised neural network technique that reduces feature dimensionality. A deep learning–based classification mechanism is then applied to distinguish between attack and non-attack traffic, preventing unauthorized access. Experimental results showed improved performance and a significant reduction in security breaches.

Yogesh et al., [15,16] constructs an Intrusion Detection and Prevention System (IDPS) that deploys a Third-Party Auditor (TPA) to protect cloud computing (CC) against Distributed Denial-of-Service (DDoS) attacks. The research methodology is based on the Dempster–Shafer Theory (DST), which provides a secured probabilistic framework under uncertainty. This system executes in three key modules: monitor, conversion, and DDoS attack evaluation. In the monitor module, the Snort detection system is deployed to identify and anomalous traffic, specifically packet flooding. At the conversion module, alerts generated by Snort are converted into the Basic Probability Assignments (BPAs) by the server. In the evaluation module, these BPAs are analyzed using DST's combination rule to assess attack, depending on decision variables. This process obtains a more robust and resilient protection against DDoS attack.

III. IMPORTANCE OF SURVEY RESEARCH STUDY

Case 1: Construct a strong, secure cryptography and deep learning model to eradicate DDoS attacks [17]
Case 2: Prevent network traffic by rejecting unauthorized packets
Case 3: Improve network performance
Case 4: Strengthen cloud security by deploying strong security algorithms [18]
Case 5: Reduce response time
Case 6: Increase packet delivery ratio
Case 7: Reduce false positive ratio
Case 8: Avail Efficient Cloud Access
Case 9: Speed up fast computation
Case 10: Minimum computational cost

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 10, October 2025
DOI 10.17148/IMRJR.2025.021006

Table I. Comparison of Strong Security Techniques: Advantages, and Limitations

Title	Advantage	Limitation
Secured Architecture for mitigation of distributed denial of service attack, integrating internet of things and cloud computing	SMS(Smart Mitigating Service) Secured Architecture is designed to achieve end-to-end cloud security	Various strong security mechanisms need to be used to eradicate DDoS attacks
Detection and Mitigation of cloud based distributed denial of service attacks	Improvements in memory utilization and CPU performance enhance efficient cloud access.	A Standard dataset is not deployed to execute the proposed security method
Detection of DDoS attack using a deep learning model in a cloud storage application	Experimental Analysis revealed better performance in the field of cloud security	A strong secured architecture has not been developed for mitigating DDoS attack
A study on the effects of DDoS attacks on the cloud environment and reduction of collateral damages to Non Targets	Time complexity is minimized to expedite cloud access	No strong security algorithms are deployed to prevent security vulnerabilities
Soft Computing based security methods for the detection and protection of DDoS attacks in the wireless sensor network	Each node utilizes very less energy and enhances the lifetime of the wireless sensor networks	There is no focus on other types of cloud networks
A hybrid detection system for DDoS attacks based on Deep Sparse AutoEncoder and Light Gradient Boost Machine	A hybrid detection system has been proposed for mitigating malicious activities to ensure a secure cloud service	There is a lack of smart security approaches in this research work

IV. CONCLUSION

Cloud Security is the biggest challenge for protecting user data and boosting high security against malicious activities. Cloud Security offers security polices for addressing security threats. A distributed denial of service attack is a major security issue and top priority security concern. This paper presents a comprehensive review of the mitigation of DDoS attacks in the context of cybersecurity, covering the security techniques and challenges. It starts with an overview of security and its growing importance in today's data-driven world. It also reviews strong security techniques such as deep neural network models, homomorphic encryption techniques, fuzzy logic, clustering techniques, and hybrid approaches. Finally, this study outlines promising limitations and future directions for advancing cybersecurity research. Overall, it provides a comprehensive understanding of current security mechanisms and serves as a valuable foundation for further research and development in this field.

V. FUTURE DIRECTIONS

There are several promising future directions for the mitigation of DDoS attacks:

- **Deep Neural Network (DNN) models**: It play a vital role in resisting DDoS attacks by accurately classifying authentic and non-authentic users.
- **Enhanced cryptographic techniques:** It can be leveraged to detect and mitigate network security attacks across various domains of cybersecurity.
- **Fuzzy Logic and clustering techniques:** These techniques help classify malicious nodes and differentiate legitimate nodes from attackers, thereby controlling network traffic and enabling efficient cloud access and services.
- **Hybrid approaches:** These approaches are increasingly being explored to identify, analyze, and prevent security vulnerabilities across sectors such as healthcare, enterprises, and public and private industries.
- **Advanced cryptographic methods:** This methods are being developed to reduce response time, minimize computational costs, and increase the packet delivery ratio.

REFERENCES

[1]. Damai Jessica Prathyusha, Govinda Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using artificial immune system in a cloud environment", Springer Journal, 2020.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 10, October 2025
DOI 10.17148/IMRJR.2025.021006

[2]. Fursan Thabit,"Security analysis and performance evaluation of a new lightweight cryptography algorithm for cloud computing", Elsevier Journal, 2021.
[3]. D.Javaheri, S.Gorgin, JA Lee, M.Masdari, "Fuzzy logic based DDoS attacks and network traffic anomaly detection methods", Elsevier Journal, 315-338, 2023.
[4]. L.Mashimbye, TE Mathonsi, Tshimangadzo, "Security Algorithms to detect and prevent advanced persistent threats in cloud computing", International Conference on Electrical Computer and Energy Technology", IEEE Journal, 1-6,2023.
[5]. Naveed Khan, Zhang Jianbiao, Huhnkuk Lim, Muhammad Salman Pathan, Shehzad Ashraf Chaudhry, "An ECC-based mutual data access control protocol for next-generation public cloud", Journal of Cloud Computing: Advances, Systems and Applications, Volume 12, doi: 10.1186/s13677-023-00464-0, 2023.
[6]. M.lakshmi priya, Dr.S.Albert Rabara, E.Helen Parimala," A Smart Cybergate Authentication for eradicating skimmer attack in ATM-Cloud Environment", Mukt Shabd Journal, ISSN NO : 2347-3150,Volume X, Issue VI, 2021.
[7]. Christila, Sivakumar , "A Deep Ensemble Framework for DDoS Attack Recognition and Mitigation in Cloud SDN Environment", Journal of Computer Science, 1281–1290, 2024.
[8]. Dayal, Srivastava, "An intelligent DDoS defense scheme to combat attacks near attack entry points", Journal of Computer Virology and Hacking Techniques, 819–839, 2024.
[9]. E.Helan Parimala, "Secured Architecture for mitigating distributed denial of service attack integrating internet of things and cloud computing", Shodhganga thesis, Department of Computer Science and Application, Bharathidasan University, Trichy, Tamil Nadu, India, 2021.
[10]. Bhardwaj, Aanshi, "Detection and Mitigation of cloud based distributed denial of service attacks", Shodhganga thesis, university institute of engineering and technology, Panjab university, 2020.
[11]. [11] Ankit Agarwal, Manju Khari, Rajiv Singh, "Detection of DDoS Attack using deep learning model in cloud storage application", Springer Journal, 419-439,2021.
[12]. Verma, Priyanka, "A study on the effects of DDoS attack on cloud environment and reduction of collateral damages to Non Targets", Shodhganga thesis, department of CSS engineering, Vajpayee Indian Institute of Information Technology and Management, Atal Bihari university, 2020.
[13]. P J Beslin Pajila, "Soft computing based security methods for the detection and protection of DDoS attacks in the wireless sensor networks", Shodhganga thesis, department of information and communication engineering, Anna University, India, 2022.
[14]. Raj Kumar Batchu, Hari Seetha, "A hybrid detection system for DDoS attacks based on Deep Sparse AutoEncoder and Light Gradient Boost Machine", Journal of Information and knowledge management, Vol.22, No.01, 2023.
[15]. Yogesh B. Sanap, Pushpalata Aher,"A Comprehensive Survey On Detection And Mitigation Of DDoS Attacks Enabled With Deep Learning Techniques In Cloud Computing",2023 6th International Conference on Advances in Science and Technology (ICAST),DOI: 10.1109/ICAST59062.2023.10454990,IEEE,2024.
[16]. A. Bixapathi, H. Mohammed Ali, R Maranan, Sudhakar AVV, Beschi I S, M. Ramya,"Efficient Detection of DDoS Attacks in E-Government Clouds Using Sparse Neural Networks", IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG),DOI: 10.1109/ICTBIG64922.2024.10911652,2025.
[17]. A. Bixapathi, H. Mohammed Ali, R Maranan, Sudhakar AVV, Beschi I S, M. Ramya,"Efficient Detection of DDoS Attacks in E-Government Clouds Using Sparse Neural Networks", IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), doi: 10.1109/ICTBIG64922.2024.10911652,2025.
[18]. Y.Sunil Raj, Dr.S.Albert Rabara, E.Helen Parimala," Enhanced TPA Based Data Integrity mechanism for object storage architecture on integrated IOT Cloud Smart Environment", Journal of Shanghai University, ISSN-1007-1172,2020.
[19]. A.AngelPreethi, S.B.R. Kumar, "Visualizing Big Data Mining: Issues, Challenges and Opportunities" International Journal of Control Theory and Applications, Volume 9, Issue 27, Pages: 455-460, 2016.
[20]. Mohammad Soleymani, David Garcia, Brendan Jou, Björn Schuller, "A survey of multimodal sentiment analysis", Elsevier, 2017, pp. 1-12.
[21]. A.AngelPreethi, and Dr.S.Britto Ramesh Kumar, "A Dictionary based Approach for improving the accuracy of opinion mining on big data", International Journal of Research and Analytical Reviews (IJRAR), Vol. 5, Issue 4, Oct-Dec 2018, pp- i836-844.
[22]. Imran Khan, S. K. Naqvi, Mansaf Alam, and S. N. A. Rizvi, "An efficient framework for real-time tweet classification", springer, March 2017, pp. 1-7.
[23]. A.AngelPreethi, and Dr.S.Britto Ramesh Kumar, " Dom_Classi: An Enhanced Weighting Mechanism for Domain Specific Words using Frequency based Probability", International Journal of Applied Engineering Research, Vol.14, Issue 1, 2019, pp 140-148
[24]. Angelpreethi, " Fuzzy Based Sentiment Classification Using Fuzzy Linguistic Hedges for Decision Making", Mapana Journal of Sciences,Vol. 22, Special Issue 2, pp 63-79, 2023 DoI:|https://doi.org/10.12723/mjs.sp2.4

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 10, October 2025
DOI 10.17148/IMRJR.2025.021006

[25]. A.AngelPreethi, and Dr.S.Britto Ramesh Kumar, "NIC_LBA: Negations and Intensifier Classification of microblog data using Lexicon Based Approach "Journal of Emerging Technologies and Innovative Research (JETIR), Volume 6, Issue 6 , PP 753-759, June 2019.

[26]. A.AngelPreethi, and Dr.S.Britto Ramesh Kumar, "A methodological framework for opinion mining", International Journal of Computer sciences and Engineering, Vol. 6, special Issue 2, 2018, pp- 6-9.

[27]. A. Angelpreethi and S. B. R. Kumar, "An Enhanced Architecture for Feature Based Opinion Mining from Product Reviews," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 89-92.