International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

An Edge-Driven Secure Backup Framework for Dos-Aware Cloud Storage

Ms. M. Vichithra[1] M.E., Ms. M C. Pradeepa[2], Ms. S. Nisha3, Ms. A. Thabasum[4]

Assistant Professor, Department of CSE, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Student, Department of Computer Science and Engineering, R P Sarathy Institute of Technology, Salem, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: storage,on-demand computation, and global accessibility of services. Organizations Cloud storage systems are widely used forstoring and managing data, but they are vulnerable to security threats such as Denial of Service (DoS) attacks. A DoS attack can overload the server and make cloud services unavailable to users. This project proposes an edge-driven secure backup system for DoS-aware cloud storage to improve data availability and security. The system creates a cloud environment that runs through a web interface using technologies such as Python, HTML, CSS, and JavaScript, with WAMP Server used for local server deployment. The system is accessed through a web browser like Google Chrome. To ensure data safety during DoS attacks, Resilio Store is used to automatically create secure backups of stored data. The project also simulates DoS attacks with different intensity levels to test the system's resilience. When a DoS attack is detected, the system sends an SMS notification to the cloud service provider for immediate awareness and response. The proposed system helps maintain data availability, improves security against DoS attacks, and ensures reliable backup through edge-based mechanisms.

KEYWORDS: Cloud Storage, DoS Attack Detection, Edge Computing, Secure Backup System, Resilio Sync, Data Availability, Cloud Security, Web-based Cloud Environment.

I. INTRODUCTION

Cloud computing has become the backbone of modern digital infrastructure, enabling scalable increasingly rely on cloud platforms such as Amazon Web Services to host applications and store critical data. To address this issue, an edge-driven secure backup system for DoS-aware cloud storage is proposed. The system creates a cloud-like environment using web technologies such as Python, HTML, CSS, and JavaScript, deployed through WAMP Server and accessed using a web browser. The proposed system monitors server activity and simulates DoS attacks with varying levels of intensity to analyze system behavior.

A DDoS attack floods a target server with excessive traffic from multiple distributed sources, leading to increased CPU utilization, abnormal bandwidth consumption, high request rates, and eventual service failure. Traditional cloud-based defense mechanisms rely primarily on centralized filtering and provider-level mitigation. However, during large-scale attacks, even cloud infrastructures may experience performance degradation, affecting data accessibility. Moreover, conventional detection systems often depend on static threshold-based rules, which may fail to adapt to dynamic traffic patterns and result in high false positives or delayed detection.

To address these limitations, intelligent traffic analysis and machine learning-based detection mechanisms have gained significant attention. In particular, the Random Forest algorithm offers robust classification capabilities by constructing multiple decision trees and aggregating their outputs, thereby improving accuracy and resilience against noisy traffic data. By analyzing IP behavior, packet rate, request frequency, and system health metrics, traffic can be classified as either normal or malicious in real time. Such adaptive detection enhances early identification of DoS attacks before complete service disruption occurs.

In addition to detection and mitigation, ensuring data availability during attack scenarios is equally critical. Relying solely on centralized cloud storage may result in temporary inaccessibility when servers are overloaded. Therefore, integrating edge-based backup mechanisms such as ResilioStore provides an additional layer of resilience. In the proposed system, encrypted converted into ISO-9660/UDF replica images and synchronized to an edge device using

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

Resilio-based peer-to-peer synchronization. This hybrid cloud–edge approach ensures that even if cloud instances become temporarily unavailable due to DoS attacks, backup data remains accessible locally.

Furthermore, automated mitigation strategies such as IP blocking, rate limiting, traffic filtering, and request redirection are implemented once malicious activity is detected. The system also includes an automated SMS alert mechanism to notify administrators and users about attack occurrence, server status, and applied countermeasures. This improves transparency, enables rapid response, and enhances trust in the system.

By combining machine learning-based DoS detection, Cloud infrastructure, ISO-based secure backup, ResilioStore edge synchronization, and automated alert notification, the proposed framework provides a comprehensive solution for secure, resilient, and highly available cloud data storage. The integration of intelligent detection and edge-assisted recovery significantly reduces downtime and strengthens overall cloud security architecture.

II. LITERATURE SURVEY

Cloud storage security and disaster recovery have been widely studied in recent years due to the increasing dependence on cloud infrastructures for storing critical data. Several research works have proposed different architectures and mechanisms to improve data availability, reliability, and security in cloud and edge environments.

[1] Wenchao Li et al. (2025) proposed a multi-cloud management architecture with intelligent disaster recovery strategies to improve high availability of cloud services. Their framework integrates cross-cloud resource management and automated failover mechanisms using intelligent scheduling and consensus algorithms such as PBFT. The system achieves very low recovery time objectives (RTO) and strong service availability. However, the architecture introduces high system complexity and significant computational overhead due to blockchain-based coordination.

Another important contribution was presented by

[2] Ferrucci et al. (2024), who proposed a decentralized replica management mechanism for edge environments. Their approach dynamically places service replicas at edge nodes based on marginal-cost optimization and latency constraints. This approach helps reduce resource consumption while maintaining service performance. Although the method improves scalability and resource utilization, it becomes difficult to optimize in highly dynamic network environments.

Similarly,

[3] Junqi Chen et al. (2023) introduced a secure cloud–edge collaborative storage scheme that combines hierarchical storage architecture with privacy-preserving coding techniques. Their system uses erasure coding and optimized data routing to provide improved fault tolerance and privacy protection. While the approach offers strong reliability and reduced write latency, it requires higher computational resources and introduces additional control overhead.

Another related work by

[4] Mohammed Abuibaid et al. (2022) proposed a workload monitoring and failover mechanism for edge computing systems. The system uses health-check monitoring and Kubernetes-based scheduling to automatically redirect workloads when failures occur. Experimental results showed improved service continuity in distributed environments. However, the recovery performance remains dependent on network conditions and hardware capabilities.

In addition, [5] Reda Maher and Omar Nasr (2021) developed DropStore, a secure backup framework that integrates fog computing and multi-cloud storage. In this approach, a fog node called a “Droplet” manages encrypted backups across multiple cloud providers. This architecture enhances privacy protection and avoids vendor lock-in problems. However, the solution requires additional hardware resources and increases infrastructure cost.it is evident that existing research focuses on improving cloud reliability through multi-cloud architectures, replication strategies, edge computing, and encryption mechanisms. However, many of these solutions still rely heavily on centralized cloud infrastructures and lack efficient edge-level backup and fast recovery mechanisms during large-scale DDoS attacks. Therefore, there is a need for a secure, edge-driven backup system that ensures fast recovery and improved data confidentiality during cloud service disruptions.

III. EXISTING SYSTEM

Current cloud storage systems rely primarily on provider-managed redundancy and replication to ensure data durability. Major cloud service providers, including AWS, manage multiple copies of data across distributed data centers and utilize snapshot-based backups, RAID configurations, and secondary sites to handle failures. While these mechanisms provide fault tolerance against hardware failures and certain disruptions, they are generally reactive rather than proactive in addressing volumetric attacks like DoS, which target availability rather than physical component failure.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

Traditional DoS defenses implemented by cloud providers often employ static rules, volume thresholds, and provider-side scrubbing, which may succeed against known attack vectors but struggle with low-and-slow or evolving attack patterns. These methods lack adaptive threat classification and generally do not provide early warnings to end users. Furthermore, existing backups are often stored in centralized cloud storage without offline or edge replication, creating a single point of dependency. When a DoS attack significantly impacts service availability, users may experience delayed access or complete unavailability until the service is restored.

Another limitation is the absence of machine learning-based traffic analysis in many existing systems. Most commercial offerings do not integrate model-based classification to distinguish between normal and malicious traffic in real time, leading to higher false positive rates and slower reaction times. Moreover, while cloud providers offer integrated alerting services, these are typically tied to internal thresholds and do not incorporate intelligent attack classification or provide context-rich notifications.

Importantly, current systems rarely integrate edge-level backups that can serve as alternative access points during large-scale attacks. As a result, users remain dependent on the cloud provider's infrastructure for both live access and recovery, which increases service downtime and reduces control over backup data. These limitations motivate the need for a system that combines machine learning-based DDoS detection, automated mitigation, encrypted backup replication, and edge-assisted recovery — enabling faster response, enhanced availability, and improved user transparency during attack incidents.

PROPOSED SYSTEM

The proposed system presents an edge-driven secure backup framework for DDoS-aware cloud storage that improves data availability and security during cloud service failures. In this system, users upload files to the cloud through a web-based interface which runs on a WAMP server environment. Before storing the files in the cloud, the data is encrypted using the PGP encryption algorithm to ensure confidentiality and protect sensitive information from unauthorized access.

To enhance reliability, the system generates ISO-based backup replicas of the encrypted cloud data. These backup images are synchronized with an edge storage device called ResilioStore, which maintains a secure backup copy outside the primary cloud infrastructure. The system continuously monitors cloud server activity to detect abnormal traffic patterns that may indicate a Denial of Service (DoS) attack.

When a DoS attack or server failure occurs, the system automatically redirects user requests to the edge backup system. The stored ISO image is mounted in a recovery node, allowing encrypted files to be retrieved and delivered to users without interruption. Additionally, the system sends SMS notifications to the cloud provider to alert them about the detected attack. This approach ensures secure data storage, rapid backup recovery, and continuous service availability even during network attacks.

IV. IMPLEMENTATION

1. SYSTEM DESIGN

The proposed system is designed as an edge-driven secure backup architecture for DoS-aware cloud storage. The system integrates cloud storage infrastructure, encryption mechanisms, and edge backup devices to ensure continuous data availability during cyberattacks or cloud failures. The architecture consists of three primary layers:

- Client Layer
- Cloud Layer
- Edge Backup Layer

Client Layer

The client layer includes the data owner and data users who interact with the cloud system through a web interface. The data owner uploads files to the cloud after encrypting them using the PGP encryption algorithm, ensuring that only encrypted data is stored in the cloud environment. Data users request files from the cloud and decrypt them locally using their private keys.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

Cloud Layer
The cloud layer acts as the central storage and management infrastructure. It handles user authentication, encrypted file storage, metadata management, ISO backup creation, and synchronization with the edge storage system. The cloud server continuously monitors system health and detects abnormal traffic patterns that may indicate a DDoS attack or service failure.

Edge Backup Layer
The edge layer consists of a ResilioStore backup device deployed at the data owner's location. This device stores synchronized ISO replicas of encrypted cloud data. When the cloud system becomes unavailable due to attacks or failures, the system redirects user requests to the edge storage device to ensure continuous service availability.

V. SYSTEM COMPONENTS

The proposed system consists of several key components that work together to provide secure cloud backup and recovery.

Cloud Service Provider Interface
The cloud service provider (CSP) interface acts as the main platform through which users interact with the cloud system. It is implemented using a web-based interface built with Python, HTML, CSS, and JavaScript. The interface provides functionalities such as:

- User authentication and login
- File upload and storage
- Data access requests
- Backup status monitoring
- Recovery management

The CSP interface also manages communication between the cloud server, edge storage system, and end users.

PGP Encryption Module
The encryption module ensures the confidentiality of stored data. Before uploading files to the cloud, the data owner encrypts them using the PGP encryption algorithm.

- Public–private key pair generation
- File encryption before cloud upload
- Secure key management
- Digital signature validation
- Client-side decryption after recovery

Cloud Replica Vault
The cloud replica vault is responsible for securely storing encrypted files and generating backup replicas.
This module includes:

- Encrypted Storage Handler: stores encrypted files
- MetadataController: manages file ownership and access permissions
- ISO Image Generator: creates full backup replicas using ISO-9660/UDF

ResilioStore Edge Backup Device
The ResilioStore edge device provides an additional backup layer outside the cloud infrastructure. It stores synchronized ISO replicas of encrypted data.

- Receiving ISO backup replicas from the cloud
- Maintaining secure storage of backup images
- Providing recovery access during cloud failures
- Transferring ISO images to backup cloud nodes during DDoS events

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

Dos-Aware Request Routing Module

This module monitors cloud service health and automatically redirects requests during failures.

- Monitoring server availability
- Detecting abnormal traffic spikes
- Identifying potential DDoS attacks
- Redirecting user requests to the edge backup system

VI. HARDWARE REQUIREMENTS

The system requires moderate computing resources to support encryption operations, cloud storage management, and backup synchronization.

- Processor: Intel i5 / AMD Ryzen 5 or higher
- RAM:16 GB
- Storage: 512 GB SSD
- Network: High-speed internet connection
- Edge Device: ResilioStore storage device

High-performance hardware improves encryption speed, backup generation, and recovery operations.

VII. SOFTWARE REQUIREMENTS

The proposed system is implemented using open-source technologies and web development frameworks.

- Software: Python 3.10+
- Flask Framework
- HTML5 / CSS3 / JavaScript
- WAMP Server
- MySQL
- PGP Library
- Resilio Sync.

VIII. DETECTION AND MITIGATION PROCESS

The detection and mitigation process plays a crucial role in ensuring the reliability and availability of the proposed cloud storage system during Denial of Service (DoS) attacks or unexpected cloud service failures. In cloud environments, DoS attacks attempt to overwhelm servers by generating a large number of malicious requests, which can significantly degrade system performance or completely disrupt service availability. To address this challenge, the proposed framework incorporates a continuous monitoring mechanism that observes multiple system performance parameters in order to identify abnormal behavior and detect potential attacks at an early stage. The monitoring system analyzes key indicators such as server response time, network latency, request processing rate, storage responsiveness, and API error frequency. Under normal operating conditions, these parameters remain within predefined thresholds; however, when abnormal traffic patterns or excessive request volumes are detected, the system interprets this behavior as a potential attack or service outage.

Once the monitoring module identifies a potential failure condition, the system automatically activates the mitigation mechanism to maintain service continuity. The first step in the mitigation process involves verifying the availability of the primary cloud server and confirming that the service disruption is not caused by temporary network fluctuations. If the system determines that the cloud server is experiencing significant degradation or has become unavailable due to a DDoS attack, the recovery mode is triggered. During this stage, the request routing module dynamically redirects incoming user requests away from the compromised cloud server and toward the ResilioStore edge backup system. This intelligent routing mechanism ensures that users can continue accessing their data even when the main cloud infrastructure is under attack.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

In addition to request redirection, the mitigation mechanism activates backup cloud resources to support recovery operations. The ResilioStore edge device transfers the required ISO backup image to an available backup cloud node where it can be mounted and accessed. The backup node then retrieves the requested encrypted files from the mounted ISO image and securely delivers them to the user. By combining early attack detection, adaptive request routing, and edge-assisted recovery, the proposed mitigation framework significantly reduces system downtime and prevents service disruption during DDoS attacks. This integrated detection and mitigation strategy enhances the overall resilience of the cloud storage system while maintaining secure and uninterrupted data access for authorized users.

If: CPU < Threshold, Request rate within normal range, No abnormal traffic spikes (State = Normal)
If: CPU ≥ Threshold OR Sudden spike in request rate OR Abnormal packet distribution (State = Malicious (DoS Attack))

IX. BACKUP AND RECOVERY PROCESS

The backup and recovery mechanism is a critical component of the proposed edge-driven secure cloud storage framework, designed to ensure continuous data availability during Denial of Service (DoS) attacks or cloud infrastructure failures. The system employs a multi-stage process that integrates encryption, ISO-based replication, and edge storage synchronization to protect sensitive information and enable rapid restoration of services. In the proposed architecture, the backup process begins at the data owner's side, where files are first encrypted using the Pretty Good Privacy (PGP) encryption algorithm before being uploaded to the cloud environment. Encrypting the data prior to transmission ensures that only ciphertext is stored in the cloud, thereby protecting sensitive information from unauthorized access or data leakage. Once the encrypted files are uploaded, the cloud server stores them in a secure storage environment while maintaining associated metadata such as ownership information, access permissions, and file integrity hashes.

To support efficient disaster recovery, the cloud system periodically aggregates encrypted files and generates a complete backup replica in the form of an ISO image using the ISO-9660/UDF file system format. This ISO-based replication method allows the backup to be stored as a structured, mountable disk image that preserves directory hierarchy and file integrity. The generated ISO backup image is then synchronized with an edge storage device known as ResilioStore, which is deployed at the data owner's location. ResilioStore functions as an independent backup repository and continuously maintains updated replicas of encrypted cloud data. By maintaining a local copy of the backup image outside the cloud infrastructure, the system ensures that data recovery can still occur even if the primary cloud server becomes unavailable.

During normal operation, user requests are processed directly by the cloud server. However, when the system detects a DoS attack or service failure, the recovery mechanism is automatically activated. In such scenarios, user requests are redirected to the ResilioStore edge device, which contains the synchronized ISO backup replica. Due to the limited computational resources of edge devices, the required ISO image is transferred from ResilioStore to a backup cloud node where it can be mounted using ISO-9660/UDF mounting procedures. After mounting the ISO image, the system extracts the requested encrypted file and securely delivers it to the requesting user. Since the files remain encrypted throughout the entire recovery process, the system ensures that sensitive information is never exposed within the cloud infrastructure. Finally, the user decrypts the retrieved file locally using their private PGP key, restoring the original data in a secure environment. This end-to-end recovery approach significantly reduces service downtime, improves system resilience during cyberattacks, and guarantees secure data restoration without compromising confidentiality.

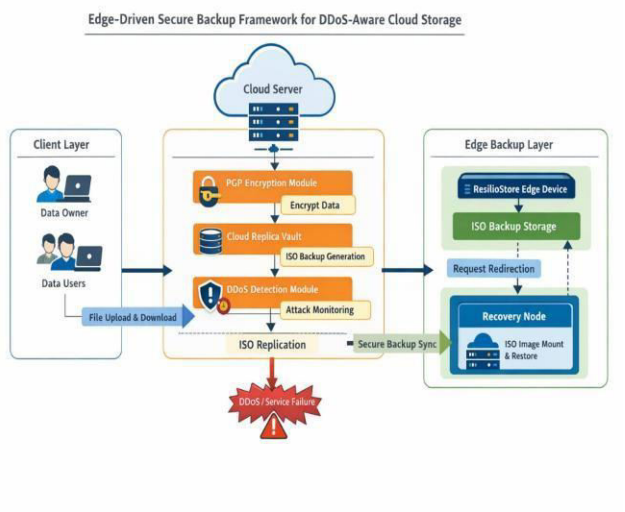
International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

X. DIAGRAMATIC REPRESENTION



TESTING AND ASSURENCE

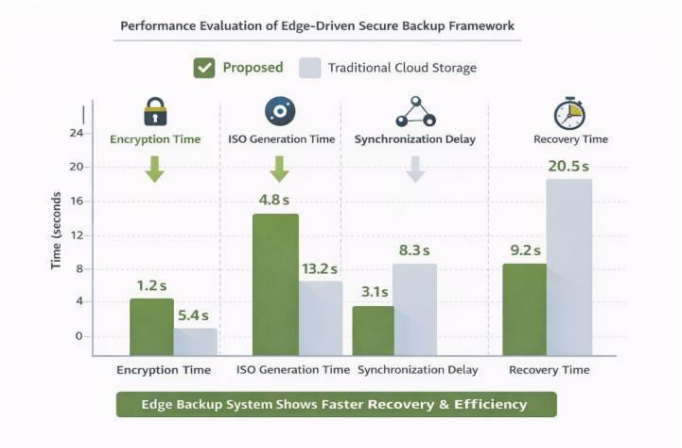
Testing and quality assurance are essential stages in the development of the proposed edge-driven secure backup framework. The proposed system undergoes multiple levels of testing to validate the functionality, security, performance, and integration of all system components.

Functional testing is conducted to verify that all modules of the system operate according to their intended design. This includes testing user registration and authentication, encryption and upload of files by the data owner.The results of these tests confirm that the core functionalities of the system perform correctly without errors.

Security testing is performed to ensure that sensitive data remains protected throughout the entire storage and recovery lifecycle. Since the proposed system relies on the PGP encryption algorithm for data protection, security testing verifies the correctness of key generation, encryption processes, and client-side decryption mechanisms.
Failure and recovery testing are conducted to simulate real-world cloud failure scenarios, including DoS attacks and cloud service outages. The successful completion of this process confirms the reliability of the recovery mechanism and demonstrates the system's ability to maintain service continuity during cloud failures.

Performance testing is also conducted to evaluate the efficiency of the proposed system under varying workloads The results show that the integration of edge-based backup significantly reduces recovery time compared to traditional cloud-only backup systems.

Integration testing is performed to ensure smooth interaction among different system modules and technologies used in the framework.The successful results confirm that the system operates as a cohesive platform capable of delivering secure cloud backup and reliable recovery during DDoS attacks.



|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

XI. RESULT

The proposed edge-driven secure backup framework for DoS-aware cloud storage was implemented and tested in a controlled cloud simulation environment to evaluate its performance, security, and recovery capabilities. The system was developed using Python for backend processing, HTML, CSS, and JavaScript for the user interface, and MySQL for database management. The application was deployed using a WAMP server environment, and ResilioStore was used as the edge backup storage device. The evaluation focused on measuring the system's ability to securely store encrypted data, generate ISO-based backup replicas, detect cloud failures, and recover data efficiently during Denial of Service (DoS) attack scenarios.

XII. CONCLUSION

This paper presented a DDoS-aware secure cloud storage and backup framework that integrates intelligent traffic analysis, automated mitigation, and edge-assisted recovery. The system encrypts user data using the PGP algorithm before storing it in the cloud and creates ISO-based backup replicas that are synchronized with an edge storage device using ResilioStore. During a DDoS attack or server failure, the system redirects requests to the edge backup to ensure continuous data access and recovery. Experimental results demonstrate that the proposed system enhances data security, reduces recovery time, and improves reliability compared to traditional cloud storage systems. FUTURE

XIII. ENHANCEMENTS

In future work, the system can be enhanced by integrating machine learning techniques for early detection and prediction of DDoS attacks. The framework can also be extended to support multi-cloud backup environments to further improve data availability and fault tolerance. Additionally, implementing data deduplication and blockchain-based integrity verification can reduce storage overhead and enhance data security. These improvements will make the system more scalable, efficient, and secure for large-scale cloud applications.

Upon detection of malicious traffic, automated mitigation mechanisms such as IP blocking, rate limiting, and traffic filtering were activated, and alert notifications were sent to administrators. Furthermore, ISO-9660/UDF backup replicas synchronized to an edge storage node via Resilio Sync ensured data availability even during severe service disruption. The integration of machine learning–based detection with cloud–edge backup significantly enhances system resilience, reduces downtime, and strengthens data security against DDoS attacks.

XIV. ACKNOWLEDGEMENT

We would like to express their sincere gratitude to the faculty members and project supervisors of the Department of Computer Science and Engineering for their valuable guidance, continuous encouragement, and constructive suggestions throughout the development of this project titled "Edge-Driven Secure Backup Framework for DDoS-Aware Cloud Storage." Their support and technical insights greatly contributed to the successful completion of this work.We also extend our thanks to the institution for providing the necessary facilities, software resources, and computing infrastructure required for implementing and testing the proposed system. Special appreciation is given to colleagues and peers who provided helpful feedback and participated in testing the system during different stages of development. Their suggestions helped improve the reliability and performance of the proposed framework.

Finally, we acknowledge the contributions of researchers and developers whose previous work in cloud computing, edge computing, and data security provided a strong foundation for the research presented in this paper.

REFERENNCES

1. J. Fu, Y. Liu, H. Chao, B.K. Bhargava, Z. Zhang, Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing, IEEE Trans. Ind. Inf. 14 (10) (2018) 4519–4528.
2. S. K. Monga, S. K. Ramachandra, and Y. Simmhan, ``ElfStore: A resilient data storage service for federated edge and fog resources," in Proc. IEEE Int. Conf. Web Services (ICWS), Jul. 2019, pp. 336 345.
3. R. Mayer, H. Gupta, E. Saurez, and U. Ramachandran, ``FogStore: Toward a distributed data store for fog computing," in Proc. IEEE Fog World Congr. (FWC), Oct. 2017, pp. 1- 6.
4. O. A. Nasr, Y. Amer, and M. AboBakr, ``The, `droplet': A new personal device to enable fog computing," in Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC), Apr. 2018, pp. 93-99.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

5. OpenPGP. Accessed: Nov. 15, 2020. [Online]. Available: https://www.openpgp.org, A.W., 2014. Data mining and complex networks algorithms for traffic accident analysis. In: Transportation Research Board 93rd Annual Meeting (No. 14-4172).
6. H. Almubark, H. Al-Raweshidy, and A. Jedidi, "Edge Computing Security: Overview and Challenges,"Springer,2024 https://link.springer.com/chapter/10.1007/978-3-031-62102-4_5
7. A. Behal, A. Chaturvedi, and R. P. Yadav, "Defense mechanisms against DDoS attacks in cloud computing: State-of-the-art and research challenges," IEEE Access, vol. 9, pp. 59870–59893, 2021.
8. Wenchao Li et al.,"Multi-Cloud Management Architecture Design and Disaster Recovery Strategy for High Availability," 2025. https://ieeexplore.ieee.org
9. S. Varma Songa and G. Reddy Karri, "An integrated SDN framework for early detection of DDoS attacks in cloud computing," J. Cloud Comput., vol. 13, art. 64,https://doi.org/10.1186/s13677-024-00625-9 2024.
10. S. Satpathy, U. Tripathy, and P. K. Swain, "Cloud-based DDoS detection using hybrid feature selection with deep reinforcement learning (DRL),"Sci. Rep.,vol. 15, art.36546, https://www.nature.com/articles/s41598-025 18857-3 2025.
11. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
12. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
13. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
14. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
15. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
16. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
17. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
18. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
19. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
20. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
21. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
22. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
23. S. Kansal, "Mitigating DDoS threats in cloud environments: A survey of vulnerabilities and AI based defense strategies," Int. J. Sci. Res. Comput Sci. Eng. Inf. Technol., vol. 11, no. 1, pp. 3208 3214,Feb.2025. https://doi.org/10.32628/CSEIT251112355
24. Anand, L., Maurya, M., Seetha, J., Nagaraju, D., Ravuri, A., & Vidhya, R. G. (2023, July). An intelligent approach to segment the liver cancer using Machine Learning Method. In 2023 4th international conference on electronics and sustainable communication systems (ICESC) (pp. 1488-1493). IEEE.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

25. Rajendran, S., Sundarapandi, A. M. S., Krishnamurthy, A., & Thanarajan, T. (2022). An intelligent face recognition technology for iot-based smart city application using condition-cnn with foraging learning pso model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), 2256018.
26. Murugeshwari, B., & Sujatha, R. (2014). Preservation of Privacy for Multiparty Computation System with Homomorphic Encryption. International Journal of Emerging Technology and Advanced Engineering, 4(3), 530-535.
27. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
28. Samrat, B., Thomas, P. K., Kumar, S., Benila, A., Bhardwaj, R., & Vigenesh, M. (2024, December). Industrial informatics in optimizing software-defined vehicles for logistics. In 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP) (pp. 1-9). IEEE.
29. Soundappan, S. J. (2024). AI-driven customer intelligence in enterprise lakehouse systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology.
30. Rajasekar, M. (2024). AI-Powered Cyber-Secure Federated Learning on AWS for Next-Generation Digital Banking Analytics. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(3).
31. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
32. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
33. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, & Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
34. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications Vol. 9, 36-43.
35. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., & Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
36. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
37. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
38. Jagadeesh, S., & Sugumar, R. (2017). A comparative study on artificial bee colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243–248.
39. Murugeshwari, B., Sarukesi, K., & Jayakumar, C. (2010, March). An efficient method for knowledge hiding through database extension. In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (pp. 342-344). IEEE.
40. Reddy, K. V. V. K., & Vimal, V. R. (2024, July). A novel approach on improved segmentation and classification of remote sensing images using AlexNet compared over linear discriminant analysis with improved accuracy. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.
41. Gowthami, D., & Vigenesh, M. (2024). Distributed and Lightweight Intrusion Detection for IoT: A Lightweight Pyramidal U-Net With Tri-Level Dual Inception-Based Framework. In The Convergence of Self-Sustaining Systems With AI and IoT (pp. 154-173). IGI Global Scientific Publishing.
42. Anand, P. V., & Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
43. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
44. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802406

45. Poornima, G., & Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.
46. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
47. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
48. Vekariya, V., Kumar, S., & Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
49. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
50. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
51. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338–356.
52. Mathew, A. (2025). Ahead of the breach: Predictive threat intelligence in aviation inspired by Scattered Spider attacks. Multidisciplinary International Journal of Research and Development (MIJRD), 4(6), 54–58.
53. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
54. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
55. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
56. Kumar, A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems (TIIS), 19(11), 3841-3855.
57. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
58. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma⁴, S. (2024, October). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor. In Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2: ICDSMLA 2023, 15–16 December, Hyderabad, India (Vol. 2, p. 433). Springer Nature.