



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

Enhanced Disaster Recovery in Cloud Environment using Fog-Based Secure Backup Solution

Deva VN¹, Harihara Sudhan S², Balaarun R³, Shivas A⁴ S. Elamathi⁵

UG Student, Dept. of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology,
Nagapattinam, India¹⁻⁴

Assistant Professor, Dept. of Computer Science Engineering, Sir Issac Newton College of Engineering and
Technology, Nagapattinam, India⁵

ABSTRACT: This project introduces a disaster recovery system that uses fog computing to store data closer to users, reducing delay and improving speed. It ensures secure, encrypted backups and fast recovery during system failures. Compared to traditional cloud backups, it offers better performance, reliability, and uptime.

KEYWORDS: Fog Computing, Disaster Recovery, Backup-as-a-Service (BaaS), FogDrive, FogStore, Data Compression, AES Encryption, OpenPGP, Real-time Data Backup, Edge Computing, Cloud Integration, Secure Storage, Low Latency, High Availability, System Resilience.

I. INTRODUCTION

In today's fast-paced digital world, ensuring data safety and availability during disasters has become a top priority for organizations. Traditional cloud-based backup systems are widely used but often struggle with high latency, centralized failures, and increased bandwidth consumption—especially during large-scale recovery operations. This project introduces a fog-based disaster recovery solution called **FogSecure Backup**, designed to overcome these limitations by decentralizing backup processes. The system uses fog computing to store compressed and encrypted data at edge nodes, closer to the source, reducing latency and improving recovery speed. It integrates two core components: **FogDrive** for local encryption and **FogStore** for secure, distributed backup. By using strong encryption standards like AES and OpenPGP, the system ensures data privacy and reliability. This solution is ideal for environments such as IoT, enterprise IT, and healthcare, where real-time recovery is essential.

II. PROPOSED METHODOLOGY

The FogSecure Backup system is designed using a fog–cloud hybrid architecture. It consists of multiple functional blocks: **Data Acquisition**, **Fog Node Processing (FogDrive)**, **Distributed Backup Storage (FogStore)**, **Optional Cloud Synchronization**, and a **Dashboard Interface** for monitoring and access control.

A. Fog Node Data Processing (FogDrive)

FogDrive is responsible for handling data preprocessing at the edge. This includes:

- Identifying critical data for backup
- Compressing data using zlib
- Encrypting data with AES-256 and OpenPGP
- Triggering backups based on time or event-driven schedules

These steps ensure that sensitive data is securely processed before being transmitted or stored.

Process	Tools/Methods	Purpose	Location
Data Identification	File Watchers / Rules	Tag important files	Edge Node
Compression	zlib (Python)	Reduce Storage Space	FogDrive
Encryption	AES-256 OpenPGP	Ensure data confidentiality	FogDrive
Scheduling	Cron/Daemon Scripts	Automate backup triggers	FogDrive

B. Distributed Storage and Recovery (FogStore)

FogStore acts as a decentralized Backup-as-a-Service (BaaS) layer. It manages encrypted backups with redundancy and rapid recovery capabilities.

Component	Function	Technology Used
Distributed Storage	Store encrypted backups redundantly	MySQL, Docker
Recovery Manager	Restore latest available data quickly	Python, REST API
Integrity Checker	Ensure consistency and data health	Hashing Algorithms

C. Cloud Sync and Dashboard Interface

The optional cloud sync module sends backups to platforms like AWS or DigitalOcean for long-term retention. A Flask-based web dashboard provides administrators with real-time control over backup processes and system status.

Feature	Tool Used	Purpose
Monitoring Dashboard	Flask Web Framework	Visualize system activity and node health
Access Control	Role-Based Login System	Ensure secure access to admin/user roles
Cloud Backup Integration	AWS S3 / DigitalOcean API	Provide cloud redundancy and archiving

III. RESULTS AND PERFORMANCE EVALUATION

To validate the effectiveness of the FogSecure Backup system, a series of tests were conducted comparing it against a traditional cloud-only backup solution. Key performance metrics such as latency, backup speed, system uptime, and security were analyzed. The tests were carried out in a controlled environment using edge devices and a local cloud emulator setup.

A. Performance Comparison

Metric	Cloud-Only Backup	FogSecure Backup	Improvement
Latency	10–15 seconds	6–9 seconds	↓ 30–40%
Backup Speed	200 MB/min	250 MB/min	↑ 25%
Encryption Success	95% (in peak loads)	100%	↑ Full reliability
Storage Efficiency	Moderate (with overhead)	High (with compression)	↑ 15% better usage
System Uptime	97% (downtime during sync)	99.9%	↑ Resilience with fog
Scalability	Limited bandwidth	Scales with edge nodes	↑ Linear scaling

B. Observations

- **Latency Reduction:** Since data is processed and stored closer to the source, fog-based storage significantly reduces the time needed for both backup and restoration.
- **Speed & Throughput:** Fog nodes reduce congestion on the cloud channel, enabling faster backups without saturating internet bandwidth.
- **Security & Integrity:** All test scenarios maintained 100% data encryption success, and no unauthorized access was detected.
- **Redundancy & Availability:** The use of distributed fog nodes ensured that backup services remained available even during network failures.
- **Compression Efficiency:** On average, FogSecure reduced file sizes by 15–20% without data loss, saving storage space.

C. Testing Environment

- **Hardware Used:** Raspberry Pi 4 (fog node), Intel Core i5 system (cloud simulation), 8GB RAM
- **Software Stack:** Python (zlib, gnupg), Flask, MySQL, Docker
- **Testing Tools:** Custom Python benchmarking scripts for latency and throughput, Flask admin dashboard for monitoring

IV. CONCLUSION AND FUTURE ENHANCEMENTS

This paper presented **FogSecure Backup**, a fog–cloud hybrid disaster recovery framework designed to overcome the limitations of traditional cloud-only backup systems. By leveraging the distributed nature of fog computing, the proposed system reduces latency, enhances backup speed, and ensures data security through advanced encryption techniques such as AES and OpenPGP.

The system successfully integrates **FogDrive** for localized data preprocessing and **FogStore** for distributed encrypted storage, providing a scalable and fault-tolerant backup-as-a-service (BaaS) model. Experimental results demonstrate significant improvements in performance metrics, including reduced latency, increased system uptime, and improved storage efficiency. The use of a web-based dashboard further simplifies monitoring and access control, making the system user-friendly and easy to manage.

Despite its advantages, the current implementation can be further enhanced in future iterations. Potential improvements include:

- **Integration of AI and machine learning** for predictive backup scheduling and failure detection.
- **Blockchain-based audit logs** to increase transparency and traceability in data operations.
- **Dynamic node allocation** for better load balancing across fog nodes.
- **Support for mobile and lightweight edge devices**, increasing deployment flexibility.
- **Enhanced compliance features** to meet data protection regulations such as GDPR and HIPAA.

In conclusion, FogSecure Backup offers a reliable, secure, and efficient solution for modern disaster recovery needs, especially in latency-sensitive and real-time environments like IoT, healthcare, finance, and smart cities.

VI. ACKNOWLEDGMENT

The authors would like to express their heartfelt gratitude to the **Department of Computer Science and Engineering** at **Sir Issac Newton College of Engineering and Technology**, Nagapattinam, for providing the necessary infrastructure, guidance, and support throughout the duration of this project.

We extend our sincere thanks to our project guide, **Mrs. ELAMATHIS**, Assistant Professor, for her continuous encouragement, technical expertise, and constructive feedback. Her mentorship played a vital role in shaping this research work and ensuring its successful completion.

We also acknowledge the valuable support of our faculty members, lab technicians, and peers, whose assistance during testing and implementation helped improve the system's performance and practical relevance.

REFERENCES

1. M. Aazam, S. Zeadally, and K. A. Harras, "Fog Computing Architecture, Evaluation, and Future Research Directions," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46–52, 2018.
2. K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Fog Computing: A Taxonomy, Survey and Future Directions," *Future Generation Computer Systems*, vol. 82, pp. 389–411, 2018.
3. M. Satyanarayanan et al., "The Emergence of Edge Computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.
4. S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in *Proceedings of the 2015 Workshop on Mobile Big Data (Mobidata '15)*, pp. 37–42, 2015.
5. H. Abualkishik et al., "A Comparative Study on Disaster Recovery Techniques in Cloud Computing," *IEEE Access*, vol. 7, pp. 150–161, 2019.
6. M. Hamadah and M. Aqel, "A Secure Model for Disaster Recovery in Cloud Computing Based on Virtual Private Cloud," *Journal of Computer Networks and Communications*, vol. 2018, Article ID 7893581.
7. A. Tamimi, K. Salah, and A. Al-Fuqaha, "Hot, Warm and Cold Sites: Disaster Recovery Strategies in Cloud Environments," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.
8. B. Anuprabha and S. Nivaashini, "Disaster Recovery in Cloud Using OpenStack," *Procedia Computer Science*, vol. 92, pp. 412–418, 2016.
9. F. Mendonça et al., "Performance Evaluation of Backup-as-a-Service Systems," *Journal of Systems and Software*, vol. 134, pp. 259–272, 2017.
10. Mohanarajesh, Kommineni (2024). Investigate Methods for Visualizing the Decision-Making Processes of a Complex AI System, Making Them More Understandable and Trustworthy in financial data analysis. *International Transactions on Artificial Intelligence* 8 (8):1-21.
11. D. Lang et al., "Data Compression Techniques for Secure Storage and Fast Retrieval in Cloud Environments," *International Journal of Computer Applications*, vol. 175, no. 3, pp. 12–17, 2020.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details