Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 10, pp 09-15, October, 2026

A SECURE DATA RECOVERY AND MANAGEMENT SYSTEM FOR RELIABLE DATA PROTECTION AND DISASTER RECOVERY

Maheta Karan I.[1], Khuman Ravi K.[2]

[1]PG Scholar, Department of CSE / IT, School of Engineering & Technology, Dr. Subhash University, Junagadh, Gujarat, India

[2] Assistant Professor, Department of CSE / IT, School of Engineering & Technology, Dr. Subhash University, Junagadh, Gujarat, India

ABSTRACT :

The increasing dependence on digital information has created a growing need for reliable data protection, secure backup, integrity verification, and rapid recovery after data-loss events. Data may be lost or compromised because of accidental deletion, hardware failure, software faults, unauthorized modification, malware, ransomware, or other disruptive incidents. This research proposes a Secure Data Recovery and Management System that integrates user authentication, encryption, automated backup, cryptographic integrity verification, secure storage, recovery-point management, and controlled restoration within a unified framework. The proposed system is designed to protect the confidentiality, integrity, and availability of important digital data while reducing recovery time and improving backup visibility. The system maintains multiple recovery points, verifies backup integrity before restoration, and records backup and recovery activities for management and auditing. The proposed architecture can use local, cloud, or hybrid storage and can support incremental backup to improve storage efficiency. The research further proposes performance and security evaluation using recovery time, backup time, recovery success rate, integrity detection, storage efficiency, and resource utilization. The resulting framework is intended to provide a practical foundation for secure and manageable data recovery in personal, academic, and organizational environments.

Keywords: Secure Data Recovery, Data Backup, Data Management, Encryption, Data Integrity, Disaster Recovery, Ransomware Recovery, Access Control, Cryptographic Hashing, Cloud Storage

INTRODUCTION

Digital data has become an essential resource for individuals, educational institutions, businesses, and public organizations. Documents, databases, photographs, financial records, application data, and other digital assets must remain available and trustworthy. At the same time, the possibility of data loss has increased because systems depend on interconnected hardware, software, networks, and cloud services.

Traditional backup practices may provide copies of files, but a complete recovery process also requires secure access, protection of stored backups, verification that backup data has not been altered, selection of an appropriate recovery point, and controlled restoration. A recovery system therefore needs to address confidentiality, integrity, availability, and operational recovery together.

The proposed Secure Data Recovery and Management System addresses this requirement by combining security and recovery functions into a unified workflow. Data selected for protection is authenticated, encrypted, hashed for integrity verification, backed up to secure storage, monitored through a management interface, and restored only after the selected recovery point has been verified. The approach is intended to reduce the impact of accidental deletion, corruption, hardware failure, and destructive cyber incidents.

LITERATURE REVIEW

No.	Year / Author	Title	Research Objective	Methodology	Limitation / Research Gap
1	2026 — Peiru Yang, Jinyong Chang, Youtong Wang, Xia Zhou, Yanyan Ji	Blockchain-based Proof of Retrievability Scheme with Data Deduplication Function for Cloud Storage	To develop a secure cloud-storage system combining data recovery, Proof of Retrievability, deduplication and public auditing.	Uses blockchain-assisted auditing, Proof of Retrievability, proof of ownership, key-server mechanisms and redundancy-based recovery.	Blockchain can introduce transaction cost and latency. The approach is mainly suitable for high-value/less-frequent auditing rather than all backup workloads.

2	2025 — Quinn Burke, Ryan Sheatsley, Rachel King, Owen Hines, Michael Swift, Patrick McDaniel	On Scalable Integrity Checking for Secure Cloud Disks	To improve the scalability and performance of cloud-storage integrity verification.	Uses Dynamic Merkle Trees (DMTs) and evaluates their performance for secure cloud disks.	Focuses mainly on integrity verification and does not provide complete backup scheduling, version management or automated recovery.
3	2025 — Hui Tian, Mengcheng Wang, Hanyu Quan, Chin-Chen Chang, Athanasios V. Vasilakos	TEEMRDA: Leveraging Trusted Execution Environments for Multi-Replica Data Auditing in Cloud Storage	To securely audit multiple replicas of cloud data and improve the reliability of replicated storage.	Uses Trusted Execution Environments (TEEs), random masking and authentication mechanisms for multi-replica auditing.	Primarily addresses auditing of replicas rather than complete data recovery and backup management.
4	2025 — Marius-Constantin Ilau, Adrian Baldwin	Modelling and Simulating Organizational Ransomware Recovery: Structure, Methodology, and Decisions	To model organizational ransomware recovery and analyze recovery decisions.	Uses modelling and simulation to represent ransomware recovery strategies and organizational decisions.	Focuses on recovery decision modelling rather than implementing a complete cryptographic backup and recovery system.
5	2025 — Quinn Burke, Yohan Beugin, Blaine Hoak, Rachel King, Eric Pauley, Ryan Sheatsley, Mingli Yu, Ting He, Thomas F. L. Porta, Patrick McDaniel	Securing Cloud File Systems With Trusted Execution	To design a secure cloud file system capable of protecting data against malicious providers, clients and co-tenants.	Uses Trusted Execution Environments and security protocols within a cloud file-system architecture.	Focuses on secure cloud file systems rather than complete backup, version control and disaster recovery.
6	2025 — Authors of the study	An Efficient and Secure Data Audit Scheme for Cloud-Based EHRs with Recoverable and Batch Auditing	To provide secure and recoverable auditing for cloud-based electronic health records.	Uses privacy-preserving auditing, batch auditing and recovery mechanisms.	Designed specifically for healthcare/EHR data and therefore is not a general-purpose recovery-management framework.
7	2024 — Josh Dafoe, Niusen Chen, Bo Chen, Zhenlin Wang	Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability	To analyze cloud-storage integrity techniques, vulnerabilities and security challenges.	Provides classification and comparative analysis of PDP, PoR, auditing, authentication and related integrity mechanisms.	It is a survey/review and does not implement a unified secure data recovery system.
8	2024 — Paromita Goswami, Neetu Faujdar, Somen Debnath, Ajoy Kumar Khan et al.	Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability	To analyze cloud-storage integrity techniques, vulnerabilities and security challenges.	Provides classification and comparative analysis of PDP, PoR, auditing, authentication and related integrity mechanisms.	It is a survey/review and does not implement a unified secure data recovery system.
9	2023/2024 — Mingyang Song, Zhongyun Hua, Yifeng Zheng, Tao Xiang, Xiaohua Jia	Enabling Transparent Deduplication and Auditing for Encrypted Data in Cloud	To enable secure deduplication and auditing while maintaining confidentiality of encrypted cloud data.	Combines encrypted deduplication, ownership verification and batch auditing.	Focuses on deduplication and auditing rather than complete disaster recovery and automated restoration.

No.	Year / Author	Title	Research Objective	Methodology	Limitation / Research Gap
10	2021 — Weijing You, Lei Lei, Bo Chen, Limin Liu	What If Keys Are Leaked? Towards Practical and Secure Re-Encryption in Deduplication-Based Cloud Storage	To address security risks caused by encryption-key leakage in deduplicated cloud storage.	Uses SEDER, all-or-nothing transformation, delegated re-encryption and Proof of Ownership.	Focuses on key leakage and re-encryption rather than complete backup and recovery management.
11	2020 — Shynu P. G., Nadesh R. K., Varun G. Menon, Venu P. et al.	A Secure Data Deduplication System for Integrated Cloud-Edge Networks	To reduce duplicate data while maintaining confidentiality and security in cloud-edge environments.	Uses Convergent Encryption, modified ECC, hash trees and SHA-based techniques.	Mainly focuses on secure deduplication and cloud-edge environments, not complete disaster recovery.
12	2020 — Priteshkumar Prajapati, Parth Dilipkumar Shah	A Review on Secure Data Deduplication: Cloud Storage Security Issue	To review secure deduplication techniques and identify their security challenges.	Reviews Convergent Encryption, PoR, PDP, Proof of Ownership, DupLESS, ABE and other methods.	A review rather than an implemented recovery system; key management and privacy remain challenging.
13	2018 — Choon-Beng Tan, Ahmad Hijazi Mohd Hanafi, Yuto Lim, Abdullah Gani	A Survey on Proof of Retrievability for Cloud Data Integrity and Availability: Cloud Storage State-of-the-Art, Issues, Solutions and Future Trends.	To study Proof-of-Retrievability techniques for ensuring cloud-data integrity and availability.	Surveys and compares different PoR schemes, security properties and performance characteristics.	Does not provide a complete integrated backup and recovery-management system.
14	2017 — Faheem Zafar, Abid Khan, Saif Ur Rehman Malik, Mansoor Ahmed et al.	A Survey of Cloud Computing Data Integrity Schemes: Design Challenges, Taxonomy and Future Trends	To classify cloud data-integrity schemes and identify security and scalability challenges.	Develops a taxonomy and comparative analysis of cloud-integrity mechanisms.	Concentrates on integrity rather than end-to-end data restoration and recovery management.
15	2016 — Junbeom Hur, Dongyoung Koo, Youngjoo Shin, Kyungtae Kang	Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage	To provide secure deduplication when data ownership changes dynamically.	Combines deduplication, Proof of Ownership and dynamic ownership management.	Focuses on ownership and deduplication; complete recovery and backup lifecycle management are not addressed.
16	2015 — Victor Chang	Towards a Big Data System Disaster Recovery in a Private Cloud	To improve disaster recovery for large-scale Big Data systems.	Uses snapshots, replication, multiple recovery destinations and different recovery technologies.	Mainly focuses on private-cloud Big Data systems and does not integrate all modern security and recovery mechanisms.
17	2013 — Kan Yang, Xiaohua Jia	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing	To efficiently verify the integrity of dynamically changing cloud data.	Uses privacy-preserving dynamic auditing and batch auditing.	Detects integrity problems but does not itself provide complete automated data restoration.
18	2013 — Mihir Bellare, Sriram Keelveedhi, Thomas Ristenpart	DupLESS: Server-Aided Encryption for Deduplicated Storage	To combine secure encryption with the storage efficiency of deduplication.	Uses message-based keys and an oblivious PRF with a key server.	Requires additional key-server infrastructure and focuses primarily on secure deduplication.
19	2011 — Shai Halevi, Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg	Proofs of Ownership in Remote Storage Systems	To prevent unauthorized users from claiming ownership of files in remote deduplicated storage.	Uses Proof-of-Ownership protocols and cryptographic verification techniques.	Addresses ownership verification rather than complete backup, monitoring and recovery.

RESEARCH GAP AND OBJECTIVES

Identified Research Gaps

- Existing data-protection solutions often treat backup, encryption, integrity verification, access control, and recovery as separate functions.
- Backup availability does not by itself guarantee that a stored copy is trustworthy; integrity verification is required before restoration.

- Recovery operations need strong authentication and authorization so that unauthorized users cannot restore, delete, or manipulate protected data.
- Ransomware and destructive incidents require recovery points that can be validated before they are restored.
- Multiple backups may increase storage and management requirements; secure storage optimization and incremental backup can improve efficiency.
- Users require a clear management interface for backup status, recovery points, integrity status, storage usage, and recovery history.
- There is scope for an integrated, automated, and measurable framework that evaluates security, recovery performance, integrity, and resource consumption together.

Research Objective

To design and develop a secure data recovery and management system for protecting critical digital information.

- To implement secure authentication and access-control mechanisms for data management and recovery.
- To implement encryption mechanisms for protecting data during storage and recovery.
- To develop automated full and incremental backup mechanisms with multiple recovery points.
- To implement cryptographic integrity verification for detecting corrupted or modified backup data.
- To provide controlled recovery following accidental deletion, corruption, hardware failure, or destructive cyber incidents.
- To develop a management dashboard for monitoring backup, storage, integrity, and recovery activities.
- To evaluate the proposed system using security, recovery-performance, storage-efficiency, and resource-utilization metrics.

Problem Definition

The problem addressed by this research is the lack of a unified and manageable approach that protects data before loss, maintains trustworthy backup copies, detects integrity violations, and restores verified information after a disruptive event. Accidental deletion, hardware failure, software errors, malware, ransomware, and unauthorized modification can make data unavailable or unreliable. Therefore, there is a need for a secure, automated, scalable, and user-manageable system that combines authentication, encryption, backup, integrity verification, recovery-point management, and secure restoration.

3.3 Problem Definition

- Secure encrypted backup of important files and data.
- Improved detection of corrupted or modified backup copies.
- Faster and more controlled recovery using multiple verified recovery points.
- Improved monitoring of backup success, failure, storage usage, and recovery history.
- Reduced redundant storage through incremental backup and optional secure deduplication.
- Improved protection against unauthorized access to backup and recovery operations.
- Generation of audit and recovery logs for accountability and management.
- A measurable framework for evaluating recovery time, backup performance, integrity detection, and storage efficiency.

METHODOLOGY

Proposed System Architecture

The proposed architecture consists of the following logical layers:

- User Layer: user login, authentication, role selection, data selection, backup requests, and recovery requests.
- Security Layer: authentication, authorization, encryption/decryption, cryptographic hashing, and key management controls.
- Backup Layer: full backup, incremental backup, scheduling, version management, and backup validation.
- Storage Layer: local storage, cloud storage, or hybrid storage for protected backup copies.
- Integrity Layer: hash generation, hash comparison, backup verification, corruption detection, and recovery-point validation.
- Recovery Layer: recovery-point selection, authentication, integrity check, decryption, restoration, and recovery logging.
- Management Layer: dashboard for backup status, storage statistics, integrity status, recovery history, and alerts.

Secure Authentication and Access Control

The system first verifies the identity of a user before allowing protected operations. Role-based permissions can be used to separate ordinary data-management activities from administrative backup and recovery operations. Sensitive operations such as deleting a recovery point or restoring organizational data should require appropriate authorization.

Data Encryption

Protected data should be encrypted before it is stored in a backup location. A symmetric encryption mechanism such as AES can be evaluated for file encryption, while an asymmetric mechanism may be used for secure key exchange or key protection. Encryption is intended to reduce the risk of unauthorized disclosure if backup storage is accessed improperly.

Automated Backup

The backup engine can support scheduled full and incremental backups. A full backup creates a complete protected copy, while an incremental backup stores changes made since an earlier backup. The system maintains timestamps and versions so that users can select an appropriate recovery point.

Data Integrity Verification

A cryptographic hash such as SHA-256 can be generated for protected data or backup objects. During validation or recovery, the system calculates the current hash and compares it with the stored integrity value. A mismatch is treated as an integrity warning and the affected recovery point should not be restored without further validation.

Secure Recovery Process

A recovery request begins with authentication and selection of a recovery point. The system verifies the selected backup, checks integrity, decrypts the protected data, restores it to the requested destination, and records the recovery operation. This sequence is designed to reduce the chance of restoring incomplete, corrupted, or unauthorized data.

Management Dashboard

The management dashboard should provide an overview of protected files, total backup size, latest successful backup, failed backups, integrity status, recovery operations, and storage utilization. Alerts can notify users when a scheduled backup fails or an integrity mismatch is detected.

Proposed Workflow

User → Authentication → Data Selection → Hash Generation → Encryption → Backup → Secure Storage → Monitoring → Recovery Request → Recovery-Point Verification → Decryption → Restoration → Recovery Log

EXPERIMENTAL SETUP AND EVALUATION PLAN

Proposed Experimental Dataset

For prototype evaluation, a controlled dataset can contain documents, images, PDFs, text files, compressed files, and sample database exports with different file sizes. Test cases should include normal backup, repeated backup, accidental deletion, intentional modification of a backup copy, simulated corruption, and recovery from different recovery points.

Hardware and Software Environment

A prototype may be implemented using a standard computer or server with sufficient storage, a local database, and optional cloud storage. A Python-based backend such as Flask or FastAPI can be used with a web-based management interface. Database options include MySQL or PostgreSQL. The final technology selection should depend on the implementation scope and available resources.

Performance Metrics

Metric	**Purpose**
Recovery Time	Time required to restore a selected data set.
Backup Time	Time required to create a backup.
Recovery Success Rate	Percentage of recovery operations completed successfully.
Integrity Detection Rate	Ability to detect intentionally modified or corrupted backup data.
Encryption Overhead	Additional processing time caused by encryption/decryption.
Storage Efficiency	Storage required before and after backup optimization.

CPU / Memory Usage	System resources consumed during backup and recovery.
Network Usage	Amount of data transferred during remote backup or recovery.

Security Test Cases

- Attempt unauthorized access to protected backup files.
- Attempt recovery without valid authentication.
- Modify a stored backup and verify integrity detection.
- Delete or disable a backup target and measure failure notification.
- Attempt restoration from a corrupted recovery point.
- Compare recovery from valid and invalid recovery points.
- Measure system performance for different file sizes.

Expected Results and Discussion

The expected evaluation should demonstrate that encrypted storage reduces exposure of backup content, integrity verification can identify modified backup data, and multiple recovery points improve restoration flexibility. Experimental results should be reported using tables and graphs rather than unsupported claims. The final paper should include measured values for backup time, recovery time, integrity detection, storage use, and system-resource consumption after implementation.

FUTURE SCOPE AND ENHANCEMENTS

- AI-based anomaly detection for unusual backup or file-modification behavior.
- Automated ransomware detection and isolation of suspicious recovery points.
- Immutable backup storage to reduce the risk of backup tampering.
- Multi-cloud and hybrid-cloud disaster recovery.
- Zero-trust security principles for sensitive recovery operations.
- Mobile application for monitoring and emergency recovery management.
- Blockchain-based audit trails for selected high-security environments.
- Intelligent recovery-point recommendation based on integrity and security status.
- Integration with enterprise databases and large-scale organizational infrastructure.

CONCLUSION

The proposed Secure Data Recovery and Management System aims to move data protection from simple file copying toward an integrated security and recovery framework. By combining authentication, encryption, automated backup, cryptographic integrity verification, recovery-point management, secure restoration, and monitoring, the proposed system can provide a structured approach to protecting critical digital information. The research also emphasizes measurable evaluation through recovery time, backup performance, integrity detection, storage efficiency, and resource utilization. The framework can serve as a practical foundation for a prototype suitable for academic, personal, or organizational environments, while advanced capabilities such as ransomware detection, immutable storage, multi-cloud recovery, and blockchain-based auditing can be considered for future development.

REFERENCES

[1] Q. Burke, R. Sheatsley, R. King, O. Hines, M. Swift, and P. McDaniel, —On Scalable Integrity Checking for Secure Cloud Disks,‖ *Proceedings of the 23rd USENIX Conference on File and Storage Technologies (FAST 2025)*, pp. 391–405, 2025.

[2] H. Tian, M. Wang, H. Quan, C.-C. Chang, and A. V. Vasilakos, —TEEMRDA: Leveraging Trusted Execution Environments for Multi-Replica Data Auditing in Cloud Storage,‖ *Computers & Security*, 2025, Art. no. 104250. doi: **10.1016/j.cose.2024.104250**.

[3] M.-C. Ilau and A. Baldwin, —Modelling and Simulating Organizational Ransomware Recovery: Structure, Methodology, and Decisions,‖ *Journal of Cybersecurity*, vol. 11, no. 1, Art. no. tyaf035, 2025. doi: **10.1093/cybsec/tyaf035**.

[4] Q. Burke, Y. Beugin, B. Hoak, R. King, E. Pauley, R. Sheatsley, M. Yu, T. He, T. F. L. Porta, and P. McDaniel, —Securing Cloud File Systems With Trusted Execution,‖ *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 1976–1992, 2025. doi: **10.1109/TDSC.2024.3474423**.

[5] Y. Zhang, X. A. Wang, W. Jiang, M. Zhou, X. Xu, and H. Liu, —An Efficient and Secure Data Audit Scheme for Cloud-Based EHRs with

Recoverable and Batch Auditing,‖ *Computers, Materials & Continua*, vol. 83, no. 1, pp. 1533–1553, 2025. doi: **10.32604/cmc.2025.062910**.

[6] J. Dafoe, N. Chen, B. Chen, and Z. Wang, —Enabling Per-File Data Recovery from Ransomware Attacks via File System Forensics and Flash Translation Layer Data Extraction,‖ *Cybersecurity*, vol. 7, Art. no. 75, 2024. doi: **10.1186/s42400-024-00287-9**.

[7] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, G. Singh, *et al.*, —Investigation on Storage Level Data Integrity Strategies in Cloud Computing: Classification, Security Obstructions, Challenges and Vulnerability,‖ *Journal of Cloud Computing*, 2024. doi: **10.1186/s13677-024-00605-z**.

[8] M. Song, Z. Hua, Y. Zheng, T. Xiang, and X. Jia, —Enabling Transparent Deduplication and Auditing for Encrypted Data in Cloud,‖ *IEEE Transactions on Dependable and Secure Computing*, 2023. doi: **10.1109/TDSC.2023.3334475**.

[9] W. You, L. Lei, B. Chen, and L. Liu, —What If Keys Are Leaked? Towards Practical and Secure Re-Encryption in Deduplication-Based Cloud Storage,‖ *Information*, vol. 12, no. 4, Art. no. 142, 2021. doi: **10.3390/info12040142**.

[10] S. P. Gopalan, N. R. K. Nadesh, V. G. Menon, V. P., M. Abbasi, and M. R. Khosravi, —A Secure Data Deduplication System for Integrated Cloud-Edge Networks,‖ *Journal of Cloud Computing*, vol. 9, Art. no. 61, 2020. doi: **10.1186/s13677-020-00214-6**.

[11] P. Prajapati and P. Shah, —A Review on Secure Data Deduplication: Cloud Storage Security Issue,‖ *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 7, pp. 3996–4007, 2022. doi: **10.1016/j.jksuci.2020.10.021**.

[12] C.-B. Tan, A. H. M. Hanafi, Y. Lim, and A. Gani, —A Survey on Proof of Retrievability for Cloud Data Integrity and Availability: Cloud Storage State-of-the-Art, Issues, Solutions and Future Trends,‖ *Journal of Network and Computer Applications*, vol. 110, pp. 75–86, 2018. doi: **10.1016/j.jnca.2018.03.017**.

[13] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, *et al.*, —A Survey of Cloud Computing Data Integrity Schemes: Design Challenges, Taxonomy and Future Trends,‖ *Computers & Security*, vol. 65, pp. 29–49, 2017. doi: **10.1016/j.cose.2016.10.006**.

[14] J. Hur, D. Koo, Y. Shin, and K. Kang, —Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage,‖ *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 11, pp. 3113–3125, 2016. doi: **10.1109/TKDE.2016.2580139**.

[15] V. Chang, —Towards a Big Data System Disaster Recovery in a Private Cloud,‖ *Ad Hoc Networks*, vol. 35, pp. 65–82, 2015. doi: **10.1016/j.adhoc.2015.07.012**.

[16] K. Yang and X. Jia, —An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing,‖ *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1717–1726, 2013. doi: **10.1109/TPDS.2012.278**.

[17] S. Keelveedhi, M. Bellare, and T. Ristenpart, —DupLESS: Server-Aided Encryption for Deduplicated Storage,‖ *Proceedings of the 22nd USENIX Security Symposium (USENIX Security 13)*, pp. 179–194, 2013.

[18] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, —Proofs of Ownership in Remote Storage Systems,‖ *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011)*, pp. 491–500, 2011. doi: **10.1145/2046707.2046765**.

[19] C. Wang, K. Ren, W. Lou, and J. Li, —Toward Publicly Auditable Secure Cloud Data Storage Services,‖ *IEEE Network*, vol. 24, no. 4, pp. 19–24, 2010. doi: **10.1109/MNET.2010.5510914**.