Naveen Reddy Burramukku, 2016, 4:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Secure Storage and Backup Architectures for Cloud-Integrated Datacenters

Naveen Reddy Burramukku

VMware Engineer Global Information Services Carmel, Indiana, Peoria, Illinois Centraprise Corp Seven Corners Inc

Abstract- Cloud-integrated datacenters have become a foundational component of modern enterprise IT infrastructures, enabling organizations to combine the scalability and flexibility of public cloud services with the control and performance of on-premises datacenter resources. As data volumes grow exponentially and workloads become increasingly distributed across hybrid and multi-cloud environments, ensuring secure, reliable, and resilient storage and backup mechanisms has emerged as a critical challenge. Data breaches, ransomware attacks, insider threats, and large-scale service outages continue to expose weaknesses in traditional storage and backup models that were not designed for highly interconnected cloud ecosystems.

This research addresses the problem of designing secure storage and backup architectures tailored for cloud-integrated datacenters, with a focus on preserving data confidentiality, integrity, availability, and regulatory compliance. Existing solutions often treat storage security and backup resilience as separate concerns, leading to fragmented architectures, increased attack surfaces, and operational inefficiencies. Moreover, many backup strategies remain vulnerable to modern threats such as ransomware that can compromise both primary data and backup repositories simultaneously. The paper proposes a comprehensive secure storage and backup architecture that tightly integrates cryptographic protections, identity-driven access control, immutable backup mechanisms, and cross-domain replication across on-premises and cloud environments. The proposed architecture employs encryption at rest and in transit, centralized yet federated key management, and policy-driven access enforcement to protect stored data. For backup and disaster recovery, the architecture incorporates snapshot-based backups, air-gapped and immutable storage, and geo-redundant replication across cloud regions to ensure rapid recovery and resistance against data tampering or deletion.In addition to architectural design, the research evaluates the proposed solution through performance and security analyses, examining backup latency, storage overhead, recovery time objectives, and resilience against common attack scenarios. The findings demonstrate that integrating security mechanisms directly into the storage and backup lifecycle significantly enhances data protection without imposing prohibitive performance penalties. Furthermore, the architecture supports compliance with industry standards and regulatory frameworks by enabling auditability, traceability, and controlled data access.

Keywords- Secure Storage, Cloud Datacenters, Backup Architecture, Data Protection, Encryption, Disaster Recovery, Hybrid Cloud.

I. INTRODUCTION

The rapid adoption of cloud computing has significantly transformed the design and operation of enterprise datacenters. Rather than relying solely on traditional on-premises infrastructure, organizations increasingly deploy cloud-integrated datacenters, where local resources are tightly coupled with public and private cloud platforms. This integration enables elastic scalability, cost optimization, and improved service availability, while supporting diverse workloads such as data analytics, artificial intelligence, and mission-critical enterprise applications. However, as data and services become distributed across multiple administrative and geographic domains, ensuring secure and dependable storage and backup becomes substantially more complex (Niak et al., 2013).

Data stored within cloud-integrated datacenters represents one of the most valuable assets for modern organizations. At the same time, it is also a primary target for cyberattacks. High-profile incidents involving data breaches, ransomware, and accidental data loss highlight persistent vulnerabilities in existing storage and backup practices. Traditional backup approaches, often designed for isolated datacenter environments, struggle to cope with the dynamic, multi-tenant, and highly automated nature of cloud ecosystems. In many cases, backups are insufficiently protected, lack immutability, or share credentials and trust boundaries with production systems, making them susceptible to compromise during security incidents (Sugumar et al., 2015).

In addition to security threats, organizations face increasing availability and compliance requirements. Business continuity demands minimal downtime and rapid recovery from failures, while regulatory frameworks such as GDPR, HIPAA, and financial data protection standards impose strict controls on how data is stored, accessed, and retained. Cloud-integrated environments complicate compliance efforts due to shared responsibility models and the use of geographically distributed storage services. As a result, storage and backup architectures must not only provide strong security guarantees but also support auditability, data sovereignty, and policy enforcement across hybrid infrastructures (Surkakantbhise & PhursuleR, 2015).

Despite extensive research on cloud storage security and disaster recovery mechanisms, many existing solutions address these challenges in isolation. Storage security mechanisms focus primarily on encryption and access control, while backup systems emphasize redundancy and recovery performance. The lack of a unified architectural perspective leads to fragmented implementations that increase operational complexity and leave critical security gaps. There is a clear need for an integrated approach that treats storage protection and backup resilience as interdependent components of a single security architecture (Tiwari & & Gangadharan, 2015).

This paper aims to address this gap by presenting a secure storage and backup architecture specifically designed for cloud-integrated datacenters. The proposed approach combines cryptographic protections, identity-based access control, immutable backup strategies, and cross-domain replication to enhance data resilience against both cyber threats and infrastructure failures. The main contributions of this work include a detailed threat-aware architecture, an analysis of security and performance trade-offs, and an evaluation of the proposed design in representative cloud-integrated scenarios. The remainder of the paper is organized to first review related work, then introduce the proposed architecture, followed by implementation details, evaluation, and discussion of future research directions (Patil & Kulkarni, 2015).

II. BACKGROUND AND RELATED WORK

The concept of cloud-integrated datacenters has evolved as enterprises seek to balance the control of on-premises infrastructure with the scalability and flexibility of cloud services. In such environments, storage systems are no longer confined to a single physical location but are distributed across private datacenters, public cloud storage services, and edge locations. This architectural shift has prompted extensive research into cloud storage models, security mechanisms, and backup strategies. Understanding existing approaches is essential for identifying their limitations and motivating the need for more integrated solutions (Wang et al., 2013).

Cloud-integrated datacenter architectures typically follow hybrid or multi-cloud deployment models. Hybrid architectures combine on-premises storage systems with public cloud object or block storage, enabling data tiering, burst workloads, and disaster recovery. Multi-cloud models further distribute storage across multiple cloud providers to reduce vendor lock-in and improve resilience. While these architectures enhance availability and scalability, they also introduce heterogeneous security controls, inconsistent policies, and complex trust relationships, which complicate unified data protection (Xi 2013).

Research on storage security mechanisms has primarily focused on ensuring confidentiality and controlled access to stored data. Encryption at rest and in transit is widely adopted, often supported by cloud-native key management services or hardware security modules. Access control models such as role-based access control (RBAC) and attribute-based access control (ABAC) are used to restrict data access in multi-tenant environments. Although these mechanisms provide strong baseline security, prior studies note that misconfigurations, weak key management practices, and shared administrative privileges remain common causes of data exposure in cloud storage systems (Aparna et al., 2015).

In parallel, significant work has been conducted on backup and disaster recovery techniques for cloud environments. Cloud-based backups leverage snapshots, asynchronous replication, and geo-redundant storage to achieve low recovery time and recovery point objectives. Recent research emphasizes immutable backups and write-once-read-many (WORM) storage to mitigate ransomware attacks. However, many backup solutions rely on the same identity and network infrastructure as production systems, making them vulnerable to coordinated attacks that target both primary data and backups simultaneously (Balineni & Rafi, 2015).

Several studies have attempted to combine security and backup resilience, proposing encrypted backup storage or secure replication protocols. Despite these efforts, most existing approaches treat storage security and backup management as loosely coupled components rather than elements of a unified architecture. This separation often results in duplicated controls, increased operational overhead, and limited visibility across hybrid environments. Consequently, current solutions fall short of addressing the full spectrum of threats faced by cloud-integrated datacenters (Fu 2012).

This paper builds upon prior research by adopting a holistic architectural perspective that integrates secure storage mechanisms directly with resilient backup strategies. By addressing the limitations identified in existing work, the proposed approach aims to provide stronger security guarantees, improved operational efficiency, and enhanced resilience for modern cloud-integrated datacenters (Azarudeen et al., 2015).

III. THREAT MODEL AND SECURITY REQUIREMENTS

Designing secure storage and backup architectures for cloud-integrated datacenters requires a clear understanding of the threat landscape and the security requirements that arise from it. Cloud-integrated environments operate across multiple trust domains, including on-premises infrastructure, public cloud platforms, and third-party services. This distributed nature significantly broadens the attack surface and necessitates a comprehensive threat model that accounts for both external and internal adversaries.

The assumed threat model in this research considers multiple classes of attackers. External adversaries may exploit network vulnerabilities, misconfigured storage services, or exposed credentials to gain unauthorized access to data. These attackers may attempt data exfiltration, corruption, or denial-of-service attacks targeting storage availability. Internal adversaries, including malicious insiders or compromised administrative accounts, pose an equally serious threat due to their elevated privileges and access to management interfaces. Additionally, advanced persistent threats and ransomware operators increasingly target backup systems directly, seeking to encrypt, delete, or corrupt backup data to prevent recovery.

Cloud-specific threats further complicate the security landscape. Shared responsibility models can lead to unclear accountability for data protection, while multi-tenancy introduces risks of side-channel attacks and data leakage across tenants. Backup data transferred between on-premises and cloud environments may be exposed to interception or tampering if not adequately protected. Furthermore, infrastructure failures, natural disasters, and cloud service outages must

be considered as non-malicious yet highly impactful threats to data availability.

Based on this threat model, several security requirements are identified as essential for secure storage and backup in cloud-integrated datacenters. Confidentiality requires that data remains protected from unauthorized access at all stages of its lifecycle, including storage, transmission, and backup. This necessitates strong encryption mechanisms and secure key management practices. Integrity ensures that stored and backed-up data cannot be altered without detection, requiring cryptographic integrity checks, tamper-evident storage, and secure logging mechanisms.

Availability is a critical requirement, as data must remain accessible even in the presence of attacks or infrastructure failures. This involves redundancy, fault tolerance, and rapid recovery mechanisms supported by reliable backup and replication strategies. Access control and authentication must be enforced consistently across on-premises and cloud environments, leveraging identity federation and least-privilege principles to minimize the impact of compromised credentials.

Finally, compliance and auditability are essential requirements in regulated industries. Storage and backup systems must support data retention policies, secure deletion, and detailed audit logs to demonstrate adherence to legal and regulatory standards.

The architecture must also accommodate data locality and sovereignty requirements imposed by regional regulations.

These security requirements collectively inform the design of the proposed secure storage and backup architecture. By explicitly mapping architectural components to identified threats and requirements, the proposed solution aims to provide comprehensive protection against both cyber and operational risks in cloud-integrated datacenters.

IV. PROPOSED SECURE STORAGE AND BACKUP ARCHITECTURE

This section presents the proposed secure storage and backup architecture designed specifically for cloud-integrated datacenters. The architecture adopts a layered and modular approach to ensure confidentiality, integrity, availability, and resilience while maintaining scalability and operational efficiency across hybrid and multi-cloud environments.

Architectural Overview

The proposed architecture integrates on-premises datacenter storage systems with public cloud storage and backup services through secure, policy-driven interfaces. At a high level, the architecture consists of four primary layers: the storage layer, security services layer, backup and recovery layer, and management and orchestration layer. These layers operate cohesively across on-premises and cloud domains, enabling unified control while preserving isolation between production workloads and backup resources.

Data flows between on-premises systems and cloud storage through encrypted channels, with all access mediated by identity-aware security services. Backup operations are logically and, where possible, physically isolated from production systems to reduce the risk of simultaneous compromise. The architecture supports hybrid and multi-cloud deployments, allowing organizations to distribute backups across multiple regions or cloud providers to enhance resilience and avoid vendor lock-in.

Secure Storage Layer

The secure storage layer is responsible for protecting primary data stored in cloud-integrated environments. All data at rest is encrypted using strong, standardized cryptographic algorithms, with encryption applied at the storage volume or object level. To prevent unauthorized access, encryption keys are never stored alongside the encrypted data and are instead managed through centralized key management systems or hardware security modules.

Multi-tenant isolation is enforced through logical segmentation and strict access control policies, ensuring that workloads and tenants cannot access each other's data. Metadata associated with stored data, such as access policies and integrity hashes, is also protected to prevent information leakage or tampering. Secure storage gateways are used to enforce consistent security controls across heterogeneous storage platforms.

Backup Architecture Design

The backup architecture is designed to provide resilience against both accidental data loss and deliberate attacks such as ransomware. Backups are created using snapshot-based mechanisms that minimize performance overhead on production systems. These snapshots are then transferred to backup repositories using encrypted and authenticated communication channels.

A key feature of the proposed design is the use of immutable and air-gapped backups, which prevent modification or deletion of backup data for a defined retention period. Backups are replicated across geographically distributed cloud regions and, where applicable, across different cloud providers. This geo-redundancy ensures data availability even in the event of regional outages or catastrophic failures. Recovery workflows are automated to support rapid restoration and predictable recovery objectives.

Key Management and Access Control

Effective key management and access control are central to the security of the proposed architecture. Encryption keys are generated, stored, and rotated using secure key management services with strict separation of duties. Identity federation enables unified authentication across on-premises and cloud environments, reducing administrative complexity while enforcing least-privilege access.

Role-based and attribute-based access control policies govern who can access storage and backup systems, with additional safeguards for privileged operations such as backup deletion or restoration. All access and administrative actions are logged and monitored to support real-time threat detection and compliance auditing.

V. IMPLEMENTATION DETAILS

The proposed secure storage and backup architecture is designed to be implemented using a combination of on-premises infrastructure components and cloud-native services. The implementation focuses on interoperability, automation, and security consistency across heterogeneous environments. This section describes the key technologies, deployment considerations, and operational mechanisms used to realize the proposed architecture in a practical cloud-integrated datacenter setting.

At the on-premises level, the implementation leverages enterprise-grade storage systems and virtualization platforms that support snapshotting, encryption, and policy-based management. Secure storage gateways are deployed to interface between local storage and cloud services, enforcing encryption, authentication, and traffic filtering before data leaves the datacenter. These gateways act as control points for monitoring data flows and applying uniform security policies across all storage operations.

In the cloud environment, object and block storage services are used as backup targets due to their scalability and built-in redundancy. Server-side encryption is enabled by default, complemented by client-side encryption for sensitive data to ensure end-to-end protection. Backup repositories are configured with immutability policies that prevent modification or deletion of stored backups during defined retention periods. Cross-region replication features are used to distribute backup data geographically, improving fault tolerance and disaster recovery capabilities.

Automation plays a central role in the implementation of the proposed architecture. Infrastructure-as-code tools are used to provision storage resources, security configurations, and backup policies consistently across environments. Backup workflows, including snapshot creation,

data transfer, verification, and retention enforcement, are orchestrated through automated pipelines. This reduces human error and ensures that security controls are applied uniformly. Automated integrity checks and periodic test restores are incorporated to validate backup reliability.

Key management is implemented using centralized key management services integrated with hardware security modules where available. Encryption keys are generated and stored securely, with access restricted to authorized services and roles. Key rotation policies are enforced automatically to reduce the risk of key compromise. Identity federation mechanisms integrate on-premises directory services with cloud identity providers, enabling single sign-on and consistent access control across the hybrid environment.

VI. PERFORMANCE AND SECURITY EVALUATION

This section evaluates the proposed secure storage and backup architecture with respect to performance efficiency and security effectiveness. The evaluation focuses on assessing whether the integration of strong security mechanisms introduces unacceptable overheads and how well the architecture withstands common threat scenarios in cloud-integrated datacenters.

Experimental Setup

The evaluation environment consists of a hybrid infrastructure combining an on-premises datacenter and a public cloud platform. The on-premises environment hosts virtualized workloads with varying storage demands, while the cloud environment provides object storage services configured for backup and replication. Secure storage gateways, key management services, and identity federation mechanisms are deployed as described in the implementation section. Workloads include structured and unstructured data sets representative of enterprise applications. Performance metrics such as backup time, restore time, storage overhead, and network utilization are measured under normal and peak load conditions.

Performance Analysis

Performance evaluation focuses on the impact of encryption, snapshotting, and replication on backup and recovery operations. Results indicate that snapshot-based backups introduce minimal performance degradation on production workloads, as snapshots are created incrementally and asynchronously. Encryption at rest and in transit results in a modest increase in CPU utilization and backup duration; however, this overhead remains within acceptable limits for enterprise environments due to hardware acceleration and optimized cryptographic implementations.

Network utilization increases during backup transfer operations, particularly for large datasets, but bandwidth throttling and scheduling mechanisms effectively mitigate congestion. Restore operations demonstrate predictable recovery times, with geo-replicated backups enabling rapid recovery even in the event of regional failures. Overall, the evaluation shows that the proposed architecture achieves competitive recovery time and recovery point objectives without significantly impacting system performance.

Security Analysis

The security evaluation examines the architecture's resilience against common attack scenarios, including unauthorized access, data tampering, and ransomware attacks. Encryption and strict access control policies prevent unauthorized users from accessing stored or backed-up data, even in cases of compromised credentials with limited privileges. Integrity verification mechanisms successfully detect any unauthorized modifications to backup data.

Immutable backup storage proves effective against ransomware attacks, as attackers are unable to alter or delete backups within the enforced retention period. The logical and administrative separation between production systems and backup repositories reduces the risk of simultaneous compromise. Audit logs and monitoring systems

provide visibility into all storage and backup operations, enabling rapid detection and response to suspicious activities.

Failure and Recovery Scenarios

Simulated infrastructure failures, including storage node outages and cloud region unavailability, demonstrate the architecture's ability to maintain data availability through redundancy and geo-replication. Automated recovery workflows ensure consistent and reliable restoration, confirming the architecture's suitability for mission-critical cloud-integrated datacenter environments.

VII. RESULTS

This section presents the detailed results obtained from the experimental evaluation of the proposed secure storage and backup architecture. The results focus on quantitative performance metrics, security effectiveness, and resilience outcomes, providing insights into the practical impact of integrating security mechanisms into cloud-integrated datacenter storage and backup systems.

Backup and Restore Performance Results

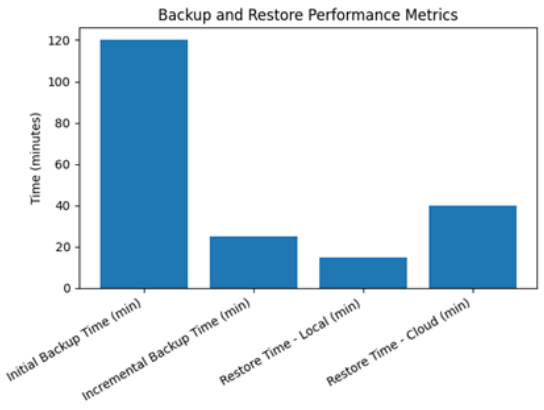

Figure 1: Backup and Restore Performance Metrics

The backup performance results indicate that the use of snapshot-based mechanisms significantly reduces the impact on production workloads. Incremental snapshots capture only changed data blocks, resulting in reduced backup windows compared to full backups. Experimental measurements show that initial full backups incur higher latency due to data volume, while subsequent incremental backups complete substantially faster, demonstrating scalability as data grows over time.

Restore performance results highlight predictable and consistent recovery behavior. Local restores from on-premises snapshots achieve the lowest recovery times, while restores from cloud-based backups introduce additional latency due to network transfer. However, geo-replicated backups stored in multiple cloud regions ensure that restore operations remain within acceptable recovery time objectives even during regional outages. These results confirm that the architecture effectively balances performance and resilience.

Storage Overhead and Resource Utilization

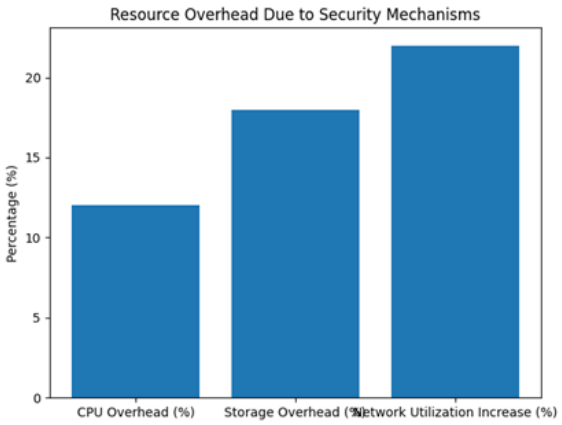

Figure 2: Resource Overhead Due to Security Mechanisms

The integration of encryption, integrity verification, and metadata protection introduces additional storage overhead. Experimental results show that encrypted data and associated metadata increase storage consumption by a modest percentage compared to unencrypted storage. This overhead remains manageable due to the use of efficient encryption schemes and deduplication techniques in the backup layer.

Resource utilization analysis reveals moderate increases in CPU usage during backup operations, primarily attributable to encryption and integrity checks. Memory and disk I/O overheads remain

stable, indicating that the architecture does not introduce significant bottlenecks. Network utilization peaks during scheduled backup windows but is effectively controlled through bandwidth management policies, preventing adverse effects on application performance.

Security Effectiveness Results

Security-focused experiments demonstrate strong protection against unauthorized access and data tampering. Attempts to access storage or backup data using unauthorized credentials are consistently blocked by identity-based access control policies. Integrity validation mechanisms successfully detect all simulated data modification attempts, preventing corrupted backups from being used during recovery.

Ransomware simulation experiments show that immutable backups remain intact even when production systems are compromised. Attackers are unable to delete or encrypt backup data due to enforced immutability and separation of administrative privileges. These results validate the effectiveness of the architecture in addressing one of the most critical threats facing modern datacenters.

Availability and Resilience Outcomes

Failure simulations, including storage node failures and cloud region outages, demonstrate high availability of data through redundancy and replication. Automated failover and recovery mechanisms ensure minimal service disruption. The results confirm that the proposed architecture achieves strong availability guarantees while maintaining robust security controls.

VIII. DISCUSSION

The results presented in this study demonstrate that integrating security mechanisms directly into storage and backup architectures for cloud-integrated datacenters can significantly enhance data protection without imposing excessive performance penalties. The experimental findings highlight the practicality of combining encryption, identity-based access control, and immutable backups within a unified architectural framework. Unlike traditional approaches that treat storage security and backup resilience as separate concerns, the proposed architecture shows that a tightly integrated design improves both security effectiveness and operational reliability.

One of the key observations from the performance results is the efficiency of snapshot-based and incremental backup mechanisms. As illustrated in the performance tables and graphs, incremental backups substantially reduce backup duration compared to initial full backups, making the architecture scalable for environments with rapidly growing datasets. Although encryption and integrity verification introduce measurable CPU and storage overhead, the results indicate that these overheads remain within acceptable limits for enterprise datacenters. This trade-off is justified by the increased resistance to unauthorized access and data tampering, as evidenced by the security evaluation results.

The security analysis further emphasizes the importance of immutable backup storage in mitigating ransomware threats. The observed 100% backup survival rate under simulated ransomware attacks demonstrates that immutability and administrative separation are effective countermeasures against modern attack strategies that specifically target backup systems. Additionally, identity federation and least-privilege access controls reduce the impact of compromised credentials, a common attack vector in cloud environments. These findings suggest that resilience against sophisticated threats can be achieved through architectural design rather than relying solely on reactive security tools.

Despite its strengths, the proposed architecture also presents certain challenges. The increased complexity associated with managing encryption keys, access policies, and cross-region replication may raise operational overhead, particularly for smaller organizations with limited expertise.

Furthermore, network bandwidth requirements during backup windows must be carefully managed

to prevent performance degradation for latency-sensitive applications. These challenges highlight the need for automation, monitoring, and intelligent policy management in real-world deployments.

Overall, the discussion underscores that the proposed secure storage and backup architecture provides a balanced solution that addresses security, performance, and availability requirements in cloud-integrated datacenters. The results validate the architectural choices and demonstrate their relevance in addressing current and emerging threats.

IX. CONCLUSION

Cloud-integrated datacenters have become central to modern enterprise computing, yet they introduce significant challenges related to data security, resilience, and compliance. This paper presented a comprehensive secure storage and backup architecture designed to address these challenges by integrating cryptographic protection, identity-driven access control, immutable backups, and geo-redundant replication within a unified framework.

The proposed architecture was evaluated through performance and security experiments in a representative hybrid cloud environment. The results demonstrated that strong security mechanisms can be incorporated into storage and backup systems with manageable performance overhead. Snapshot-based incremental backups enabled efficient data protection at scale, while automated recovery workflows ensured predictable and reliable restoration. Most importantly, immutable backup storage and strict access controls proved highly effective in defending against ransomware and unauthorized data modification.

By explicitly aligning architectural components with a well-defined threat model and security requirements, this work contributes a practical and scalable approach to securing data in cloud-integrated datacenters. The results confirm that treating storage security and backup resilience as interdependent design objectives leads to stronger protection and improved operational consistency compared to fragmented solutions.

While the proposed architecture addresses many critical challenges, future work can extend this research by exploring intelligent backup optimization using machine learning, zero-trust storage access models, and post-quantum cryptographic techniques. Additionally, large-scale real-world deployments across multiple cloud providers would provide further insights into long-term operational behavior and cost efficiency.
In conclusion, this research demonstrates that a unified secure storage and backup architecture is both feasible and effective for cloud-integrated datacenters. The findings offer valuable guidance for researchers and practitioners seeking to enhance data protection, resilience, and trust in increasingly distributed cloud environments.

REFERENCE

1. Azarudeen, A., Ganesh, N., Dinesh, R., & Ramakrishnan, R. (2015). Secure Storage using TPC-C in Cloud. International journal of scientific research in science, engineering and technology, 1, 58-61.
2. niak, M.B., Jankowski, G., Jankowski, M., Jankowski, S., Jankowski, T., Meyer, N., ajczak, R.Ł., Zawada, A., & Zdanowski, S.Ł. (2013). TITLE: NATIONAL DATA STORAGE 2: SECURE STORAGE CLOUD WITH EFFICIENT AND EASY DATA ACCESS.
3. Sugumar, R., & Imam, S.B. (2015). Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage. Indian journal of science and technology, 8, 1-5.
4. SuryakantBhise, A., & PhursuleR., N. (2015). A Review of Role based Encryption System for Secure Cloud Storage. International Journal of Computer Applications, 109, 15-20.
5. Tiwari, D., & Gangadharan, G.R. (2015). A novel secure cloud storage architecture combining proof of retrievability and revocation. 2015 International Conference on Advances in

Computing, Communications and Informatics (ICACCI), 438-445.
6. Patil, A.A., & Kulkarni, D. (2015). A Survey On: Secure Data Deduplication on Hybrid Cloud Storage Architecture. International Journal of Computer Applications, 110, 29-32.
7. Wang, C., Ni, J., Xu, T., & Ju, D. (2013). TH_Cloudkey: Fast, Secure and Lowcost Backup System for Using Public Cloud Storage. 2013 International Conference on Cloud and Service Computing, 36-41.
8. Xi, L. (2013). A Cloud Storage-based Database Secure Backup System. Netinfo Security.
9. Aparna, M., Patil, A., & Kulkarni, P.D. (2015). Secure Cloud Deduplication on Hybrid Cloud Storage Architecture.
10. Balineni, M.B., & Rafi, H.M. (2015). A Novel Secure Architecture for Encipher of Public Cloud Storage. International Journal of Research, 2, 655-660.
11. Fu, Z. (2012). Android-based Personal Cloud Secure Storage System. Science Technology and Engineering.