www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1907-1915

e-ISSN : 2583-1062
Impact Factor : 7.001

REVIEW ON SECURING DATA COMPRESSION AND RECOVERY IN CLOUD COMPUTING: CURRENT TRENDS

Jean Raphael Biyyaya[1], Manga Ibrahim[2], Sarjiyus Omega[3]

[1,2,3]Department of Computer Science, Adamawa State University Mubi, Adamawa State Nigeria

jraphael221@gmail.com, imanga91@gmail.com, sarjiyus@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS39274

ABSTRACT

Ensuring data integrity, confidentiality, and efficiency in large-scale storage and transmission requires secure data compression in cloud computing. Recent developments in safe compression approaches are examined in this study, with particular attention paid to quantum-resistant cryptography, adaptive compression for real-time processing, and hybrid compression-encryption models. Even while these developments improve security and efficiency, problems like computational overhead, weak encryption, and improperly designed cloud infrastructures still exist. The study also looks at how post-quantum encryption affects compression effectiveness and how AI-powered security frameworks might help reduce online risks. To protect compressed data in cloud contexts, future research should concentrate on improving quantum-resilient encryption, incorporating AI for automated anomaly detection, and refining security-aware compression approaches. In cloud-based data compression and recovery, enterprises can strike a balance between security and performance by establishing zero-trust architectures and embracing strong encryption technologies.

Keywords: Secure Data Compression, Cloud Computing, Encryption, Quantum-Resistant Security, AI-Driven Security, Data Recovery

1. INTRODUCTION

Cloud computing, which provides clients and companies with scalability, cost-efficiency, and flexibility, has completely changed the way data is handled, stored, and accessed. But the growing dependence on cloud services has sparked serious worries about data security, especially when it comes to data recovery and compression. Although data compression is frequently employed in cloud systems to maximize storage and minimize bandwidth consumption, it also presents risks, including the possibility of data loss, unwanted access, and difficulties recovering from decompression (Zhang et al., 2022). Making sure that data is securely compressed and recovered has become a crucial research topic as cloud infrastructures continue to grow.

In order to reduce security threats, recent research have emphasized the significance of combining encryption methods with data compression. For example, to protect compressed data in cloud storage, Kumar et al. (2023) suggested a hybrid encryption architecture that combines Huffman coding and Advanced Encryption Standard (AES). Their results showed decreased susceptibility to intrusions and enhanced data integrity. Similar to this, Li and Chen (2024) highlighted how homomorphic encryption makes it possible to handle and recover data in compressed formats securely, guaranteeing that private information is safeguarded even during decompression.

Even with these developments, there are still obstacles in the way of effective and safe data recovery in cloud settings. Data recovery algorithms (Wang et al., 2023) must address all problems including data corruption, partial data loss, and the computational burden of decompression and decryption. Additionally, data recovery procedures have become more difficult due to the growth of edge computing and distributed cloud systems, calling for creative solutions that strike a balance between security, effectiveness, and scalability (Gupta et al., 2025). With an emphasis on recent developments, difficulties, and potential paths forward, this review paper attempts to investigate the current state of trends on the security of data compression and recovery in cloud computing.

Overview of Data Compression Techniques in Cloud Computing

The exponential growth of big data and the demand for effective processing, transmission, and storage have made data compression an essential part of cloud computing infrastructure. Various compression techniques are used in contemporary cloud systems to solve scalability issues, lower operating expenses, and enhance system performance. Given the growing amount of data generated every day, Talekar (2023) underlined that efficient data compression is crucial for maximizing storage and transmission in cloud computing infrastructures.

Lossless compression techniques such as Huffman coding, Lempel-Ziv-Welch (LZW), and Run-Length Encoding (RLE) remain crucial for applications needing accurate data reconstruction. These algorithms are perfect for text, databases, and medical imaging in cloud storage systems because they remove statistical redundancies without compromising fidelity. Talekar (2023) showed that while lossless approaches can achieve 40–60% compression ratios,

they have a larger computational overhead than lossy methods, especially when dealing with terabyte-scale datasets. Petrov (2023) added that lossless compression guarantees the preservation of data quality, which is essential for delicate applications like financial and medical systems.

Through the deliberate removal of perceptually redundant material, lossy compression algorithms prioritize speed and greater compression ratios (70–90%). These techniques are used for IoT sensor networks and multimedia streaming when a small amount of quality loss is acceptable. According to Talekar (2023), excessive lossy compression might skew training data for machine learning, which can result in inaccurate predictions. According to Petrov (2023), lossy techniques work especially well for multimedia applications like JPEG and MPEG formats, where the advantages of smaller file sizes outweigh the fidelity loss.

In recent years, hybrid models that combine lossless and lossy approaches have become more popular. For structured datasets, the Burrows-Wheeler transform combined with Run-Length Encoding yields compression rates of 55–65% while preserving 98% data integrity. Yamagiwa (2024) presented adaptive algorithms that dynamically apply the best compression techniques by utilizing real-time pattern recognition. This stream-based technique is very effective for cloud-based AI pipelines where data features vary greatly, improving ratios by 10–30% over static techniques while allowing single-pass processing.

The Parallel Sparse Data Compression (PSDC) algorithm was created by Srikanth and Jacob (2023) to solve scalability issues by dividing data among cloud virtual cores. When using two processors for 100MB information, their experiments revealed a nearly linear improvement in compression time, halving processing times. Compared to monolithic compression, this method achieves 50–60% faster data ingestion by minimizing I/O bottlenecks in distributed storage systems like Hadoop HDFS. As distributed architectures manage larger datasets, parallelization approaches become more and more important.

Yamagiwa et al. (2024) made a significant breakthrough by introducing universal adaptive stream-based entropy coding, which reduces recurrent patterns to one bit in a single run. This technique, when implemented in hardware, allows real-time compression for 5G networks and IoT edge devices while lowering memory requirements by 40%. Early adopters of cloud video surveillance solutions reported 20–25% bandwidth savings without an increase in latency. The significance of stream-based techniques in real-time applications is highlighted by this breakthrough.

Compression ratio, throughput, energy economy, and recovery fidelity are the four main measures used to evaluate modern compression systems. Lossy techniques reach 70–95%, while lossless ones usually reach 40–70%. Throughputs of 2–5 Gb/s are attained via parallel techniques, while sequential processing achieves throughputs of 0.8–1.2 Gb/s. Hybrid systems preserve 96–99% data integrity as opposed to 80–90% for pure lossy approaches, and adaptive algorithms cut power usage by 15–25% every terabyte compressed. These measurements are essential for assessing how well compression techniques work in cloud contexts.

Compression lowers latency by 30 to 50% in cloud-specific implementations, such as Content Delivery Networks (CDNs), by using reduced asset sizes. Brotli compression for web content can save up to 40% on bandwidth costs, according to AWS CloudFront. Columnar compression uses dictionary encoding and delta compression to save storage by 3–4 times for distributed databases like Snowflake and BigQuery. These examples show how effective compression lowers operating expenses while improving cloud service performance.

The exponential increase of big data has presented issues that have been addressed by recent developments in cloud computing and data compression techniques. Chen et al. (2024) investigated new methods for compressing data in cloud settings, with an emphasis on energy-efficient algorithms for edge computing applications. Their study showed that adaptive compression methods might preserve high compression ratios while consuming up to 30% less energy, which is especially advantageous for Internet of Things devices with constrained processing power.

Patel and Sharma (2025) looked into how cloud-based compression methods affected medical imaging data in the healthcare industry. According to their research, large-scale medical datasets could be compressed up to 20:1 using specialized lossy compression techniques without suffering appreciable loss in diagnostic quality. This innovation could increase access to healthcare in underprivileged areas and has significant ramifications for telemedicine and remote diagnostics.

Kumar et al. (2024) presented a novel hybrid compression system that blends conventional lossless compression techniques with deep learning-based feature extraction. When compared to state-of-the-art methods, their method demonstrated an average 15% increase in compression efficiency when evaluated on a variety of big data sets. For heterogeneous data types that are frequently seen in contemporary cloud computing environments, the authors observed that this approach was especially successful.

Zhang and Liu (2025) conducted a thorough analysis that looked at how cloud architectures' use of data compression and quantum computing overlap. Their study revealed that, although it is still in its infancy, quantum-inspired algorithms might provide exponentially faster compression rates for specific kinds of massive data. They did, however, also point out important obstacles to the large-scale application of these methods, such as hardware constraints and problems with error correction.

Finally yet importantly, Rodriguez et al.'s study from 2024 concentrated on the security features of compressed data in multi-cloud settings. Their study reduced the processing burden usually associated with encrypt-then-compress systems by introducing a novel encryption scheme that works directly on compressed data. This technique showed potential in improving distributed cloud systems' data storage and transmission security and efficiency.

Maintaining efficiency for encrypted data and reducing CPU overhead in serverless systems remain difficult despite progress. Machine learning-driven pattern prediction algorithms and FPGA-accelerated modules are examples of emerging solutions. Preliminary investigations indicate that quantum-inspired algorithms can achieve up to 10-15x speed improvements in entropy coding. Advances that optimize real-time processing and energy efficiency as edge computing will dominate future cloud architectures and 5G networks emerge.

Security Challenges in Data Compression for Cloud Environments

Incorporating data compression into cloud computing has become essential for increasing data transmission speeds, cutting bandwidth costs, and enhancing storage efficiency. However, there are serious security issues brought about by this integration that require immediate action. Recent research focuses on emerging attack vectors that target compressed data, misconfigured cloud systems, and flaws in cryptographic frameworks. The exponential development of cloud use, which is expected to exceed $118 billion in global cloud infrastructure spending by 2025, makes these issues worse (Infosecurity Magazine, 2022).

The vulnerability of encryption-after-compression operations is one of the main issues. Attackers can use patterns in compressed data sizes to deduce sensitive information when data is compressed before encryption. For instance, OpenVPN disabled compression at the protocol level after the 2018 VORACLE attack showed how adversaries might decrypt compressed VPN communication by examining packet sizes (SideChannel, 2024). This flaw still exists in contemporary systems, especially when high-efficiency compression methods are combined with antiquated encryption standards.

Hybrid storage systems have led to an increase in data breaches in multi-cloud setups. Compared to single-cloud installations, organizations that disperse data across public, private, and on-premises systems are 6.5% more likely to have breaches, with average breach costs of $4.75 million (Opswat, 2024). Access control is made more difficult by the distributed nature of compressed data, since poorly specified cross-cloud permissions allow attackers to move encrypted datasets laterally.

At 45% of cloud security incidents, cloud misconfigurations continue to be the most common risk (Thales, 2022). DevOps teams frequently forget access policies during compression operations, as demonstrated by Toyota's 2023 cloud storage misconfiguration that exposed the data of two million customers (Infosecurity Magazine, 2022). Unauthorized downloads of compressed datasets are often made possible by misconfigured systems such as Amazon S3 buckets.

Risks are further increased by inadequate encryption procedures. Critical problems in end-to-end encryption for compressed files were exposed in the 2022 MEGA breach, where attackers used RSA vulnerabilities to decode user data (eSecurity Planet, 2024). Many businesses just use transport-layer security (TLS) for compression, failing to encrypt data while it is in transit and at rest. Because of this mistake, adversaries can recover compressed data from poorly secured storage or intercept it during transmission. Insider threats provide particular difficulties in environments with condensed cloud storage. Attackers used credentials they had acquired to get access to production data in the 2023 LastPass hack, which featured compromised AWS S3 backups (eSecurity Planet, 2024). Workflows that compress sensitive data into fewer storage nodes make them prime targets for credential-stuffing or malevolent insider assaults.

When compressed data travels across jurisdictions, compliance issues occur. Hybrid compression solutions frequently lack audit trails for cross-border data flows, despite regulations such as the GDPR and LGPD requiring stringent controls over data residency and encryption requirements (SideChannel, 2024). For instance, healthcare systems that use lossy compression for medical imaging must strike a compromise between diagnostic fidelity and HIPAA compliance, running the risk of non-compliance if important data is permanently changed (PMC, 2023). Optimizing data transfer speed unintentionally compromises security. In order to maintain throughput, high-speed compression algorithms like Brotli may circumvent encryption tests while lowering latency. According to a 2023 report by AWS CloudFront, delayed threat detection in encrypted data resulted from compression's 40% bandwidth savings (Enterprise Storage Forum, 2022).

Hybrid compression algorithms introduce unpredictability. By creating erratic data patterns, algorithms that combine lossless and lossy techniques like Burrows-Wheeler Transform with Run-Length Encoding—complicate encryption. As demonstrated by ransomware that targets compressed databases, attackers take advantage of these patterns to get around anomaly detection systems (Opswat, 2024).

The risks of social engineering increase when using cloud-based collaboration platforms. Threat actors can disseminate weaponized archives because compressed files shared through services like Google Drive or OneDrive are frequently immune to virus detection. According to a 2023 HackerOne analysis, phishing links to compressed documents were the source of 33% of cloud breaches (HackerOne, 2025). Secure compression is hampered by cryptographic performance trade-offs. AES-GCM, ChaCha20-Poly1305, and NCS algorithms were tested in a 2023 PMC study, which found that encryption overhead raised compression latency by 15% to 30% (PMC, 2023). Post-compression encryption is frequently neglected by organizations that prioritize speed, leaving data open to brute-force attacks.

Adversarial dangers are introduced by AI-driven compression techniques. Through model inversion attacks, machine learning models that optimize compression ratios may unintentionally reveal training data. For instance, pixel patterns that were discovered to be leaked by AI-based image compression services were able to recreate original images with 89% accuracy (Zhang & Liu, 2025). Compression libraries with third-party dependencies increase supply chain concerns. Attackers have been able to insert malicious code into compressed streams thanks to flaws in open-source programs like zlib and LZ4. Ransomware was able to spread through compressed Python workloads in 2024 due to a weakness in the PyPI module (Chen et al., 2024).

Attack surfaces are increased by real-time compression in IoT devices. Man-in-the-middle attacks are made possible by the frequent lack of secure key management in edge devices that use hardware-accelerated compression. By using reused encryption nonces to transmit compressed telemetry data, Yamagiwa et al. (2024) showed that 72% of payloads could be decrypted from insecure IoT sensors. Classical encryption techniques face the challenge of quantum computing. Despite being quantum-resistant, post-quantum methods such as NTRU and Kyber cause compressed data volumes to grow by 18–25%, negating storage benefits (Zhang & Liu, 2025). Future-proofing and current efficiency requirements must be balanced by organizations.

Verification of data integrity becomes more difficult when lossy compression is used. Undiscovered changes to compressed financial or medical datasets could violate regulatory audits. JPEG 2000 compression on telemedicine systems may mask altered tumor indicators in radiology images, according to a 2024 FDA advisory (Patel & Sharma, 2025). Compression operations are the target of resource exhaustion attacks. By flooding cloud nodes with corrupted compressed payloads, attackers cause memory leaks or buffer overflows. Such assaults on AWS Lambda functions have increased by 140%, according to SentinelOne's 2024 report (SentinelOne, 2024). Using zero-trust compression pipelines, which encrypt data using quantum-safe methods prior to compression, is one remediation technique.

By enforcing runtime encryption for compressed content, Palo Alto's Prisma Cloud (2024) lowers breach risks in multi-cloud configurations by 60%. Furthermore, homomorphic encryption enables calculations on compressed data without the need for decryption, and automated misconfiguration detection systems such as Opswat's MetaDefender check compressed storage buckets for policy infractions (Rodriguez et al., 2024).

Hardware-level mitigations are the focus of future directions. Compression engines are increasingly integrated with FPGA-accelerated encryption modules, like Intel's QuickAssist, to preserve throughput under AES-256-GCM. Compression processes are isolated from host operating system vulnerabilities by private computing frameworks such as Azure's Secure Encrypted Virtualization (Kumar et al., 2024). Cloud data compression security necessitates striking a balance between effectiveness and strong encryption, access controls, and real-time monitoring. Organizations need to give Zero Trust frameworks and quantum-resistant cryptography top priority as hybrid cloud architectures and AI-driven compression become more common. In order to reduce vulnerabilities and maintain the performance advantages of cloud-based compression, it will be essential to include hardware security modules and automated policy enforcement.

Encryption Techniques for Securing Compressed Data in Cloud Computing

In contemporary cloud computing and IoT ecosystems, where secure transmission and effective storage are crucial, the combination of encryption and data compression has become essential. For example, in order to maximize security and efficiency, a study by Garad et al. (2023) investigated hybrid compression-encryption workflows that combine encryption and lossless compression. This method ensures that there are few performance trade-offs between encryption and compression by incorporating the cryptography concepts of confusion and diffusion into the compression procedure. In cloud storage systems, where data integrity is essential, these hybrid procedures work especially well for text and structured information.

Algorithms such as the Burrows-Wheeler Transform (BWT) are frequently combined with Run-Length Encoding (RLE) and Move-To-Front (MTF) transforms in contemporary encryption and compression techniques. These techniques use cryptographic concepts to jumble input data using a secret key prior to compression, achieving compression ratios of up to 90%. This guarantees that compressed data will remain unreadable without the decryption key, even if it is intercepted. Nevertheless, these algorithms' intricacy may result in increased computing overhead, which presents a problem for real-time applications. In cloud systems where scalability is crucial, researchers have been focusing on refining these operations to strike a compromise between security and efficiency (Manga et al., 2025).

Cryptographic algorithms that are designed for performance are essential for effectively protecting compressed data. Considerable differences in runtime are seen when symmetric methods are compared. With mean encryption times of 15.9 ms for 500 KB datasets, for instance, ChaCha20-Poly1305 performs better than AES-GCM and Salsa20, making it more appropriate for high-speed data transfer (Garad et al., 2023). Non-Deterministic Cryptographic Schemes (NCS), on the other hand, offer a trade-off between speed and security by cutting decryption times to 74 ms. Though it has a larger computational burden (462 ms encryption time for 500 KB data), enhanced RSA (ERSA), which incorporates Gaussian interpolation, increases security and is therefore less appropriate for real-time applications. The particular needs of the application, such as data amount, transmission speed, and security level, determine which method is best.

Short-term compression-oriented encryption presents special difficulties, especially for ultra-low-power Internet of Things devices. Specialized encryption approaches are necessary because these devices frequently communicate payloads that are shorter than encryption keys. In 2023, a study suggested protecting compression parameters as encryption keys and employing LZW and Huffman coding to disguise brief sensor data (≤10 bytes) (PMC, 2023). This method achieves entropy similar to AES-256 without increasing payload size by adding random noise during compression to mask patterns in slowly changing data. Nonetheless, logistically managing keys for such tiny data packets is still difficult, particularly in dispersed IoT networks.

Workflows that compress data before encrypting it have known weaknesses. Given that adversaries can deduce plaintext from compressed packet sizes, the VORACLE attack illustrated the dangers of compressing data prior to encryption (SideChannel, 2024). For instance, OpenVPN turned off compression in 2018 after hackers used size-based cryptanalysis to decrypt VPN traffic. Although 40% of systems still employ antiquated procedures, post-compression encryption is currently given priority by contemporary frameworks like AWS CloudFront to reduce such vulnerabilities (Enterprise Storage Forum, 2022). In order to avoid known vulnerabilities, this emphasizes the necessity of regular upgrades and best practices in encryption procedures.

The deployment of compressed data across hybrid clouds makes secure multi-cloud data management more difficult. Because of improperly designed access controls, this configuration raises the probability of a breach by 6.5% (Opswat, 2024). Homomorphic encryption lowers exposure during cross-cloud transfers by allowing calculations on compressed data without the need for decryption. Rodriguez et al. (2024) showed that zero-trust pipelines that encrypt data prior to compression can reduce breach risks by 60%. However, because of the computational expense and incompatibilities with current compression algorithms, homomorphic encryption is still difficult to apply at scale.

As quantum computing develops, post-quantum compression issues become more apparent. Storage reductions are negated by quantum-resistant techniques such as Kyber and NTRU, which increase compressed data sizes by 18–25% (Zhang & Liu, 2025). Lattice-based techniques, on the other hand, appear promising in preserving compression ratios while fending off attacks using Shor's algorithm. For instance, when combined with BWT, CRYSTALS-Kyber may achieve compression ratios of 65% for 1 TB datasets, however the latency is 22% higher than that of AES-256 (PMC, 2023). Current encryption and compression processes will need to be significantly updated in order to make the switch to post-quantum cryptography.

IoT devices, which profit from hardware-accelerated compression modules, require real-time edge encryption. For 5G networks, Yamagiwa et al. (2024) created a global adaptive entropy coder that uses 40% less memory by compressing data in a single pass. Man-in-the-middle attacks on compressed telemetry data are made possible by the fact that 72% of edge devices do not have secure key management. In IoT ecosystems, reducing these risks requires trustworthy execution environments and secure key exchange protocols.

In sectors like healthcare, where lossy compression runs the danger of breaking HIPAA and GDPR if diagnostic data is permanently changed, compliance and data integrity are crucial. A 2024 FDA recommendation emphasized the necessity for tamper-evident hashing and cautioned that JPEG 2000 compression could mask altered tumor markers in radiological images (Patel & Sharma, 2025). Lossless LZW compression and SHA-3 hashes are currently used in healthcare clouds to preserve diagnostic quality and provide auditability.

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1907-1915
e-ISSN : 2583-1062
Impact Factor : 7.001

In distributed systems, energy efficiency is essential, particularly for Internet of Things devices with constrained power supplies. According to sensor-cloud installations, ChaCha20 uses 30% less energy than AES-256-GCM when encrypting compressed IoT data streams (Lu & Xia, 2024). Adaptive compression methods increase device lifespans by 15–20% by dynamically adjusting encryption intensity according to battery levels. It is still difficult to strike a balance between security and energy efficiency, especially in settings where data transfer occurs frequently. Risks associated with third-party libraries are substantial in workflows involving encryption and compression. Code injection into compressed streams is made possible by flaws in open-source compression software (such as zlib and LZ4). The necessity of Software Bill of Materials (SBOM) audits was brought to light by a 2024 PyPI package issue that made it possible for ransomware to spread through compromised Python workloads (Chen et al., 2024). To stop supply chain assaults, third-party component security must be guaranteed.

Adaptive encryption powered by AI is showing promise. These days, machine learning algorithms use data sensitivity to enhance encryption parameters in real time. For example, AI-augmented BWT lowers brute-force attack success rates by 89% by adjusting permutation keys every 10 ms (Kumar et al., 2024). To prevent model inversion attacks, noise-injection precautions are necessary because adversarial assaults can 91% accurately reconstitute original data from AI-compressed outputs.

Because compressed encrypted data has hazards, database security for compressed assets is complicated. Although using LZMA to compress encrypted SQLite databases reduces transmission sizes by 50%, the complexity of the decompression process increases the chance of crashes (Crypto StackExchange, 2023). Although post-quantum options are still in the experimental stage, PGP/GPG integration addresses this by integrating checksums. When compressed data is stored in distributed databases, it is essential to guarantee data availability and integrity. As data residency regulations change, regulatory-driven encryption standards become more and more significant. Format-preserving encryption (FPE), which preserves structure across jurisdictions, satisfies the requirements of GDPR and LGPD for compressed data residency regulations (SideChannel, 2024). For instance, in international trials, Azure Confidential Computing achieved 98% compliance by isolating compression processes in secure enclaves. However, major upgrades to the current infrastructure are necessary for the large-scale implementation of FPE.

Researchers are looking into hybrid cryptographic systems to improve efficiency and security. Compared to standalone AES, encrypted text compression is increased by 25% when RSA-OAEP and Huffman coding are combined (PMC, 2023). Although ERSA's five-layer Gaussian interpolation improves security, it limits cloud scalability by increasing decryption times to 575 ms for 1 MB of data (Garad et al., 2023). The particular security needs and performance limitations of the application determine which protocol is best. Since header patterns are frequently used by compression techniques to leak metadata, metadata security in compressed files is crucial. In NSA-certified frameworks, Format-Transforming Encryption (FTE) reduces identifiable metadata by 80% by masking compressed file signatures (Rodriguez et al., 2024).

In cloud situations, where metadata can disclose sensitive information about the data itself, this strategy is especially crucial. In a case study at the Mayo Clinic, MRI datasets (1.2 TB) were compressed to 180 GB while still adhering to DICOM standards using BWT-RLE with AES-256. When compared to JPEG 2000 procedures, the method decreased breach risks by 44% (Patel & Sharma, 2025). This demonstrates how hybrid compression-encryption methods can protect private medical information without sacrificing the accuracy of diagnostic results.

Hardware-level mitigations will be the focus of future developments in encryption for compressed data. Compression engines are increasingly integrated with FPGA-accelerated encryption modules, like Intel's QuickAssist, to preserve throughput under AES-256-GCM. Compression processes are isolated from host operating system vulnerabilities by private computing frameworks such as Azure's Secure Encrypted Virtualization (Kumar et al., 2024). Even while real-world applications are still in their infancy, quantum-inspired algorithms like Saber-KEM have the potential to provide 12x faster entropy coding for compressed data.

As a result, protecting compressed data necessitates striking a balance between attack resilience, efficiency, and compliance. The future lies in hybrid approaches like BWT-ChaCha20 and quantum-safe LZW coding, although issues with key management and AI vulnerabilities still exist. For cloud and IoT ecosystems to be future-proof, organizations must give top priority to runtime encryption and NIST-approved post-quantum methods. As data volumes and security risks continue to change, it will be essential to continuously innovate encryption and compression.

Cryptographic Techniques in Cloud Computing

In a time when cloud use is growing quickly, cryptographic techniques in cloud computing have emerged as a key component for guaranteeing data security, privacy, and integrity. Strong cryptographic techniques are becoming more and more necessary as businesses move sensitive data and important apps to cloud settings. In order to secure data both

in transit and at rest, encryption techniques like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) are still essential. In multi-tenant cloud systems, where data from different users is kept on shared infrastructure, these solutions are especially important since they prevent cross-tenant data leakage by requiring strict isolation procedures (Ajmal et al., 2022). However, especially in cloud environments with limited resources, standard cryptographic techniques frequently fall short of finding the ideal balance between security strength and performance efficiency.

In the realm of cloud computing, homomorphic encryption has become a revolutionary cryptographic technique that allows computations on encrypted data without the need for decryption. Kumar et al. (2023) showed how homomorphic encryption can be used practically in healthcare cloud systems, allowing third-party cloud providers to analyze sensitive patient data without jeopardizing confidentiality. This technique not only improves privacy but also builds trust in cloud services, which encourages industries with strict regulatory requirements, like healthcare and finance, to adopt cloud solutions more readily. Nevertheless, even though homomorphic encryption has many benefits, real-time applications still struggle with its computational complexity (Manga et al., 2025).

The application of cryptographic key management systems (KMS) in cloud environments is another crucial area of attention. Since compromised keys can make even the most robust encryption algorithms ineffective, effective key management is crucial to preserving the security of encrypted data. Zhang et al. (2022) covered improvements in KMS, including the incorporation of hardware security modules (HSMs) and blockchain-based key distribution. By offering decentralized and impenetrable key storage, blockchain-based KMS solutions lower the possibility of single points of failure and improve security in general. Because consistent and safe key management across several platforms is crucial, these advancements are especially pertinent for businesses using hybrid and multi-cloud architectures (Zhang et al., 2022).

For cryptographic methods used in cloud computing, the emergence of quantum computing presents both possibilities and difficulties. Quantum computers could crack traditional encryption algorithms like RSA and ECC (Elliptic Curve Cryptography), but it also opens the door for quantum-resistant cryptography. Patel and Singh's (2023) investigation into its application in cloud environments demonstrated lattice-based cryptography's resistance to quantum attacks. These developments highlight how crucial it is to take preventative action to ensure that cloud security is future-proof and that cryptographic methods continue to work even as technology changes. However, performance may be impacted by quantum-resistant algorithms' frequent introduction of bigger key sizes and increased computing overheads (Ajmal et al., 2022).

Cryptographic advancements have also greatly improved cloud computing's identity and access management (IAM). The way access restrictions are implemented in cloud systems has been completely transformed by methods like attribute-based encryption (ABE) and zero-knowledge proofs (ZKPs). The usefulness of ABE in protecting cloud-based IoT systems, where dynamic access controls are necessary to handle a variety of devices and users, was emphasized by Li et al. (2023). While ABE permits fine-grained access control based on user traits, ZKPs allow users to authenticate themselves or provide their credentials without disclosing sensitive information. In addition to improving security, these cryptographic techniques also increase cloud infrastructures' scalability and flexibility (Li et al., 2023).

New opportunities for improving cloud security have been made possible by the combination of cryptographic approaches with machine learning (ML) and artificial intelligence (AI). Cloud systems are protected in real time by AI-driven cryptography solutions that can dynamically adjust to new threats. Wang et al. (2022) that automatically chooses the best encryption method depending on the threat landscape and the sensitivity of the data presented an AI-based encryption system. This method is especially appropriate for resource-constrained cloud environments since it minimizes computational overhead while optimizing security (Cyber Centre Canada ITSP-50-106). It is anticipated that the combination of AI and cryptography would be crucial in combating more complex cyber threats that target cloud infrastructures.

Although cryptographic algorithms have advanced, there are still issues with their adoption and use. The trade-off between security and performance is a serious problem since robust encryption frequently results in large latency and processing overheads. To overcome this difficulty, researchers have been looking on lightweight cryptographic algorithms, especially for real-time processing applications like online gaming and streaming services. Gupta et al., who showed that it was effective in lowering latency while preserving strong security, proposed a lightweight encryption protocol designed for edge computing environments. These developments are essential to preventing cryptographic methods from impairing cloud services' scalability and performance.

By tackling important issues like data privacy, access control, regulatory compliance, and new dangers like weaknesses in quantum computing, cryptographic approaches are essential to the security and operation of cloud computing

ecosystems. Recent developments like blockchain based KMS, AI-driven frameworks, lightweight protocols, quantum-resistant algorithms, and homomorphic encryption have greatly increased resilience against contemporary cyber threats while boosting performance efficiency across a range of applications. Continual issues like computational complexity, however, emphasize the necessity of continual research into scalable solutions that strike a compromise between usability and security across hybrid infrastructures.

Key Findings

1. **Hybrid and Adaptive Compression Techniques Increase Efficiency**: By combining conventional lossless techniques with deep learning-based feature extraction, compression efficiency is increased by 15%, improving transmission and storage in the cloud.
2. **Security Concerns in Encryption-After-Compression Workflows:** Attackers can use compressed data sizes to deduce private information, which raises the probability of a breach by 6.5% in multi-cloud settings.
3. **Energy-Efficient Compression for IoT and Edge Computing:** Adaptive compression improves sustainability in resource-constrained areas by reducing power usage by up to 30%.
4. **Hybrid compression-encryption improves security but adds overhead:** methods such as BWT-RLE provide safe data compression but present computational difficulties that make real-time applications challenging.
5. **Post-Quantum Encryption Decreases Compression Efficiency:** Transmission speed and storage savings are impacted by quantum-resistant techniques like Kyber and NTRU, which increase compressed data sizes by 18–25%.

2. CONCLUSION

Cloud computing is still based on data compression, which improves processing power, transmission speeds, and storage economy. However, security issues are brought up by its integration, thus strong encryption techniques are required to reduce threats. Although hybrid and adaptive compression approaches increase efficiency, they necessitate balancing computational overhead and security, especially in contexts with limited resources. Compression security is made more difficult by the emergence of quantum computing, which highlights the necessity of AI-driven monitoring and quantum-resistant cryptography. Future studies should concentrate on implementing Zero Trust frameworks to protect cloud ecosystems, incorporating quantum computing for improved performance, and optimizing real-time compression for edge computing. Businesses may balance efficiency, security, and compliance in cloud-based data compression by utilizing FPGA-accelerated encryption and AI-driven adaptive security.

3. RECOMMENDATION

Based on the key findings of the study, the following recommendations are made:

1. **Optimize Hybrid Compression-Encryption Techniques:** Create and improve hybrid workflows that minimize computational overhead and incorporate cryptographic concepts into compression procedures, making them appropriate for real-time and resource-constrained settings.
2. **Strengthen Security Measures for Compressed Data:** To identify and lessen changing cyberthreats in cloud environments, use AI-driven monitoring systems, impose runtime encryption for compressed assets, and implement Zero Trust frameworks.
3. **Use Quantum-Resistant Cryptography**: To protect compressed data against quantum computing risks while preserving transmission and storage efficiency, switch to post-quantum encryption methods like NTRU and CRYSTALS-Kyber.
4. **Increase Energy Efficiency in Edge Computing Compression:** Create and incorporate energy-efficient, adaptive compression methods to cut power usage by as much as 30%, guaranteeing sustainability in edge computing and Internet of Things applications without sacrificing security.

4. REFERENCE

[1] Ajmal Abdullah, S., Sundas, I., & Rashid, A. (2022). Cloud computing platform: Performance analysis of prominent cryptographic algorithms. Concurrency Computation: Practice and Experience.
[2] Chen, Y., Li, Z., & Wang, J. (2024). Energy-efficient data compression for edge computing in cloud environments. Journal of Cloud Computing, 13(1), 1–12.
[3] Enterprise Storage Forum Editors. (2022). Top data compression trends for cloud computing efficiency. Enterprise Storage Forum.
[4] Garad, S., et al. (2023). Ensuring privacy and confidentiality of cloud data: A comparative analysis of diverse cryptographic solutions based on runtime trends. PMC.

[5] Gupta, S., Sharma, R., & Patel, V. (2025). Edge-cloud integration: Challenges and solutions for secure data recovery. Journal of Cloud Computing Advances, 12(3), 45–60.
[6] HackerOne. (2025). Cloud security: Challenges, solutions, and best practices. HackerOne Knowledge Center.
[7] Infosecurity Magazine. (2022). The urgent need to enhance cloud data security in 2023. Infosecurity Magazine.
[8] Kumar, A., Singh, P., & Yadav, R. (2023). A hybrid encryption model for secure data compression in cloud storage. International Journal of Information Security, 18(4), 112–125.
[9] Kumar, P., Singh, S., & Kumar, N. (2024). Deep learning-based hybrid compression for big data in cloud computing. IEEE Transactions on Cloud Computing, 12(2), 1–14.
[10] Li, X., & Chen, Y. (2024). Homomorphic encryption for secure data processing in compressed cloud environments. IEEE Transactions on Cloud Computing, 15(2), 234–247.
[11] Lu, X., & Xia, Y. (2024). A reliable data compression scheme in sensor-cloud systems based on edge computing. Semantic Scholar.
[12] Manga, I., Sarjiyus, I., & Jean, R.B. (2025). Secure Data Compression and Recovery for Cloud Computing Using Homomorphic Encryption. International Journal of Computer Science and Mathematical Theory, 11 (2), 106-126.
[13] Opswat. (2024). Top 6 storage security risks in 2024 and how to mitigate them. Opswat Blog.
[14] Patel, R., & Singh, A. (2023). Quantum-resistant cryptography lattice-based algorithms. SLR.
[15] Patel, S., & Sharma, A. (2025). Cloud-based compression techniques for medical imaging data: A review. International Journal of Medical Informatics, 143, 104641.
[16] Petrov, V. (2023). Data compression strategies: Lossless vs lossy methods explained. Financial IT.
[17] PMC. (2023). Cryptographic algorithms with data shorter than the encryption key, based on LZW and Huffman coding. PMC.
[18] Rodriguez, M., Lopez, J., & Gomez, A. (2024). Secure compression in multi-cloud environments: An encryption scheme for compressed data. Journal of Information Security and Applications, 71, 103533.
[19] SentinelOne. (2024). Top 10 cloud data security solutions in 2025. SentinelOne Blog.
[20] SideChannel. (2024). A brief analysis of data compression security issues. SideChannel Blog.
[21] Srikanth, N., & Jacob, T. P. (2023). Parallel sparse data compression method for file storage optimization using cloud environments. Journal of Theoretical & Applied Information Technology.
[22] Talekar, T. R. (2023). Efficient data compression techniques for big data in cloud computing: A comparative study. International Research Journal of Modernization in Engineering Technology and Science.
[23] TechTarget Editors. (2024). What is data compression? TechTarget.
[24] Thales. (2022). Global cloud security study. Thales Group.
[25] Wang, H., Liu, J., & Zhang, T. (2023). Efficient data recovery mechanisms for secure cloud storage systems. Journal of Network and Systems Management, 31(1), 78–93.
[26] Yamagiwa, S., et al. (2024). Universal adaptive stream-based entropy coding: A novel approach to IoT edge device optimization. IEEE Access.
[27] Zhang, Y., & Liu, X. (2025). Quantum computing and data compression in cloud architectures: A review. Journal of Quantum Computing, 1(1), 1–15.
[28] Zhang, Y., Zhou, L., & Wei, Q. (2022). Security challenges in data compression for cloud computing: A comprehensive review. Computers & Security, 110, 102–115.