iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57414

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Secure Cloud Storage using End-to-End Encryption

Sujal Sinha[1], Mohit Shankar[2], Yash Pande[3], Kislay Kumar[4], Shivank Sharma[5], Khushwant Virdi[6]
Computer Science & Engineering Chandigarh University, Mohali, India

Abstract: ***Cloud Storage is revolutionizing how the world man- ages data by providing an incredible level of flexibility, increased capacity, and easy accessibility. Nevertheless, the technology development is associated with a number of fears related to data protection and privacy. E2EE is an end-to-end encryption concept for ensuring secure storage, transmission as well as integration of data in a cloud environment. With E2EE in place, data is encrypted right at the source and decrypted only when it reaches its intended end-points, ensuring that it remains securely hidden from eavesdroppers or other unauthorized party. As the world becomes more connected, with data housed on distant servers and traversed by broad networks, it becomes essential that one comprehends the significance of E2EE in securing cloud storage. This encryption technique does not only act as a safeguard; it is an emerging and ever-changing field that has broad implication on data protection, users' privacy and the future of Cloud-based information management. The primary goal of this paper is to provide a thorough understanding of the evolving trends and implications of End- to-End Encryption (E2EE) in the realm of secure cloud storage. By synthesizing and analysing the latest research findings and practical implementations, we aim to shed light on how E2EE fundamentally reshapes the landscape of cloud data security.***

Index Terms: End-to-End Encryption (E2EE), Cloud Storage, Security, Privacy, Trends

I. PAPER STRUCTURE

The organization of this paper is as follows: Section II provides an Introduction to the topic of secure cloud storage using End-to-End Encryption (E2EE). Section III presents the Literature Review, where we comprehensively analyse existing research and findings related to E2EE in secure cloud storage. Section IV delves into E2EE Algorithms and Technologies, offering insights into the technical aspects of encryption in this context. In Section V, we Compare E2EE with Other Security Approaches, highlighting the strengths and weaknesses of E2EE in relation to alternative security methods in cloud storage. Section VI explores Future Trends and Research Directions, offering forward-looking insights into the field's evolution. Finally, Section VII presents the Conclusion, summarizing key findings, emphasizing the significance of E2EE in secure cloud storage, and potentially offering recommendations for future research and practice.

II. INTRODUCTION

The emergence of cloud computing has completely trans- formed the manner in which we store, access, and manage data. Cloud storage services have become the backbone of modern digital infrastructure, offering unparalleled conve- nience, scalability, and accessibility.

Organizations, from small businesses to large enterprises, and individuals alike, have embraced cloud storage as a means to store and share data seamlessly across the globe. However, this digital transforma- tion has also exposed a critical concern: the safeguarding and confidentiality of data stored in cloud environments.

According to the "Cost of a Data Breach Report" by IBM Security, the worldwide mean expense incurred due to a data breach in 2020 stood at $3.86 million, with a substantial portion of these breaches involving cloud-stored data [1].

In this landscape, secure cloud storage stands as a critical pillar of information management, and within its realm, the application of End-to-End Encryption (E2EE) has emerged as a transformative safeguard. E2EE, a cryptographic technique, ensures that data remains confidential and intact throughout its journey, from the moment it leaves the sender to its final desti- nation in the cloud storage repository.

This review embarks on a comprehensive exploration of the multifaceted relationship between secure cloud storage and E2EE, delving into its principles, technologies, challenges, and promising directions to provide valuable insights for researchers, practitioners, and policymakers navigating the complexities of data security and privacy in the digital age.

©IJRASET: All Rights are Reserved

III. LITERATURE REVIEW

The paper [2] addresses the challenge of reconciling end- to-end encryption with storage optimization techniques like data deduplication in the context of cloud storage. The authors recognize the growing need for end-to-end encryption in light of recent data breaches while acknowledging that conventional encryption methods hinder storage optimization methods like deduplication. In response to this concern, they propose a novel encryption scheme that dynamically adjusts the level of security based on a file's popularity among users. Unpop- ular data is protected with robust semantic security, while popular data enjoys weaker security but significant storage and bandwidth benefits, allowing for effective deduplication. The transition between security modes occurs seamlessly on the storage server side when a file becomes popular. The paper demonstrates the scheme's security under the Symmetric External Decisional Diffie-Hellman Assumption and evaluates its performance through benchmarks and simulations. [2]

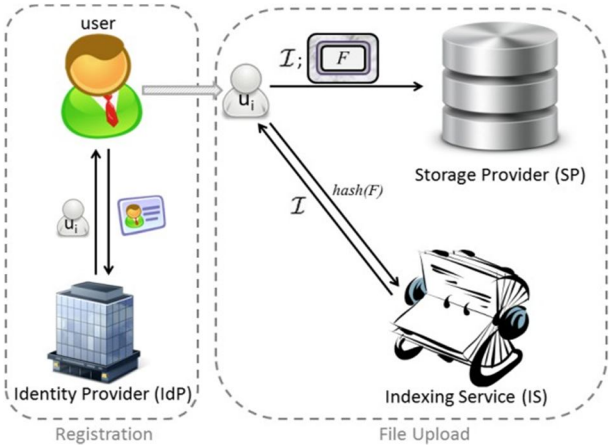


Fig. 1. Illustration of the proposed system model [2]

It offers an innovative approach to the inherent tension between data security and storage optimization in cloud stor- age. Unlike previous work that treated all files as equally sensitive, this scheme adapts security provisions based on a file's popularity, allowing for efficient data deduplication of less sensitive content. Encryption occurs at the client side, while decryption is client-independent, ensuring a seamless transition for files between security modes as their popularity changes. The authors also provide evidence of the scheme's security and scalability, making it a promising solution for enhancing the security and efficiency of cloud storage systems. [2]

Cloud computing has become a widely recognized paradigm for providing computing services, yet it presents challenges related to data management, trust, and security. Existing research has primarily focused on storage security in the cloud, but the paper [3] introduces a groundbreaking protocol called SecCloud [3]. It bridges the gap between secure storage and secure computation auditing, offering a comprehensive approach to safeguarding both data and computation in the cloud. It accomplishes deterrence of privacy breaches through designated verifier signatures, batch verification, and proba- bilistic sampling techniques. The paper also provides a detailed analysis to determine the optimal sampling size for cost minimization. [3]

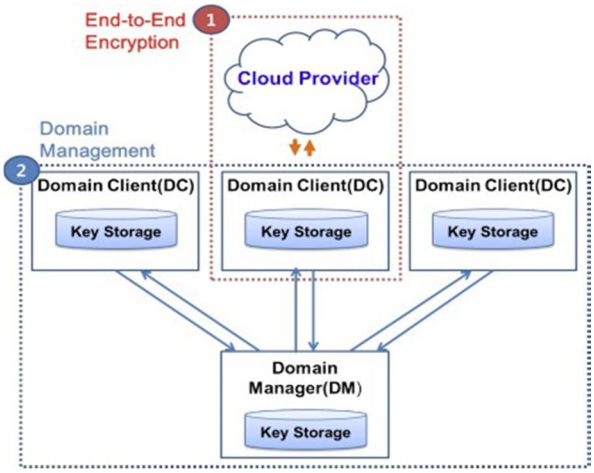


Fig. 2. The proposed EnCloud framework [4]

The efficiency of the protocol is enhanced through con- current handling of user requests using batch verification. Through extensive security analysis and performance simula- tions, the paper demonstrates the effectiveness and efficiency of SecCloud [3]. The authors plan to extend their work by considering more detailed computations, formalizing security models, addressing privacy-preserving issues, and implement- ing these advancements in real cloud platforms, such as EC2 and OpenStack, in future research. [3]

The paper [4] introduces the concept of Encrypted Cloud (EnCloud), a system designed to establish end-to-end en- cryption between cloud applications. EnCloud [4] addresses privacy concerns by securely storing data on cloud servers in an encrypted form while allowing authorized EnCloud applications to decrypt this data. The paper demonstrates the viability of EnCloud through a prototype implementation for Dropbox, showcasing that the longer wait time caused by EnCloud operations remains acceptable, amounting to just 11.5% of the execution time in total. [4]

The authors propose EnCloud [4] as a safeguard against potent adversaries, such as intelligence agencies, who may obtain info stored in the cloud. EnCloud ensures end-to-end encryption within the data owner's personal domain, safe- guarding private information kept in the cloud servers while granting authorized EnCloud applications decryption privi- leges. The prototype implementation for Dropbox validates EnCloud's feasibility, with minimal execution-time overhead. Future research will explore methods to conceal metadata attributes, further enhancing data privacy in cloud applications. [4]

To resolve the pressing issues of privacy and security in the context of public cloud environments, which are increasingly being used to store and distribute content on a massive scale, the authors of [5] introduce CloudSeal, a compre- hensive scheme designed to securely share and distribute content via public cloud services. CloudSeal [5] prioritizes content confidentiality within these environments, offering adaptable subscriber access control standards and effective content distribution through a content delivery network. This scheme combines various cryptographic techniques, including symmetric encryption, proxy-based re-encryption, k-out-of-n secret sharing, and broadcast revocation mechanisms. These algorithms enable CloudSeal to store a significant portion of encrypted content in the delivery network while storing a smaller portion in cloud storage for key management. This separation allows for flexible and scalable deployment, safeguarding cached content within the network. The authors implement and evaluate CloudSeal on Amazon Web Services, demonstrating its end-to-end efficiency and scalability. [5]

The paper presents CloudSeal [5] as a comprehensive solution to safeguard content confidentiality in large-scale systems for distributing and storing content within public cloud environments. Making use of sophisticated crypto- graphic techniques, CloudSeal addresses challenges related to content transformation, content caching, user management, and key management. The experimental implementation on Amazon's cloud infrastructure confirms CloudSeal's efficiency and scalability. Future work aims to extend CloudSeal's design to support open services, empowering users to publish content and delegate group membership control, further enhancing its practical utility and security in public cloud settings. [5]

There is a challenge of protecting user data in cloud storage against the cloud service provider itself, referred to as "privacy from the server itself" or cloud-blind storage. While End-to-End encryption has efficiently solved similar issues for messaging apps, applying this concept to apps that store and retrieve user data in the cloud remains an open problem. Existing proposals require new protocols and may not be programmable on popular commercial cloud storage services. In response, the authors of [6] propose a novel system called Portable Blind Cloud Storage (PBCS) [6] that, with the help of a key server, safely saves user data in the cloud. This system guarantees the protection of data against potential threats originating from the cloud server, key server, or unauthorized users, all the while permitting authorized users to access data on any device through the use of a passphrase. Notably, PBCS eliminates the necessity for cloud storage servers to accommodate new programmable functions, mak- ing it highly portable across various cloud storage services. The paper demonstrates the security and efficiency of PBCS through rigorous modelling, real-world network experiments over Amazon S3, and its successful deployment in Snapchat's My Eyes-Only module. [6]

ChainFS [7] is a middleware system designed to enhance the security of cloud storage services by leveraging a Blockchain with minimal trust requirements. ChainFS addresses the vul- nerability of cloud storage to forking attacks by giving users access to a file-system interface. Internally, the system stores data files in the cloud while limiting the Blockchain's in- volvement to crucial functions such as key distribution and file operation logging. The authors implement ChainFS [7] on Ethereum and S3FS and seamlessly integrate it with FUSE clients and Amazon S3 cloud storage. Their performance measurements demonstrate minimal overhead, ensuring practical usability. [7]

The paper introduces ChainFS as a multi-client file system hosted in the cloud, fortified by Blockchain security measures. It successfully mitigates the risk of forking attacks by harness- ing the Blockchain's inherent resistance to double-spending. ChainFS systematically applies these security enhancements to encrypted cloud storage, particularly in the areas of key management and file operation logging.

The authors provide a working prototype built upon S3FS and the Ethereum platform, showcasing its real-world implementation and its potential to enable secure data sharing among end users in cloud storage environments. [7]

Traditionally, cache servers need to observe content to deter- mine whether it has been cached or not, potentially violating end-to-end encryption. In response, the authors of [8] propose Cache-22, an encrypted cache system designed to overcome this catch-22 situation. What sets Cache-22 apart is its focus on deploying ability, avoiding complex cryptographic tools and depending just on conventional SSL/TLS transmission. It uses tags to make content searches more effective and gives service providers the ability to manage user access through authentication procedures. The authors implement Cache-22 using various post-quantum cipher suites, including lattice-based, code-based, and isogeny-based approaches, and demonstrate that it can significantly reduce communication between cache servers and service providers, especially in hierarchical networks. [8]

In conclusion, the paper introduces Cache-22 [8] as a novel encrypted cache system that maximizes deploying ability by leveraging SSL/TLS, offering a precise and comprehensive security definition, and presenting a working prototype using post-quantum cipher sets. Cache-22 offers substantial communication reduction benefits, particularly in hierarchical networks with varying costs. By addressing the catch-22 dilemma of cache observation in encrypted communication, Cache-22 presents a practical solution to enhance privacy while optimizing cache system performance. [8]

Post-quantum cryptography, as a burgeoning research area, seeks to create cryptography solutions that are safe in the face of potent quantum computers. The paper [9] underscores the vital role of cryptography in guaranteeing the security of diverse technologies, including internet communication, auto- mobiles, and medical devices. It underscores the impending threat of quantum computers to commonly used cryptosystems, which will become vulnerable once large-scale quantum computers become a reality. The research has made strides in identifying mathematical operations that resist quantum speedup and building cryptosystems based on these principles. However, the central challenge is to create post-quantum cryptographic solutions that maintain usability, flexibility, and trust without compromising security. [9]

Researchers have proposed various methods to address the threat of quantum computing by providing essential crypto-graphic functions like public-key encryption and signatures. Some of these proposals have withstood rigorous scrutiny, but they often come with significant network traffic overhead. Other proposals offer more efficient deployment options but raise concerns about security. [9]

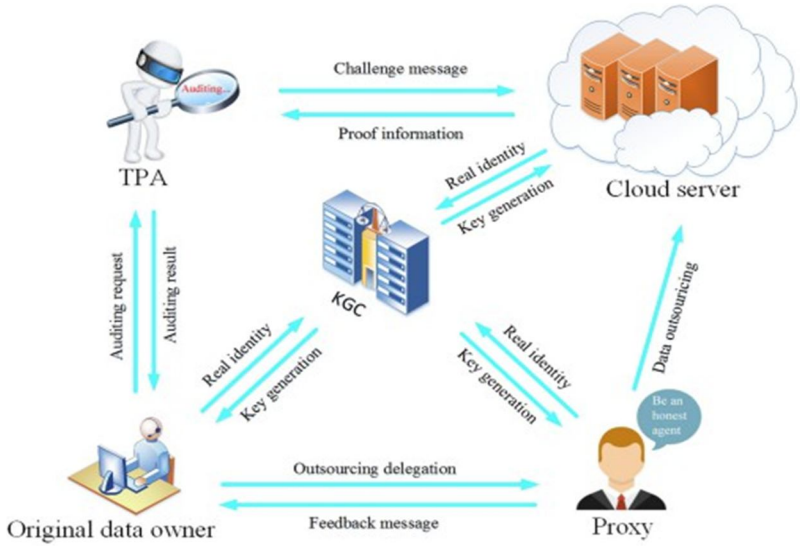


Fig. 3. The system model of DOPIV [10]

Existing public verification schemes are vulnerable to quantum adversaries, so the paper [10] introduces DOPIV, an identity-based data outsourcing program created with post- quantum security in consideration, relying on lattice-based cryptography. DOPIV [10] allows assigning a proxy to create data signatures on behalf of the actual data owner and out- sourcing them to a cloud server. Third-party auditors (TPAs) can efficiently verify data integrity on behalf of the data owner without the need to retrieve the entire dataset. DOPIV simplifies certificate management through its identity-based design. The study conducts a thorough performance evaluation and provides security proofs for DOPIV in the random oracle model, showcasing its applicability in post-quantum safe cloud storage systems. [10]

Leveraging lattice-based cryptography, DOPIV [10] ad- dresses the quantum computing threat and allows data owners to delegate data processing to proxies while enabling efficient third-party audits. The security analysis affirms its efficiency in delivering storage integrity, proxy-focused security, and data confidentiality in the face of inquisitive third-party asses- sors (TPAs). DOPIV's superior efficiency on the TPA's side enhances its practicality, making it a promising option for post-quantum secure cloud storage systems. Future work will explore enhancements using lattice-based cryptographic tech- nologies, focusing on security, performance, and functionality. [10]

A fusion of Cryptography and Steganography, has a poten- tial solution to enhance the security of cloud communications and computations. The paper [11] draws attention to how vulnerable current encryption methods—like RSA and Elliptic Curve Cryptography—are to the emerging threat that comes from quantum computing. The security of these systems relies on the difficulty of solving problems like the Integer Factor- ization Problem (IFP) and the Discrete Logarithm Problem (DLP), but as quantum computing capabilities advance, the effectiveness of these schemes diminishes. To tackle this, the study suggests a unique Crystographic System [11] that integrates Steganography and Post-Quantum Cryptography to guarantee cloud communication security in both post-quantum and classical computing eras. [11]

Crystography [11] is a potential direction for study that uses steganography and cryptography together to address security issues. With protection for both classical and post-quantum computing environments, the suggested public key multi-level security architecture seeks to give strong security for cloud computing. [11]

The paper [12] addresses the growing concern in the technology industry about the impending threat of quantum computing rendering current public key encryption schemes vulnerable. It details a tried-and-true method for putting into practice an end-to-end encryption strategy that is immune to quantum attacks in a real-world online web application. The paper emphasizes the importance of preparing for the quantum era and highlights that this implementation has shown promising results, demonstrating its feasibility without signif- icantly impacting performance compared to its pre-quantum counterpart. [12]

The transition to a quantum-resistant cryptographic era holds promise, and there is room for further research and im- provements. It [12] outlines potential future extensions, includ- ing a deeper understanding of the underlying cryptographic methods, vulnerability analysis, enhanced key storage security, testing for larger data sizes, and code optimizations. The paper's primary objective is to provide a valuable resource for future developers, offering a starting point for implementing post-quantum security in their web applications and ensuring data remains protected in the face of advancing quantum computing capabilities. [12]

Key transparency comprises two vital components: a map- ping of usernames to public keys, cryptographically committed to by the server, and an out-of-band consistency protocol for delivering concise commitments to users. The paper [13] addresses the unique challenges of implementing key transparency in real-world, production-scale scenarios. It pro- poses solutions, including a memory-optimized and privacy- preserving data structure for the username-to-public-key store, support for persistent and distributed storage, and a forward- looking concept called "compaction" to address practical is- sues arising from server data structures that continually grow. Additionally, the paper presents a consensus-less solution to efficiently distribute small and consistent commitments to users, resulting in the development of a production-grade key transparency system named "Parakeet". [13]

There is a need to consider large-scale applications, such as those involving billions of users, when implementing key transparency. It identifies gaps in previous academic-scale im- plementations and addresses these issues through the design of Parakeet [13], a key transparency system specifically tailored for large-scale deployment. The production-grade implementa- tion of Parakeet demonstrates the feasibility of their approach, showcasing its potential through practical experiments and benchmarks. [13]

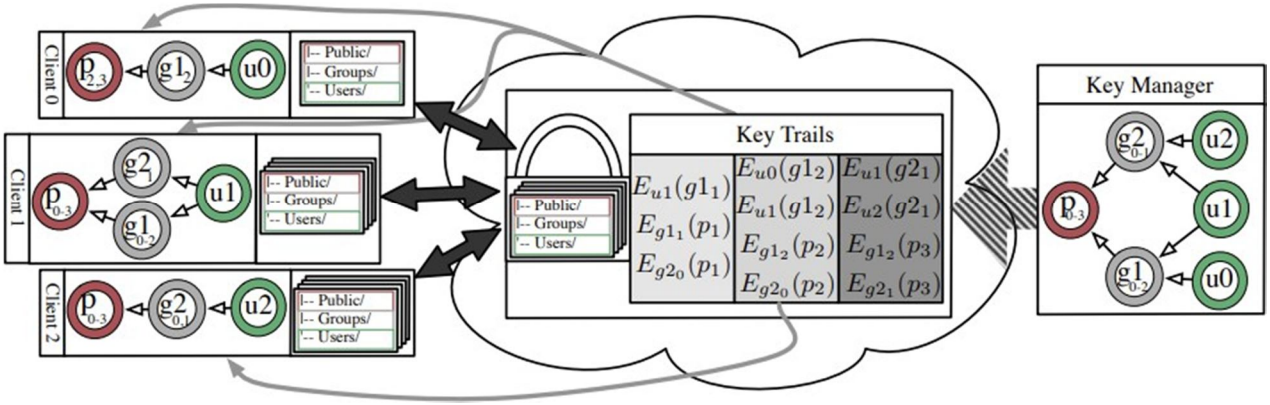


Fig. 4. Overview of proposed architecture [14]

Traditional encryption approaches fall short in supporting dynamic client access to shared data in diverse settings, such as cloud scenarios. To address this issue, the paper [14] introduces an innovative approach inspired by stream encryption methods. The graph-like representation of access rights allows for flexible join and leave operations for clients by differentiating between keys used for encrypted updates and those used for encrypting hierarchical data. This distinction enables the utilization of cloud-based infrastructures for key management without compromising data confidentiality. The proposed graph-based key management system continuously updates nodes related to changed keys, resulting in an adapt- able and scalable approach that leverages cloud resources for sharing keys and sensitive data in cooperative workflows. [14]

In reference to the paper [14], it effectively applies stream- based Key Graph methods to the realm of cloud storage, presenting a distributed architecture capable of accommodat- ing alterations among accessing clients without the necessity of re-encrypting the data. The approach's ability to update keys and access former versions, whether through a shadow structure or distributed architecture, enhances data security and accessibility. The paper also identifies areas for further improvement, such as the dispersion of key management and the incorporation of advanced security objectives such as non-repudiation. This innovative key management system addresses key challenges in secure cloud storage and has the potential to enhance data sharing and collaboration in cloud environments. [14]

As cloud computing involves dynamic resource allocation and multi-tenancy, traditional access control models fall short in providing fine-grained access control. The paper [15] intro- duces an enhanced version of the "Hierarchical attribute-set-based encryption" (HASBE) access control model to overcome the limitations of existing models. The improved HASBE model supports a hierarchical assembly of roles within a configurable domain hierarchy and a predetermined secure key distribution policy. [15]

By enhancing HASBE with hierarchical domain struc- tures and predefined key distribution policies [15], the paper addresses the challenges of fine-grained access control in dynamic cloud environments. The proposed model offers a promising approach to ensuring data security and access con- trol in the cloud and can potentially be extended to incorporate dynamic access control features in the future, enhancing its applicability and flexibility in cloud computing scenarios. [15]

IV. E2EE ALGORITHMS AND TECHNOLOGIES

End-to-End Encryption (E2EE) serves as the cornerstone of secure cloud storage, ensuring that data remains confidential and protected throughout its lifecycle. This section delves into the fundamental algorithms and technologies underpinning E2EE in the context of cloud storage.

1) *Symmetric and Asymmetric Encryption:* Symmetric encryption uses a single shared key for both encryption and decryption, offering efficiency but requiring secure key distribution. Asymmetric encryption, on the other hand, employs a pair of keys (public and private) for secure communication, ensuring confidentiality and au- thentication, but at the cost of increased computational complexity. Both encryption methods play crucial roles in securing data, with symmetric encryption prioritizing speed and asymmetric encryption emphasizing security and privacy.
2) *AES (Advanced Encryption Standard):* It is a widely adopted symmetric encryption algorithm that enhances data security by using a fixed key size of 128, 192, or 256 bits. Renowned for its efficiency and robustness, AES replaces older encryption standards like DES. It employs a substitution-permutation network to perform multiple rounds of encryption, ensuring strong protection against unauthorized access and maintaining data confidentiality across various applications, from secure communications to data storage.
3) *RSA and ECC (Elliptic Curve Cryptography):* RSA relies on the difficulty of factoring large composite num- bers, using a public key for encryption and a private key for decryption. ECC, on the other hand, leverages the mathematics of elliptic curves to achieve similar security with smaller key sizes, making it more efficient for resource-constrained environments like mobile devices. Both RSA and ECC play vital roles in securing digital communication, but ECC's advantage lies in its ability to provide strong encryption with shorter key lengths, reducing computational overhead while ensuring data privacy and integrity.
4) *Hybrid Encryption Schemes:* Hybrid encryption schemes combine the strengths of symmetric and asym- metric encryption methods. They use asymmetric en- cryption for secure key exchange, allowing parties to share a secret key while protecting it with their public keys. Once the key is established, symmetric encryption is employed for the actual data encryption, providing efficiency and speed. This hybrid approach combines the security benefits of asymmetric encryption with the com- putational efficiency of symmetric encryption, making it a versatile solution for secure data transmission and storage in various applications, striking a balance between security and performance.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

5) *Key Management and Distribution:* These involve generating, storing, distributing, and safeguarding cryp- tographic keys to ensure the security of encrypted data. Proper key management encompasses key generation pro- tocols, secure storage methods, and secure key distribu- tion mechanisms. Key distribution often relies on secure channels or protocols like Diffie-Hellman key exchange for symmetric keys or public key infrastructure (PKI) for asymmetric keys. Effective key management and distribution are essential to maintain the confidentiality, integrity, and authenticity of data in secure communica- tion and storage systems while minimizing the risk of unauthorized access or compromise of encryption keys.

V. COMPARISON WITH OTHER SECURITY APPROACHES

With End-to-End Encryption (E2EE), data is encrypted at the source and only decrypted at the point of destination, serving as a beacon of data confidentiality. It guarantees that information, even when kept on distant servers, is safe from outside surveillance. Alternative security strategies do, how- ever, exist; each has special qualities and trade-offs. For exam- ple, server-side encryption transfers the encryption burden to the cloud provider, whereas client-side encryption necessitates local encryption by the user. Access control policies allow or restrict data access based on permissions, and tokenization substitutes sensitive information with placeholders or tokens, providing data masking. A comparison of these security strategies indicates a complex environment in which decisions must take individual use cases, data sensitivity, and trust factors into account.

VI. FUTURE TRENDS AND RESEARCH DIRECTIONS

As secure cloud storage continues to evolve in the digital landscape, the integration of End-to-End Encryption (E2EE) is poised to shape the future of data security. To anticipate the emerging trends and research directions in this domain, it is essential to consider the dynamic nature of technology, security threats, and user expectations.

1) *Post-Quantum Security:* With the advancement of quan- tum computing, traditional encryption methods may be- come vulnerable. Future research will likely focus on developing and implementing post-quantum encryption techniques that can withstand quantum attacks, ensuring long-term data security in cloud storage.
2) *Homomorphic Encryption:* Research into homomorphic encryption is gaining momentum. This technology allows computation on encrypted data without the need for decryption, enabling secure and privacy-preserving data analytics in the cloud. Future studies will delve into its practical applications and optimizations.
3) *Usability and User Experience:* Balancing security with usability is an ongoing challenge. Future research will explore user-friendly E2EE implementations that do not sacrifice data security, making secure cloud storage more accessible and convenient for a broader user base.
4) *Secure Key Management:* Addressing the complexities of key management will remain a significant research area. Solutions that streamline key generation, distribu- tion, and revocation while ensuring robust security will be a priority.
5) *Quantum Key Distribution (QKD):* QKD offers an ultra-secure method for key exchange. Future research will examine the feasibility of integrating QKD with E2EE in cloud storage, providing an additional layer of quantum-resistant security.

VII. CONCLUSION

The dynamic landscape of secure cloud storage, bolstered by End-to-End Encryption (E2EE), stands at the forefront of data security in an era marked by digital ubiquity and evolving threats. Through a comprehensive literature review, we have illuminated the fundamental principles, E2EE algorithms, and technologies that underpin the safeguarding of data in cloud storage environments. This examination has revealed E2EE's paramount role in ensuring data confidentiality and integrity, offering an unparalleled shield against unauthorized access. Moreover, by comparing E2EE with other security approaches and investigating future trends, it is evident that E2EE is poised to remain central to the discourse on secure cloud storage. As we gaze into the future, the integration of post- quantum security, privacy-preserving technologies, and user- centric usability will continue to shape the trajectory of E2EE in cloud storage. In this context, researchers, practitioners, and policymakers are presented with a compelling imperative: to adapt, innovate, and collaborate in fortifying the security and privacy of data within the expansive realm of secure cloud storage. By embracing these challenges and opportunities, we pave the way for a more resilient, user-friendly, and privacy- conscious digital ecosystem that secures the data entrusted to the cloud.

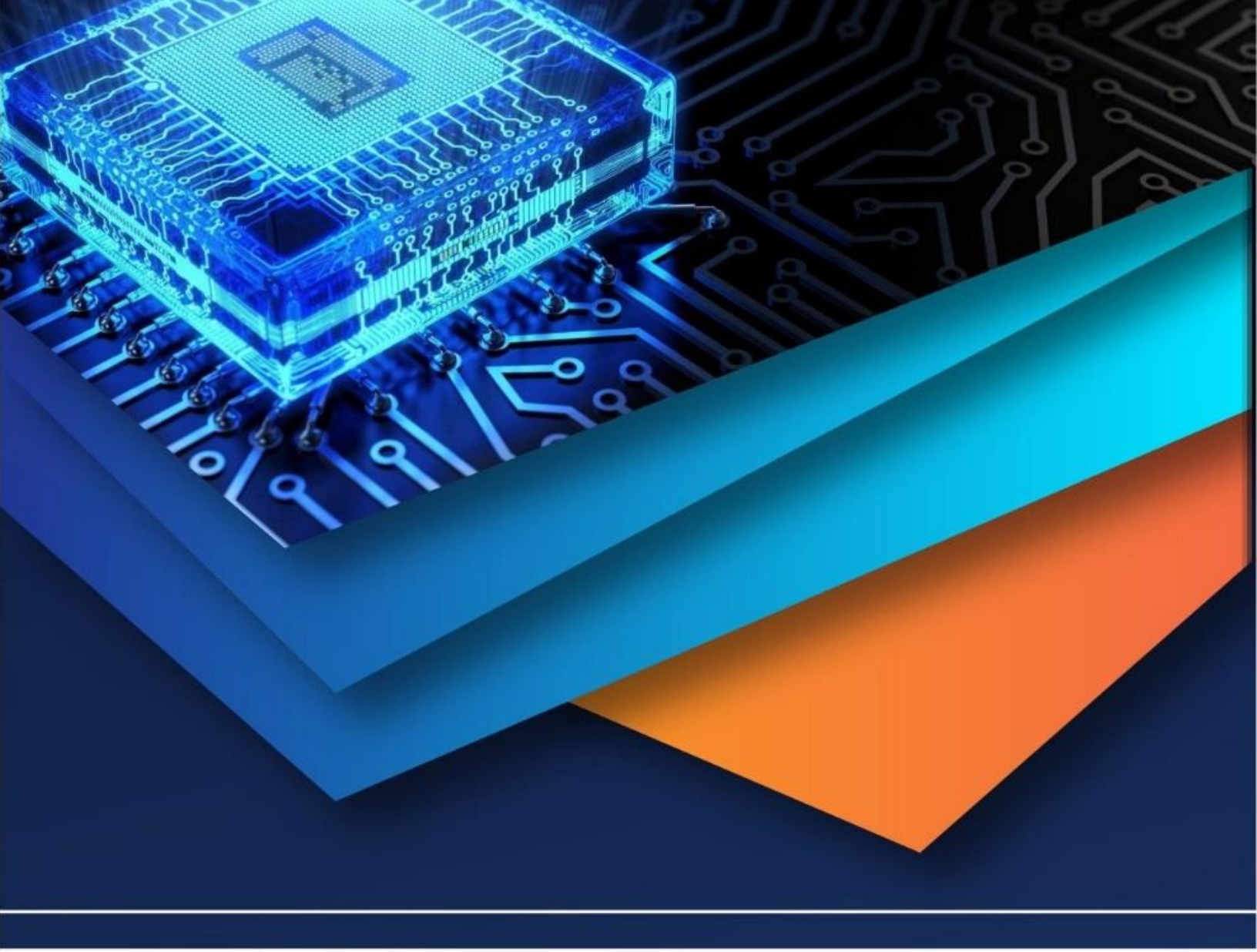
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

TABLE I
COMPARISON WITH OTHER SECURITY APPROACHES

Security Approach	Description	Advantages	Disadvantages
E2EE in Cloud Storage	Encrypts data at its source and decrypts it only at its final destination, ensuring data remains confidential throughout its lifecycle.	Exceptional data confidentiality, resilient against unauthorized access, ideal for data privacy compliance	Key management can be complex, potential performance overhead for encryption and decryption
Server-Side Encryption	Encrypts data at the cloud server, which manages keys. Clients receive and send data in encrypted form.	Simplifies client-side processes, good for collaboration and sharing	Relies on trust in cloud service provider, sensitive data may be exposed if provider is compromised
Client-Side Encryption	Data is encrypted locally on the client device before transmission to the cloud. The client manages encryption keys.	Enhanced data control and security, minimal trust in cloud provider	Key management and user responsibility, can be less convenient for collaboration
Tokenization	Replaces sensitive data with tokens or placeholders, which are reversible only with a secure key.	Effective for data masking, reduces exposure of sensitive information	May not provide complete confidentiality, requires secure token management
Access Control Policies	Enforces strict access controls and per- missions to regulate who can access and modify data in cloud storage.	Granular control over data access, complements encryption for fine-grained security	Cannot prevent data breaches in case of compromised accounts or insider threats

REFERENCES

[1] IBM Security, Cost of a Data Breach Report, Link, 2020.
[2] Stanek, Jan, et al. ”A secure data deduplication scheme for cloud storage.” Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18. Springer Berlin Heidelberg, 2014.
[3] Wei, Lifei, et al. ”Security and privacy for storage and computation in cloud computing.” Information sciences 258 (2014): 371-386.
[4] Song, Youngbae, Hyoungshick Kim, and Aziz Mohaisen. ”A private walk in the clouds: Using end-to-end encryption between cloud applica- tions in a personal domain.” Trust, Privacy, and Security in Digital Busi- ness: 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings 11. Springer International Publishing,2014.
[5] Xiong, Huijun, et al. ”Towards end-to-end secure content storage and delivery with public cloud.” Proceedings of the second ACM conference on Data and Application Security and Privacy. 2012.
[6] Chen, Long, et al. ”End-to-Same-End Encryption: Modularly Augment- ing an App with an Efficient, Portable, and Blind Cloud Storage.” 31st USENIX Security Symposium (USENIX Security 22). 2022.
[7] Tang, Yuzhe, et al. ”ChainFS: Blockchain-secured cloud storage.” 2018 IEEE 11th international conference on cloud computing (CLOUD). IEEE, 2018.
[8] Emura, Keita, et al. ”Cache-22: A Highly Deployable End-To-End Encrypted Cache System wSith Post-Quantum Security.” Cryptology ePrint Archive (2022).
[9] Bernstein, Daniel J., and Tanja Lange. ”Post-quantum cryptography.” Nature 549.7671 (2017): 188-194.
[10] Zhang, Xiaojun, et al. ”DOPIV: Post-quantum secure identity-based data outsourcing with public integrity verification in cloud storage.” IEEE Transactions on Services Computing 15.1 (2019): 334-345.
[11] Gabriel, A. J., et al. ”Post-quantum crystography based security frame- work for cloud computing.” J. Internet Technol. Secur. Trans.(JITST)
[12] 4.1 (2015): 351-357.
[13] Tutoveanu, Anton. ”Active implementation of end-to-end post-quantum encryption.” Cryptology ePrint Archive (2021).
[14] Malvai, Harjasleen, et al. ”Parakeet: Practical key transparency for end- to-end encrypted messaging.” Cryptology ePrint Archive (2023).
[15] Graf, Sebastian, et al. ”Versatile key management for secure cloud storage.” 2012 IEEE 31st Symposium on Reliable Distributed Systems. IEEE, 2012.
[16] Aluvalu, Rajanikanth, Vanraj Kamliya, and Laksmi Muddana. ”HASBE Access Control Model with Secure Key Distribution and Efficient Domain Hierarchy for Cloud Computing.” International Journal of Electrical & Computer Engineering (2088-8708) 6.2 (2016).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)