INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 10 ISSUE: 04 | APRIL - 2026 SJIF RATING: 8.659 ISSN: 2582-3930

Zero-Knowledge Cloud Platform for End-to-End Encrypted Photo Storage and Sharing

Ms.T.A.Krithika
Assistant Professor
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India

Mayank Raj
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
mayank.rj2004@gmail.com

Mugilan S
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
mugilsubramani@gmail.com

Muniappan.M
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
madank4349@gmail.com

Naveen T
Department of Computer Science and Engineering
Bharath Institute of Higher Education and Research
Chennai, India
naveen16004@gmail.com

***Abstract*—This paper defines the privacy focused alternative for popular cloud storage providers. It differentiates itself from conventional service providers by incorporating client side encryption and zero knowledge proofings. It proposes a secure, private and trust-less system for photo storage and sharing.**

***Keywords*—End-to-End Encryption(E2EE), Zero-Knowledge, Cloud Computing, Photo Storage, Cryptography, Key Management, Client-side Encryption**

I. INTRODUCTION

In the past two decades, Cloud computing, specially Storage as a Service(STaaS) has become the invisible foundation of modern digital life. For the regular individual, this service can be useful in various ways and some commonly used ones are Google Photos, Dropbox, etc. It revolutionizes how individuals and organizations manage their data. Rather than relying on local hard drives or physical storage devices, users can upload data to the cloud and access it remotely through secure interfaces. This paradigm brings several critical benefits, such as high scalability, reduced operational costs, improved reliability, enhanced accessibility, and easy data backup. These advantages make cloud storage an attractive option for businesses handling large datasets and individuals managing personal media, such as photos and videos. In fact, billions of personal files and sensitive media are now entrusted daily to these remote infrastructures, making modern digital life functionally dependent on their availability and security. This massive, global dependence underscores the critical necessity of a storage model that can guarantee both high accessibility and absolute data confidentiality.

However, while cloud services offer convenience and performance, they also introduce complex challenges in security, privacy, and trust. As the volume of stored data increases, so does the risk of unauthorized access, breaches, and data misuse. Addressing these challenges is central to building a truly secure and privacy-preserving cloud storage model.

II. BACKGROUND AND RELATED WORK

A. Cloud Storage and Privacy Challenges

[1]Cloud computing has transformed how individuals and organizations manage their digital assets, with Storage as a Service (STaaS) becoming the default method for storing sensitive media, such such as personal photos and videos. However, this convenience is compromised by complex challenges in security and privacy. Conventional STaaS relies on Server-Side Encryption (SSE), which places the service provider in control of the decryption keys. This architecture introduces significant vulnerabilities, exposing user data to data breaches, third-party legal access (such as government data requests), and potential exploitation by malicious internal administrators. These vulnerabilities pose a threat to the privacy of sensitive photo archives and can lead to identity theft or data misuse. Therefore, the current cloud environment fails to create a necessary and enforceable border between the service provider and the user's private information.

B. Existing Solutions and Their Limitations

Mainstream cloud platforms like Google Photos, Dropbox, and iCloud serve as prime examples of the centralized SSE model. While they offer superior features like deep

integration and real-time photo organization, their architecture fundamentally fails the ZK test, as they retain continuous, centralized control over the keys.A few niche second-generation ZK platforms have succeeded in implementing a CSE and E2EE. However, these solutions often face a trade-off: they may introduce noticeable performance overheads, restrict usability such as disabling live previews or smart search, or suffer from less mature synchronization and recovery processes due to the complexity of managing keys within a strict ZK perimeter.

C. Research Gap

[2]Despite the clear demand for ZK storage, there remains a significant absence of substantial research on building a zero-knowledge platform that is secure, high-performance, and user-friendly for the storage and retrieval of images on a large scale. Other commercial ZK solutions sacrifice some aspects of performance or usability, or operate under proprietary key management that is not completely transparent. This work will directly address this gap by proposing a brand new ZK-CSE architecture using a hybrid AES-ECC model along with a dynamic, multi-layered key protection scheme that ensures absolute privacy while still shown to carry the speed and low overhead requirements of mass-market multimedia consumption.

III. LIMITATIONS OF EXISTING SYSTEM

A. Centralized Key Management

Despite offering significant convenience, current mainstream cloud storage platforms such as Google Photos and other major providers operate under a model of Server-Side Encryption (SSE). This architectural decision necessitates centralized key management, where the service provider holds and maintains the master encryption keys. While data is protected in transit using Transport Layer Security (TLS), once the data reaches the provider's infrastructure, the company possesses the full capability to decrypt the stored files. This arrangement forces users into a fundamental trust deficit, as confidentiality depends on the provider's operational integrity and ability to withstand internal misuse or external legal pressures, violating the core user expectation of complete data privacy.

B. Vulnerability to Data Analysis and Mining

A less recognized but equally critical limitation of Server-Side Encryption (SSE) is that it enables the cloud provider to easily access the plaintext content for their own internal operations. Since the decryption keys reside within their infrastructure, they have unimpeded access to execute extensive data mining and analysis on user files for purposes such as improving proprietary algorithms, targeted advertising, or metadata extraction, often without explicit user knowledge or control. This practice is increasingly challenging for organizations navigating strict global regulations, such as GDPR and HIPAA, which mandate that service providers should not have access to sensitive user information. Furthermore, the ability to perpetually profile users based on the content of their photos undermines the expectation of confidentiality, creating a system of continuous, low-level surveillance. This practice effectively strips the user of data sovereignty by transforming private files into a corporate asset for passive analysis.

IV. PROPOSED METHODOLOGY AND SYSTEM ARCHITECTURE

To overcome the architectural failures of centralized key management, data mining vulnerability, and integrity loss, we propose Zero-Knowledge Client-Side Encryption (ZK-CSE) mechanism that fully delegates cryptographic control to the user. This architecture utilizes a hybrid cryptographic stack, combining the speed of symmetric encryption with the trustless security of asymmetric encryption. The following sub-sections detail the implementation of this solution, demonstrating how it enforces end-to-end privacy by ensuring that no plaintext data or decryption key ever leaves the user's local device.

A. Core Cryptography: Hybrid AES-ECC Model

[4]To effectively satisfy high security and performance efficiency, hybrid AES-ECC model has been proposed. This architecture takes the advantage of two different cryptographic families. The Advanced Encryption Standard (AES-256), an advanced encryption standard, works on better speed with linear time complexity (O(N)) making it suitable for bulk encryption of large multimedia files, in particular digital photos. On the other end, more computationally intensive Elliptic Curve Cryptography (ECC) is used only for key protection, whereby the information is secured using advanced trustless security in combination and compact key size. Key wrapping the AES data key with ECC would yield a strong shielded mathematical assurance without compromising the system's overall throughput. The hybrid approach is end-to-end secure and lightweight in its computational overhead.

B. Dynamic Key Generation

To eliminate the key reuse vulnerability inherent in static key systems, proposed architecture imposes the use of dynamic key generation, which enables cryptographic separation for every file. Just before a file gets encrypted, a unique 256-bit AES key is derived in real-time, preventing exposure of one key from compromising the entire dataset. This is accomplished by generating a high-entropy file fingerprint

(hash) from the file content itself using the SHA-256 algorithm. The file hash will then be combined through XOR with a changing cryptographic parameter. The derived key, therefore, is employed solely for that particular instance of encryption. This methodology guarantees per-file isolation, meaning the system remains resilient against replay and correlation attacks, significantly enhancing data security against external and internal threats.

C. Client-Side Encryption Logic and Data Flow

[5]This module operates on the zero-knowledge model and ensures that all cryptographic operations are performed on the user's device, satisfying the property of confidentiality protection (CSSM Property 1). The process starts at the moment the user selects a file for upload, following a multi-stage workflow to maximize data security and obfuscation. Before AES encryption, a local, low-level data transformation is performed to enhance security. By converting the file data into ASCII and binary representations, with bits split, swapped, and reversed. A key-dependent offset introduces randomness, increasing data stream complexity known as salt. This proprietary bit-level scrambling provides a secondary defense layer, ensuring data obfuscation even if AES encryption is compromised. Then a unique AES-256 key is generated and applied to the file to produce high-entropy ciphertext, securing data with high speed and secure encryption. Post-encryption, the file is divided into encrypted fragments. The AES key is encrypted using the user's ECC Public Key, ensuring decryption only with the ECC Private Key, which remains on the user's device. Only two components are transmitted to the cloud via a secure TLS tunnel: the fragmented, AES-encrypted ciphertext and the ECC-encrypted AES key. The server receives two unintelligible data streams, unable to decrypt either, thus maintaining zero-knowledge status throughout storage and transmission.

V. CONCLUSION

The primary goal of this project was to establish a secure, privacy-centric cloud photo storage system that fundamentally eliminates the inherent trust dependency on service providers, a critical failing of conventional centralized models. This objective was successfully met through the development of a Zero-Knowledge Client-Side Encryption (ZK-CSE) mechanism that fully delegates cryptographic control to the user, satisfying the requirements of Confidentiality Protection and Key Protection. The proposed hybrid scheme ensures that sensitive user data and decryption keys never leave the local device by marrying the speed of AES-256 for bulk data encryption and the trustless security of ECC Key Wrapping along with a dynamic key generation scheme. This design is restoring digital sovereignty by having such a solution that protects files not just from external attackers but even against unauthorized access from the actual provider through internal systems or analytical arms. Besides, experimental analysis has proved that the system retains a very good linear time complexity with minimal performance overhead for an adversary resisting design. The future is set toward a mobile integration of this solution with ECC energy-efficient use, followed by a redundant multi-server architecture that leads the system to a trustless, deployable structure for the next generation of privacy-aware cloud services.

REFERENCES

[1] "Enhancing cloud security: Strategies and technologies for protecting data in cloud environments," Int. J. Appl. Math. Comput. Sci. Syst. Eng., vol. 6, pp. 224–229, November 2024. doi:10.37394/232026.2024.6.18.

[2] P.-W. Chi, Y.-H. Lu, and A. Guan, "A privacy-preserving zero-knowledge proof for blockchain," IEEE J. Sel. Areas Inf. Theory, 2023. doi:10.1109/JSAIT.2023.3290666.

[3] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," IEEE Access, vol. 10, pp. 71247-71277, 2022. doi:10.1109/ACCESS.2022.3188110.

[4] S. Kumar and D. Kumar, "Securing of cloud storage data using hybrid AES-ECC cryptographic approach," J. Mobile Multimedia, vol. 19, no. 2, pp. 363–388, 2022. doi:10.13052/jmm1550-4646.1921.

[5] M. A. Musa and M. A. Mahmood, "Client-side cryptography based security for cloud computing system," in Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS), 2021, pp. 627–632. doi:10.1109/ICAIS50930.2021.9395890.

[6] H. Song, J. Li, and H. Li, "A cloud secure storage mechanism based on data dispersion and encryption," IEEE Access, vol. 9, pp. 63735–63741, 2021. doi:10.1109/ACCESS.2021.3075340.