A Cloud - Based Secure File Vault with Role-Based Access Control and Encrypted Storage Mechanism

Saranya P[1], Manikandan D[2], Pavilan T[3], Raghul Raj P[4], Kumaran P[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, The Kavery Engineering College, M. Kalipatti, Salem, Tamilnadu, India*
[2,3,4,5]*UG Students, Department of Computer Science and Engineering, The Kavery Engineering College, M. Kalipatti, Salem, Tamilnadu, India*

Abstract*—Cloud Storage refers to the use of encrypted data in the Cloud where data is initially encrypted into a ciphertext state when it is being stored in a Cloud environment and authentication is only provided to valid users with cryptographic keys for them to be able to access valid information. However, along with this process comes a number of challenges with respect to Key Management within the environment and if the keys used to secure the encrypted data are mishandled or lost, the data becomes unobtainable and the process cannot be reversed. In order to mitigate these challenges, the research provides a Cloud Based – Secure File Vault System that is based on a Role-Based Access Control (RBAC) model that uses a Hybrid Cryptographic Architecture to secure the data with RBAC and hybrid architecture to allow for improved enforcement of security. The Hybrid Architecture used the Advanced Encryption Standard (AES) to provide an efficient and secure means to encrypt the data and maintain confidentiality and integrity, while using Elliptic Curve Cryptography (ECC) for a lightweight and secure means to generate and distribute cryptographic keys to securely protect the access to the data. The separation of the responsibilities within the Hybrid Architecture improves on both the strength of security and the efficiency of the computational resources being used. The use of Zero Knowledge Proof (ZKP) provides for secure authentication without exposing the use of sensitive credentials; therefore, providing improved Privacy and Role Verification for the secure access of data in the Cloud environment. The structured access control applied to the secured data implements predefined roles (Administrator, Manager, User) based on compliance of strict environmental policies, thereby minimizing the risk of unauthorized access to the secured data within the Cloud environment. Experimental evaluations of the Cloud Based – Secure File Vault System revealed improved encryption performance, reduced latencies in the generation of cryptographic keys, and increased authentication performance when compared to previous systems.

***Index Terms*—Cloud Security, Encrypted Storage, Role-Based Access Control, key generation, Data Confidentiality, Authentication, verification.**

I. INTRODUCTION

The rise of cloud computing has revolutionized how data is stored, managed and accessed by offering scalable, affordable and flexible storage. But with the outsourcing of data to the cloud, the need for enhanced security, privacy and access management has emerged [1]. To overcome these challenges, current research aims to integrate access control with encryption and trust-based measures to enhance data security in cloud computing environments. One of the fundamental methods for secure access to the cloud is through role-based access control (RBAC), where users are granted access rights according to their roles in the system. This approach helps control access to resources based on user roles, reducing the risk of unauthorized access [2]. Extensions to RBAC include incorporating privacy preserving methods and trust assessment. This involves considering user trust and privacy policies to dynamically adapt access policies according to user actions and other contextual information. These enhancements mitigate insider attacks and enhance data confidentiality in the cloud computing environment, particularly with sensitive data. Enhanced access control is not the only way storage security has improved. Integrating blockchain and artificial intelligence technologies has also led to secure storage enhancements. Vaults based on blockchain assure immutable records and

decentralized security, along with transparency and data integrity in digital storage [3]. AI-based features also enhance security by enabling anomaly detection and access monitoring for smart security [4]. Additionally, the secure vault architecture has been applied to specific use cases such as password vault systems that use offline encrypted storage for storing highly sensitive passwords [6]. These systems use advanced encryption, key management and dedicated storage environments to protect against external threats. Overall, these innovations support the creation of a secure file vault solution for cloud computing that combines role-based access control and secure storage technologies to ensure data confidentiality, integrity and access control in today's cloud environments [5].

A. Objective

- To Increase security of data stored in a cloud-based file storage system through role-based access control (RBAC) to provide a structured, managed method of access.
- To Create a hybrid cryptographic system incorporating an efficient method of encryption (using both AES and ECC) along with secure key management.
- To Develop enhanced user authentication security via zero-knowledge proof (ZKP) without compromising the sensitive credentials of the user.

B. Contribution of work

The contribution of a hybrid security model that combines AES, ECC, and ZKP architecture improves the overall ability to secure data stored in the cloud. The hybrid security model integrates a highly efficient Role Based Access Control (RBAC) and greatly reduces the resources needed to provide storage protection while also enhancing the security of data within the cloud through an effective authorization and authentication process.

C. Organization of the Paper

In this paper, various sections are comprised of the introductory and background information about the challenges faced by cloud security today and are divided into different categories for ease of access. Sections one through five have been created to allow an orderly flow of the different parts presented throughout this paper: introductory, background, methods used (RBAC-based hybrid cryptographic framework), results obtained, and finally a summary and discussion of the findings, as well as future work to be completed using this hybrid cryptographic framework.

II. RELATED WORK

A decentralized trust architecture based on blockchain technology is also becoming popular as document storage systems. Vault systems that are based on blockchain enforce the use of distributed ledger technology (DLT) to guarantee the immutability and transparency of data as well as its resistance to tampering. They are based on hash-linked block chains, Merkle tree authentication and access control based on smart contracts to implement trust less authentication and remove the risk of single-point-of-failure in cloud storage models in [6]. Cloud data protection services promote the use of strong cryptographic enforcement to ensure confidentiality, integrity and handling of data lifecycle. Secure file storage systems use hybrid encryption designs that have both symmetric encryption (AES-256-GCM) to provide data protection and asymmetric cryptography (RSA/ECC) to exchange secure keys. The cryptography hash algorithms like SHA-256/SHA-3 and HMAC-based authentication are used to ensure integrity by avoiding data alteration maliciously when storing and transferring data in [7]. The systems of cloud access governance are based on identity-focused security models. Modern IAM architectures combine the Role-Based Access Control (RBAC), the Attribute-Based Access Control (ABAC) and Policy-Based Access Control (PBAC) to enforce granular authorization. These systems use authentication techniques (Multi-Factor Authentication (MFA), Single Sign-On (SSO), and JSON Web Tokens (JWT)) to ensure identity verification, sessions, and delegation of access in distributed clouds are safely performed in [8].

Secure vault systems of enterprise quality are highly dependent on the constant security validation and monitoring processes. Penetration testing (PT), vulnerability assessment (VA), standards of compliance auditing, including ISO/IEC and NIST guidelines, are all security testing methodologies. Also, Security Information and Event Management (SIEM), audit trail logging and forensic analytics are employed to facilitate real-time threat detection,

incident response, and compliance with regulations enforcement in [9]. The current cybersecurity designs of secure storage systems are based on the zero-trust, defence-in-depth approach to security. These frameworks combine encryption-at-rest, Transport Layer Security (TLS), Intrusion Detection and Prevention Systems (IDS/IPS) and secure key management systems (KMS). The higher-order applications are also based on AI/ML-inspired anomaly detection, behavioural risk analytics, and dynamic access control policies to counter threats in [10].

Table 1: Fine-grained anonymous attribute-based encryption for secure cloud access

Ref.	Technique	Key Focus	Key Features	Limitations
11	Anony Control-style Attribute-Based Encryption (ABE)	Fine-grained cloud access control	Attribute-based encryption, anonymity preservation, policy enforcement	High encryption and key management overhead
12	Decentralized Multi-Cloud Access Control Model	Secure distributed cloud storage	Decentralized access control, multi-cloud coordination, high resilience	Complex system coordination across clouds
13	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	Scalable access control in cloud	Policy-based encryption, fine-grained authorization, flexible sharing	High computation cost with large attribute sets
14	Machine Learning-based Cloud Security Framework	Intelligent security and key management	AI-based threat detection, adaptive security, anomaly detection	Requires large datasets and high computation resources
15	CP-ABE-based Secure Access Control System	Secure and scalable data access	Attribute-based encryption, policy enforcement, flexible access control	Performance degradation with increasing attributes

The table 1 described Cloud security solutions are primarily concerned with the improvement of secure data access, encryption efficiency, and scalability in a distributed environment. Using an ABE method or CP-ABE method provides a policy controlled/ fine grained access control mechanism, but at a high computational cost. A decentralized multi-cloud model increases trust and reliability; however, they add coordination complexity and coordination issues among multiple cloud platforms. Machine learning security frameworks provide intelligence threat detection and adaptive security. For these solutions to operate effectively, large training datasets and significant computational resources will be required.

III. PROPOSED METHODOLOGY

The proposed system is a cloud-based secure file vault that is founded on Role-Based Access Control (RBAC) and hybrid cryptography solution. Encryption of data with Advanced Encryption Standard (AES) and efficient generation and distribution of keys with the aid of Elliptic Curve Cryptography (ECC) provide strong confidentiality and efficiency, respectively. Zero-knowledge Proof (ZKP), is used to authenticate users without revealing sensitive credentials. This combination offers enhanced security, reduced complexity in key management together with limited user access based on user roles.

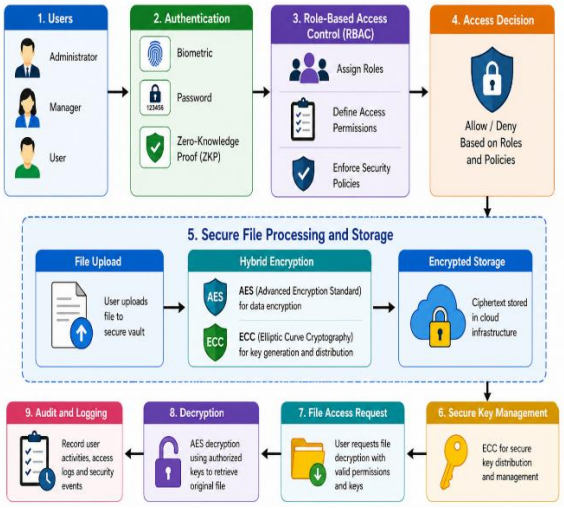

Figure 1: Secure RBAC-Based Cloud Encryption Framework

The figure1 describes a secure data flow, which combines Zero-Knowledge Proof (ZKP) as privacy-preserving authentication and Role-Based Access Control (RBAC) as the authorization enforcement. The plaintext files are then encrypted by Advanced Encryption Standard (AES) when verified successfully and secure key generation and distribution is done by Elliptic Curve Cryptography (ECC). The data encrypted is stored in a controlled cloud vault, which is confidential and resistant to unauthorized access. Key retrieval by authorized users

is done through ECC and AES-based decryption and ensures secure and controlled access to data.

A. Role-Based Access Control Module for Secure Data Management System

Role-Based Access Control (RBAC) is a security module that provides control of user permissions according to the predefined roles including the administrator, manager, and user. It makes sure that only authorized resources are accessed by each user based on his/her assigned role. This module implements a tight control over access to prevent illegal operations and misuse of data. It assists in ensuring a secured control of the system resources.

$$RA: U \rightarrow R \quad (1)$$

The equation (1) describes the role assignment process with an individual user (U) assigned to a particular role (R). It is used to make sure that all users within the system have a valid role like administrator, manager or user.

$$PA: R \rightarrow P \quad (2)$$

The equation (2) represented is a permission assignment, with each role (R) associated with a permission set (P). It determines the operations a role can perform, which could be read, write or delete.

$$UP(u) = P(RA(u)) \quad (3)$$

The equation (3) calculates the effective permissions of a user which are based on the assigned role. The $RA(u)$ function determines the role of user u and P returns the permissions of the role.

$$A(u, r) = \begin{cases} 1, & \text{if } r \in UP(u) \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

The access control decision function is defined by this equation (4), in which access can be granted (1) or denied (0). In case the set of permissions granted to a user contains the requested resource/action, the user is permitted to it. Otherwise, there is no access.

B. Advanced Encryption Standard Module for Secure Cloud Storage

Securing of data by using strong symmetric encryption methods is done by Advance encryption Standard (AES) module. It encrypts and decrypts stored files effectively without compromising and integrity of data. AES provides protection of sensitive information both in storing and transmitting in the cloud. Its high speed and high security performance has made it popular.

$$C = E_K(P) \quad (5)$$

The equation (5) indicates that plaintext file P is transformed into ciphertext output C through the encryption algorithm E, with the additional input of the secret key K. This process produces an unintelligible version of data before being saved on a cloud provider's infrastructure or environment.

$$P = D_K(C) \quad (6)$$

The equation (6) represents the decryption algorithm, with ciphertext (C) transformed back to plaintext (P) by the decryption algorithm D and the identical key K. It guarantees authentic users to retrieve the original data only.

$$S_{i+1} = MixColumns\big(ShiftRows\big(SubBytes(S_i)\big) \oplus K_i\big) \quad (7)$$

The AES round operation can be characterized by this equation (7), each state S_i is then subjected to Sub Bytes, Shift Rows and Mix Columns operations, and then key addition K_i.

$$S' = S \oplus K_r \quad (8)$$

The equation (8) described a Add Round Key step which is the state matrix S is and round key K_r XOR operation. It is a crucial process of each AES round that incorporates the secret key in the encryption process.

C. Elliptic Curve Cryptography Module for Secure Key Exchange

The Elliptic Curve Cryptography (ECC) module deals with the secure key creation as well as the key exchange between the users and the system. It offers good cryptographic security with smaller key size, and is therefore more efficient in comparison to conventional algorithms. ECC provides safe transfer of encryption keys to networks which are not trusted without leakage. It decreases the computational load at the cost of high security level. Generally, ECC improves system efficiency and the safe communication.

$$y^2 = x^3 + ax + b \quad (9)$$

The equation (9) represented a basic elliptic curve in ECC over a finite field. a and b are the values that define the shape of the curve, and should meet the security requirements.

$$P + Q = R \quad (10)$$

The equation (10) represented an elliptic curve point addition, with two valid points P and Q on the curve being added to the other to form a new point R. This is

a basic operation in ECC to produce complicated cryptographic values.

$$Q = kP \quad (11)$$

The equation (11) determines scalar multiplication in which a point P multiplied by a private key k to give a public key Q. It is the fundamental functioning in the generation of ECC keys.

$$K = n_A \cdot n_B \cdot P \quad (12)$$

The equation (12) calculation of the shared secret key, in which there are two users with secret keys n_A and n_B who use a common secret key by a common base point P. The two users come up with a common key independently.

D. Zero-Knowledge Proof Module for Secure Authentication System

Zero-Knowledge Proof (ZKP) module allows authenticating the user without disclosing real user identities like passwords or private keys. It enables the users to authenticate themselves to the system without revealing sensitive data to the system. This greatly minimises chances of credential theft and unauthorised access. ZKP enhances privacy by making authentication to be secure and confidential. In general, it increases trust and security in the cloud-based systems.

$$C = g^r \cdot h^x mod p \quad (13)$$

In equation (13) represents the commitment stage whereby a user forms a commitment value C using a random number rand secret value x. The g and hare public are the values, p is is a large prime number.

$$s = r + c \cdot x \quad (14)$$

The step of response generation is defined in this equation (14): the user calculates s using random value r, challenge c and secret x.

$$P(Verifier\ learns\ x) = 0 \quad (15)$$

The equation (15) representation of zero-knowledge property that means that the verifier does not get any information on the secret value x. The real credentials are still not displayed even after the authentication.

IV. RESULT AND DISCUSSION

The findings of the experiment prove that the proposed Cloud-Based Secure File Vault System is more efficient in cryptography and access control than the current methods. AES + ECC integration greatly minimizes the encryption and key generation overheads whilst ensuring high data confidentiality and integrity. Moreover, ZKP integration increases the accuracy of authentication without revealing sensitive credentials, which further improves privacy protection. In general, the system has better security performance, computational efficiency, and secure access management in case of RBAC enforcement than conventional approaches.

A. Dataset Description

The database consists a secure access of the database by the various authorization types used by the cloud storage system users as well as their user levels with respect to the access authorizations they have. Additionally, this database also considers many security features of the cloud storage system such as Network Access Control (NAC), Encryption and Event Logging. Therefore, the information provided in this database will assist in assessing the level of security and control over a cloud file vault system.

	Authentication	User_Identity	Access_Levels	User_Roles	Security_Policies	Third_Party	Cloud_Service	User_Be	Network_	Encryptio	Logging_
2	Biometric	TRUE	Admin	Admin	FALSE	FALSE	GCP	TRUE	FALSE	FALSE	FALSE
3	MFA	TRUE	Modify	User	TRUE	TRUE	IBM Cloud	TRUE	TRUE	FALSE	TRUE
4	Password	TRUE	Admin	Guest	FALSE	FALSE	AWS	FALSE	FALSE	TRUE	FALSE
5	MFA	TRUE	Modify	User	TRUE	FALSE	IBM Cloud	TRUE	TRUE	FALSE	FALSE
6	MFA	TRUE	Read	SuperAdmin	TRUE	TRUE	GCP	TRUE	TRUE	FALSE	FALSE
7	MFA	FALSE	Write	SuperAdmin	TRUE	FALSE	IBM Cloud	TRUE	FALSE	FALSE	FALSE
8	Biometric	TRUE	Write	SuperAdmin	TRUE	TRUE	AWS	TRUE	TRUE	FALSE	FALSE
9	Biometric	TRUE	Modify	SuperAdmin	TRUE	FALSE	IBM Cloud	TRUE	FALSE	TRUE	FALSE
10	Password	TRUE	Write	Guest	TRUE	TRUE	Azure	TRUE	TRUE	TRUE	FALSE
11	MFA	TRUE	Read	User	FALSE	FALSE	IBM Cloud	FALSE	FALSE	FALSE	TRUE
12	Biometric	TRUE	Read	Guest	TRUE	TRUE	IBM Cloud	FALSE	TRUE	FALSE	FALSE
13	Biometric	TRUE	Admin	Guest	FALSE	TRUE	IBM Cloud	TRUE	FALSE	TRUE	TRUE
14	Password	TRUE	Admin	Admin	TRUE	FALSE	GCP	FALSE	TRUE	FALSE	FALSE
15	Biometric	TRUE	Admin	Admin	TRUE	TRUE	AWS	TRUE	TRUE	FALSE	TRUE

Figure 2: Cloud File Vault Security Dataset with Hybrid Cryptographic Attributes

The figure 2 represents an access control and data protection can be unified in a cloud file vault solution, which is based on a concept-based security model. The goal is to combine authentication methods with RBAC (role-based access control) for the purpose of ensuring that only authorized users can perform certain actions, such as creating or deleting files. Identity verification is used to validate the identity of each user and assign them roles that have assigned access rights and permissions. The inclusion of security policies and third-party involvement indicates governance and trust in the system. Cloud platforms show where the service is deployed, while encryption, network control, and

logging identify critical security mechanisms. This concept emphasizes the need for multiple layers of security through the use of authentication and authorization (as opposed to just using a user's password) and provides multiple levels of data protection (as opposed to just protecting data when it is on disk).

B. Comparison Table

Table 2: Encryption time performance analysis

Method	Encryption Time (ms)
CP-ABE	85
ABAC	110
MFA	120
ZKP (Proposed)	145

The comparison of encryption time of various security models in milliseconds (ms) in Table 2. CP-ABE has the lowest encryption latency (85 ms) which implies that attribute-based encryption is efficiently performed. ABAC and MFA have medium computational overhead of 110ms and 120ms respectively because of policy enforcing and multi-factor validation. The version of the proposed ZKP-based model incurs a longer encryption time (145 ms), which can be explained by the fact that it involves more cryptographic verification procedures.

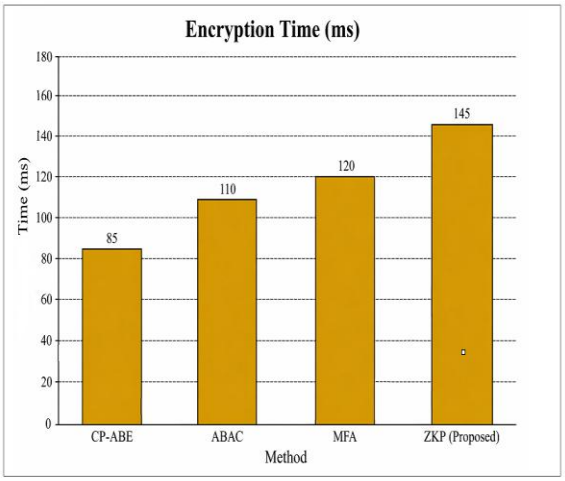

Figure 3: Encryption Latency Comparison

Figure 3 illustrates a comparison of the encryption time of CP-ABE, ABAC, MFA and the proposed ZKP model. CP-ABE has the shortest latency (85 ms), whereas ABAC (110 ms) and MFA (120 ms) come at moderate delays as they involve extra processing operations. The longest time (145 ms) is used in the proposed ZKP model due to the sophisticated cryptographic processes, which guarantee greater security and privacy.

Table 3: Decryption latency evaluation

Method	Decryption Time (ms)
CP-ABE	75
ABAC	98
MFA	105
ZKP (Proposed)	130

Table 3 compares the decryption time of CP-ABE, ABAC, MFA, and ZKP model proposed. CP-ABE has the lowest time (75 ms) and ABAC (98 ms) and MFA (105 ms) have moderate delays because of extra verification procedures. The ZKP model proposed has the longest time (130 ms) due to the sophisticated cryptographic validation, which guarantees higher security and integrity of the data.

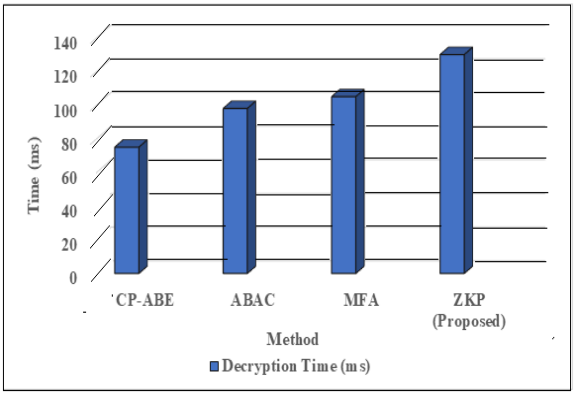

Figure 4: Decryption Performance Comparison

Figure 4 demonstrates the time variation in the decryption of the data in CP-ABE, ABAC, MFA and the proposed ZKP model, which has differences in the computational efficiency. CP-ABE is the fastest to decrypt (75 ms), which means that it can recover data much faster with the least overhead. The middle delays of ABAC (98 ms) and MFA (105 ms) are moderate as a result of the policy verification and multi-factor authentication processes. The suggested ZKP model is the lowest in terms of decryption time (130 ms).

Table 4: Authentication accuracy evaluation

Method	Authentication (%)
CP-ABE	89.5
ABAC	91.2
MFA	94.8
ZKP (Proposed)	97.6

Table 4 present the comparison of authentication performance of CP-ABE, ABAC, MFA and the proposed ZKP model. CP-ABE has an accuracy of 89.5% which shows that the system has basic authentication ability, whilst ABAC (91.2%) and MFA (94.8%) are more accurate due to policy-based and multi-factor authentication. The proposed ZKP model has the best authentication rate (97.6%) because of its sophisticated privacy preservation validation system, which guarantees better security and accurate user authentication.

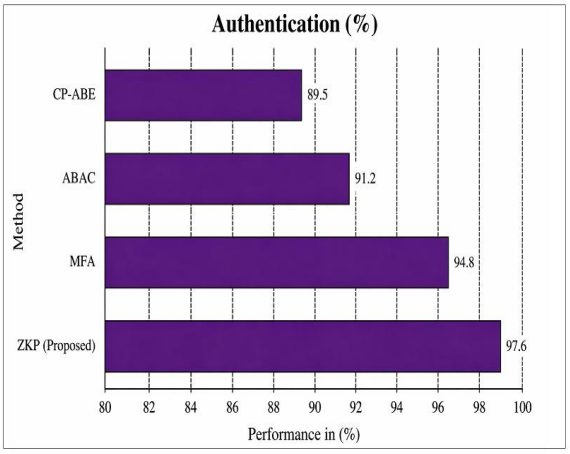

Figure 5: Authentication Performance Comparison

The figure 5 described an authentication performance of various security methods. ZKP (Proposed) has the highest accuracy of 97.6% which is higher compared to other methods. MFA performs well with 94.8%, and ABAC and CP-ABE have moderate performance. The findings show that ZKP has a higher authentication reliability and security effectiveness.

Table 5: Integrity performance comparison analysis

Method	Integrity (%)
CP-ABE	90.3
ABAC	92.5
MFA	94.1
ZKP (Proposed)	98.2

The table 5 present an integrity performance by various security mechanisms. ZKP (Proposed) has the best integrity of 98.2%, which implies a better protection of data. MFA and ABAC are the most intermediate with the lowest value of CP-ABE. On the whole, the findings demonstrate the efficiency of ZKP in guaranteeing improved data integrity.

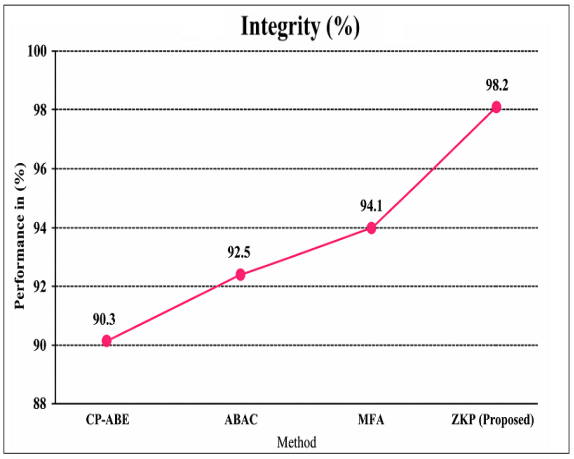

Figure 6: Integrity performance comparison

Figure 6 indicates the integrity performance comparison between CP-ABE, ABAC, MFA and proposed ZKP-based system. It is noted that CP-ABE has the lowest integrity of 90.3%, which means that there is a lack of data integrity. The integrity is gradually raised to 92.5% and 94.1% by ABAC and MFA because improved mechanisms to control access are implemented. The ZKP model proposed has the highest integrity of 98.2% and indicates high security with excellent data protection.

Table 6: File Size Analysis

Method	File Size (MB)
CP-ABE	0.39
ABAC	0.44
MFA	0.47
ZKP (Proposed)	0.51

The file size overhead due to various security models is compared in Table 6. The lowest file size overhead is produced by CP-ABE, with a file size of 0.39 MB. This shows that there is better compression with lower complexity in regards to security. The moderate file sizes of ABAC and MFA (0.44 MB and 0.47 MB, respectively) would imply that they have more metadata as well as authentication overhead; therefore, they would produce larger files than CP-ABE. Finally, using the proposed ZKP model produces the largest file size of 0.51 MB.

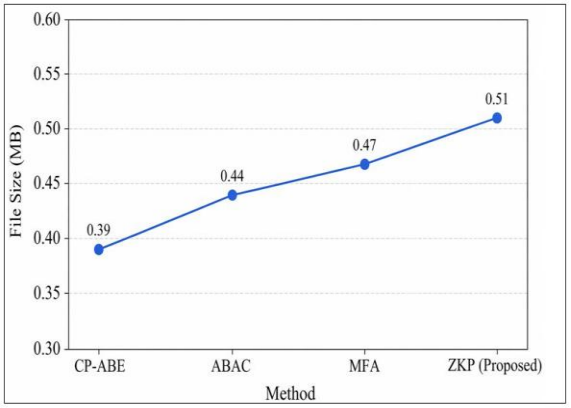

Figure 7: File Size Comparison Analysis

Figure 7 comparison of the file size (MB) based on various security methods including CP-ABE, ABAC, MFA, and the proposed ZKP model. The findings have shown that CP-ABE has the lowest file size of 0.39 MB, which is more efficient in storage. ABAC and MFA have a slower growth of file size as a result of extra security processing overhead. The suggested ZKP system has the largest file size (0.51 MB).

V. CONCLUSION

The Cloud Based Secure File Vault System will increase Cloud Security through the application of Zero Knowledge Proofs (for secure user authentication), Role Based Access Control (to limit user access) and the use of a Hybrid Cryptographic Architecture (AES encryption, plus ECC based key management). All of these methods combined will provide strong user authentication, secure data integrity, and maintain confidentiality while reducing the problems associated with key management. The proposed System will guarantee to make it impossible for anyone to alter or tamper with data after it has been stored and/or transmitted without detection thus ensuring the integrity of that data once it has been created. The experimental results indicate that this system performs better with respect to Authentication 97.6%, Integrity 98.2%, and the amount of latency experienced compared to the currently existing systems.

REFERENCE

[1] U. N. Anirudh and S. L. Shiva Darshan, “Role-Based Virtuosity in Virtual Environments: A Technical Exploration of Access Control and Authentication Mechanisms,” in *Cloud Security*. Boca Raton, FL, USA: Chapman and Hall/CRC, 2024, pp. 183–196.

[2] K. Mythili and S. Rajalakshmi, “Enhancing Role Based Access Control with Privacy in Cloud Computing,” *Turkish Online Journal of Qualitative Inquiry*, vol. 13, no. 1, 2022.

[3] A. U. R. Butt *et al*., “An optimized role-based access control using trust mechanism in e-health cloud environment,” *IEEE Access*, vol. 11, pp. 138813–138826, 2023.

[4] C. Chowdary and R. Naresh, “Enhancing Digital Security with eVault: A Blockchain and AI-Based Storage System.”

[5] M. Abdulkadir *et al*., “Vault-PMS: A Vault-Based Password Management System for Secure Offline Data Storage,” in *Proc. Int. Wireless Communications and Mobile Computing (IWCMC)*, 2024.

[6] V. Pramodkumar *et al*., “e-Vault: A Blockchain-Based Secure Document Storage System,” 2025.

[7] R. B. Madhumala *et al*., “Secure file storage & sharing on cloud using cryptography,” *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 5, pp. 49–59, 2021.

[8] J. E. Ike *et al*., “Identity and Access Management in Cloud Storage: A Comprehensive Guide,” 2025.

[9] J. Komarthi, “Security Testing of Enterprise Vault & eDiscovery Solutions,” *IJAIDR – Journal of Advances in Developmental Research*, vol. 16, no. 2.

[10] M. S. Sozol *et al*., “Building an impenetrable vault: Advanced cybersecurity strategies for database servers,” *Indian Scientific Journal of Research in Engineering and Management*, vol. 8, no. 11, pp. 1–7, 2024.

[11] P. Nainar Balasubramanian and J. Owen, “AnonyControl-Style Attribute-Based Encryption in Azure Cloud Environment,” *SSRN Electronic Journal*, 2025.

[12] M. El Moudni and E. Ziyati, “Decentralized and Secure Access Control Model for Multi-Cloud

Data Storage," *International Journal of Safety & Security Engineering*, vol. 15, no. 2, 2025.

[13] R. K. Yadav, "Scalable and Secure Data Access Control in Cloud Environments Using Ciphertext-Policy Attribute-Based Encryption," *IAENG International Journal of Computer Science*, vol. 52, no. 9, 2025.

[14] S. Ahmad *et al*., "Machine learning-based intelligent security framework for secure cloud key management," *Cluster Computing*, vol. 27, no. 5, pp. 5953–5979, 2024.

[15] S. Suresh and R. K. Yadav, "Scalable and Secure Data Access Control in Cloud Environments Using Ciphertext-Policy Attribute-Based Encryption."