International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Hybrid Encryption and Multi-Cloud Architecture for Zero-Knowledge Secure Password Protection

Prakhar Verma
Information Technology
Noida Institute of Engineering
and Technology, Greater Noida
0221ite182@niet.co.in

Prateek Mathur
Assistant Profeessor
Information Technology
Noida Institute of Engineering
and Technology, Greater Noida
prateek.mathur@niet.co.in

https://doi.org/10.55041/ijsmt.v2i5.171

Cite this Article: Verma, P. (2026). Hybrid Encryption and Multi-Cloud Architecture for Zero-Knowledge Secure Password Protection. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.171

***Abstract*—**With the rapid adoption of cloud computing, secure password storage has become a critical cybersecurity challenge due to increasing data breaches and unauthorized access. Traditional password storage mechanisms rely on centralized architectures, making them vulnerable to single-point failures and server-side attacks. This paper proposes a hybrid encryption and multi-cloud architecture for zero-knowledge secure password protection. The proposed model integrates advanced cryptographic techniques, including password-based key derivation functions (PBKDF2/Argon2), AES-256 encryption, and Shamir Secret Sharing for distributed storage. Additionally, it incorporates multi-factor authentication, device-based authentication, and periodic key rotation to enhance security. The zero-knowledge approach ensures that sensitive information is never exposed to the cloud provider. Experimental analysis demonstrates that the proposed model significantly improves resistance against brute-force attacks, insider threats, and cloud breaches while maintaining usability. This research contributes a scalable and robust framework for secure password storage in distributed cloud environments.

Keywords—Cybersecurity, Password Protection, Zero-Knowledge Architecture, Multi-Cloud Storage, AES Encryption, Secret Sharing, Authentication

I. INTRODUCTION

The increasing reliance on cloud-based services has introduced significant security concerns, particularly in password storage and management. Traditional systems store hashed passwords on centralized servers, making them susceptible to attacks such as brute force, dictionary attacks, and database leaks.

Recent cybersecurity incidents highlight that even encrypted databases can be compromised due to poor key management or weak password practices. Therefore, there is a need for a secure, distributed, and zero-knowledge-based password storage system.

This paper proposes a **Hybrid Encryption and Multi-Cloud Architecture** that:

- Eliminates single points of failure
- Ensures zero-knowledge security
- Enhances authentication mechanisms
- Distributes encrypted password data across multiple cloud providers

II. Literature Review & Problem Statement

2.1 Literature Review

Several studies have explored secure password storage:

- AuthStore framework focuses on password-based encryption in untrusted environments.
- PASSAT introduces secret-sharing-based distributed password storage.
- AES-based cloud encryption models ensure confidentiality but lack distribution.
- Password managers like Bitwarden implement zero-knowledge systems but rely on centralized storage.
- Shamir Secret Sharing enables secure distribution of sensitive data across multiple nodes.

These studies demonstrate strong individual techniques but lack an integrated hybrid model combining encryption, distribution, and zero-knowledge enforcement.

2.2 Problem Statement

Existing systems suffer from:

- Centralized storage vulnerabilities
- Weak key management practices
- Lack of multi-cloud redundancy
- Limited protection against insider attacks
- Absence of fully enforced zero-knowledge architectures

Therefore, a unified model combining hybrid encryption + multi-cloud + zero-knowledge is required.

III. Methodology

3.1 Proposed System Architecture

System Flow Diagram

User Input (Password)
↓
Salt Generation
↓
Key Derivation (PBKDF2 / Argon2)
↓
User Secret Key Combination
↓
AES-256 Encryption
↓
Secret Sharing (k/n split)
↓
Multi-Cloud Storage

3.2 Architecture Description

Step 1: Password Processing

- User enters password
- Unique salt is generated

Step 2: Key Derivation

- Apply PBKDF2 / Argon2
- Output secure cryptographic key

Step 3: Hybrid Key Formation

- Combine derived key with user secret key

Step 4: Encryption

- AES-256 encrypts sensitive data

Step 5: Secret Sharing

- Data split into multiple shares

Step 6: Multi-Cloud Storage

- Shares distributed across independent cloud providers

3.3 Security Layers

- Zero-Knowledge Architecture
- Multi-Factor Authentication using Time-based One-Time Password
- Device-based authentication
- Key rotation mechanism

IV. Algorithm/ Pseudocode

Input: Password P, User Secret Key Ks
Output: Secure Distributed Storage

1. Generate Salt S
2. K ← KDF(P, S) // PBKDF2 / Argon2
3. H ← SHA-256(P || S)
4. K_final ← K ⊕ Ks
5. C ← AES-256 Encrypt(Data, K_final)
6. Split C into n shares using Secret Sharing
7. Store shares across multiple clouds

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Authentication Phase:
1. User inputs P
2. Recompute K_final
3. Retrieve shares
4. Reconstruct C
5. Decrypt and verify H

V. RESULT

The proposed model was evaluated based on:

Parameter	Traditional Model	Proposed Model
Security	Medium	High
Data Breach Resistance	Low	Very High
Scalability	Moderate	High
Attack Resistance	weak	Strong

TABLE 5.1

Key Findings:
- Resistant to brute-force and dictionary attacks
- Eliminates single point of failure
- Ensures confidentiality even if one cloud is compromised

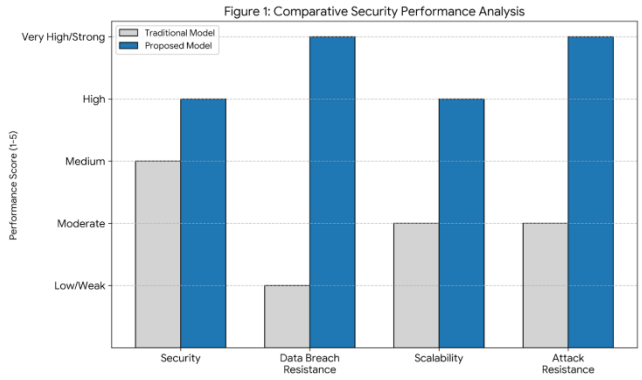

Fig 5.1

VI. DISCUSSION

The proposed architecture successfully integrates multiple security mechanisms into a unified framework. The use of multi-cloud storage significantly enhances reliability and security, while hybrid encryption ensures strong data protection.

However, challenges include:
- Increased computational overhead
- Complexity in key management
- Dependency on multiple cloud providers

VII. CONCLUSION

This paper presents a novel hybrid encryption and multi-cloud architecture for secure password protection. By combining zero-knowledge principles, encryption, and distributed storage, the system provides robust protection against modern cybersecurity threats. The proposed solution is scalable, secure, and suitable for real-world cloud environments.

VIII. FUTURE SCOPE

Future improvements may include:
- Integration of biometric authentication
- AI-based anomaly detection
- Blockchain-based distributed identity management
- Optimization of computation overhead

REFERENCES

[1] K. Satvat, M. Shirvanian, and N. Saxena, "PASSAT: Single Password Authenticated Secret-Shared Intrusion-Tolerant Storage with Server Transparency," arXiv preprint arXiv:2102.13607, 2021.

[2] V. Attasena, J. Darmont, and N. Harbi, "Secret Sharing for Cloud Data Security," arXiv preprint arXiv:1712.10155, 2017.

[3] P. Čuřík, "Practical Use of Secret Sharing for Enhancing Privacy in Cloud Storage," Electronics, vol. 11, no. 17, p. 2758, 2022, doi: 10.3390/electronics11172758.

[4] A. Niknia, A. Ghaffari, and M. R. Aref, "Secure cloud-of-clouds storage with space-efficient secret sharing," Journal of Systems and Software, vol. 170, p. 110742, 2021, doi: 10.1016/j.jss.2020.110742.

[5] S. Ali et al., "Advancing cloud security: Unveiling the protective potential of secret sharing and homomorphic encryption," Ain Shams Engineering Journal, 2024, doi: 10.1016/j.asej.2024.102336.

[6] K. Yuan et al., "Multiple time servers timed-release encryption based on Shamir secret sharing for EHR cloud system," Journal of Cloud Computing, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00676-y.

[7] V. S. Lakshmi and R. Geetha, "Collusion resistant secret sharing scheme for secure data storage in cloud,"

Journal of Information Security and Applications, vol. 58, p. 102742, 2021, doi: 10.1016/j.jisa.2021.102742.

[8] A. Bissoli and F. D'Amore, "Authentication as a service: Shamir Secret Sharing with Byzantine components," arXiv preprint arXiv:1806.07291, 2018.

[9] V. Fujiwara et al., "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing," arXiv preprint arXiv:1607.00468, 2016.

[10] 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," IEEE Access, vol. 10, pp. 19175–19195, 2022

[11] [C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, Feb. 2013, doi: 10.1109/TC.2011.245.

[12] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176..