Advanced Secured File Vault with Multi-Layered Security and Cloud Backup

DR.J.SATHYA PRIYA
Department of Information Technology
Velammal Engineering College
Chennai , Tamilnadu
dr.sathyapriyaanand@gmail.com

Rahul Kumaran R
Department of Information Technology
Velammal Engineering College
Chennai , Tamilnadu
rahulprajith005@gmail.com

Manova Daniel J
Department of Information Technology
Velammal Engineering College
Chennai , Tamilnadu
jmanovadaniel.11@gmail.com

***Abstract*— The dramatic rise in digital information and increased reliance on cloud storage have increased threats of unauthorized access, breaches, and cyber attacks. Traditional storage systems employ single-level security measures that are inadequate in fighting sophisticated threats, internal attacks, and ransomware attacks. This research presents the Advanced Secured File Vault with Multi-Layer Security and Cloud Backup that is intended to promote "defense-in-depth" when it comes to storing and managing confidential information.**

The proposed system combines various levels of security mechanisms such as user authentication, role-based access control, symmetric and asymmetric techniques for encrypting files, file integrity check, as well as end-to-end cloud backup encryption. The sensitive files will be encrypted through the Advanced Encryption Standard before they are stored, while the use of public key cryptography will help in the secure exchange of the key. Multiple-factor authentication increases the overall resistance to possible breaches of security through passwords. The cloud backup will take place on the encrypted files. Experimental evaluation has confirmed that it has a minimal impact on the system and gives a greatly improved level of security.

Keywords— Secure File Vault, Multi-Layered Security, Data Encryption, Cloud Backup, Access Control, Cybersecurity, Defense-in-Depth, Secure Cloud Storage

I. INTRODUCTION

In recent times, the exponential increase in digital information and the pervasiveness of cloud storage solution use have significantly impacted the manner in which data is handled. Though cloud storage technology promotes scalability, flexibility, and easy access to information, it also creates grave concerns relating to possible unauthorized access, data breaches, threats from insiders, and ransomware attacks.

It is the sensitive information now being stored digitally, which is the major attraction for cyber attackers, thereby making the traditional storage solution mechanism with single-layer security redundant.

The majority of current file storage and vault solutions mainly make use of password-driven access security and simple encryption schemes. While encryption ensures confidentiality to a certain degree, any leakage or compromise involving authentication credentials or keys may cause complete visibility of all stored files. Moreover, most current solutions have poor key management, verification, and access auditing. Cloud storage adds to these risks when credentials for encryption keys belong to third-party entities.

To overcome such difficulties, there have been increased adoption and popularity of security architectures that have adopted the defense-in-depth strategy. The strategy concentrates on leveraging a variety of independent security layers such that even when one layer fails, it does not have a cascading effect on the overall system. Applying such strategy for safe file archiving entails integrating efficient authentication, multi-factor analysis, encryption of files both at rest and motion, role-based access management, integrity checks, and safe backup processes. Currently, most implementations exist and operate in silos.

This study proposes an Advanced Secured File Vault with Multi-Layered Security and Cloud Backup, which integrates those security measures in a holistic manner. This proposed system uses symmetric cryptography in encrypting data efficiently, asymmetric cryptography in facilitating secure key exchange, multi-factor authentication to ensure access security, and cloud backups encrypted end-to-end to guarantee availability of data without compromising confidentiality. The main goal of this study is to conceptualize a secure, scalable file vault system which will improve confidentiality, integrity, as well as availability of data, while incurring an acceptable performance cost in a cloud-enabled setting.

Despite the great advancement made in secure storage solutions, many of the existing solutions tend to deal with a particular aspect of security individually as a whole. Most of these systems concentrate only on encrypting the files without considering key management for secure storage, access control for stored files, validation for file integrity, and recovery. Additionally, some cloud-based storage solutions tend to utilize security measures that are controlled by cloud providers. This tends to decrease user trust and control over their sensitive information.

In regard to the context, the proposed work ensures a defense-in-depth approach for a secured file vault design, which integrates authentication, encryption, access control, integrity check, audit logging, and cloud backup encryption into a single framework.

II. LITERATURE SURVEY

Secure data storage is a continually evolving area of research as a result of the growing volume of sensitive data being stored in electronic and cloud systems. The early methodologies for file protection were mainly carried out by using password protection and encryption. Though it offered a certain level of confidentiality protection against unauthorized access, it had the drawback of being vulnerable to password attacks and brute-force cracking [1].

For enhanced confidentiality of data, cryptographic file systems were developed, which used symmetric encryption algorithms like AES to encrypt files [2]. Encrypted file systems, client encryption, and other similar technologies ensured that unauthorized users had no insight into the content of the data. But these technologies also had scalability issues regarding keys, as once those keys were compromised, the entire dataset was at risk of exposure [3].

The emergence of cloud computing led to the focus on ensuring the security of data stored in untrusted cloud systems. Models for client-side encryption emerged for encrypting data before uploading it to the cloud; this ensured that the cloud services providers do not read the data in clear form [4]. While this enhanced data secrecy, problems associated with secure key exchange, verification of data integrity, and efficient control mechanisms in data access still lingered. Moreover, most schemes employed single-layer security mechanisms that lacked effectiveness in combating advanced attacks [5].

Multi-factor authentication and role-based access control methods were later incorporated into the storage systems for countering unauthorized access [6]. It was proved that the combination of authentication factors effectively limits the threat of attack using credentials. However, some systems considered the processes of authentication and encryption as isolated modules with an absent overall multi-layer security framework [7].

To counter such unauthorized access, multi-factor authentication techniques were implemented within secure storage solutions. Analysis showed that passwords paired with secondary factors like one-time passwords and biometric authentication could lower risks associated with compromising credentials effectively [8], [9]. Unfortunately, few solutions for authentication were completely autonomous and did not focus on integrating levels of encryption and access management.

Other access control methods such as role-based access control (RBAC), attribute-based access control (ABAC), to limit the access to the file based on roles/authorizations of the user [10], [11], were further continued. However, access control systems were inadequate to protect the information if the encryption keys were compromised [12]. Additionally, access control systems were inadequate to protect the information if the keys were compromised.

Recent work additionally illustrated the need for “defense in depth” techniques in ensuring the safe storage of data [13]. “Defense in depth” promotes a multi-layered security approach that incorporates authentication, encryption, integrity checks, audits, and backups. It was shown to provide substantially improved protection levels against APTs and insiders when comparing multi-layered to single-layered security systems [14].

Data integrity verification became another prominent field of research; hash function cryptography and message authentication codes were widely used to detect any unauthorized file changes [15]. There were some research papers that combined integrity verification with secured logging mechanisms for traceability purposes within file access operations [16]. However, such mechanisms were designed without considering synchronized secured cloud storage.

The need for encrypted cloud backup and disaster recovery services arose with the growth of the need for data availability as an essential requirement. Studies have proposed end-to-end encryption for backup services, maintaining confidentiality and ensuring data recoverability during system crashes and ransomware attacks [17-18]. The effectiveness of these solutions was hampered by the lack of strong coupling between many backup systems and access and authentication processes.

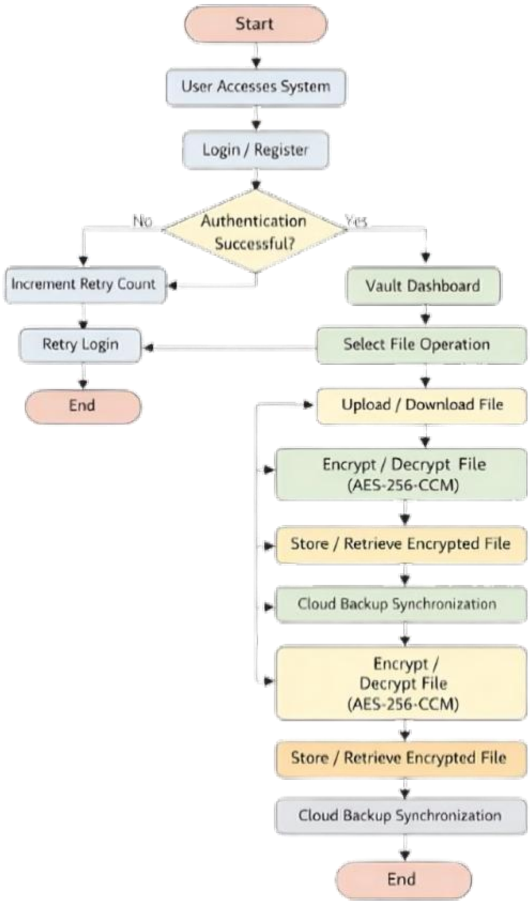

Start
User Accesses System
Login / Register
No
Authentication Successful?
Yes
Increment Retry Count
Vault Dashboard
Retry Login
Select File Operation
End
Upload / Download File
Encrypt / Decrypt File (AES-256-CCM)
Store / Retrieve Encrypted File
Cloud Backup Synchronization
Encrypt / Decrypt File (AES-256-CCM)
Store / Retrieve Encrypted File
Cloud Backup Synchronization
End

Fig. 3.1 System Flowchart of the Proposed Secured File Vault

More recent efforts involved applying zero-trust-based models to file storage systems without assuming any level of inherent trust concerning users, devices, and networks [19]. Verification of access requests and enforcement of encryption and authentication policies are necessary. Though promising, current solutions using zero-trust models are complex and resource-intensive [20].

Based on a study of existing works, it is clear that there are solutions available that deal solely with encryption processes, cloud backup processes, and authentication processes. However, there is a lack of development towards designing a complete solution that considers multi-layered security, secured key management, secured access processes, integrity checks, and secured cloud backup within a single secured file vault design. This propose will fill that gap.

III. METHODOLOGY

The proposed Advanced Secured File Vault with Multi-Layered Security and Cloud Backup is implemented based on Defense in Depth Architecture. The proposed approach primarily relies on combining several independent security measures to guarantee confidentiality, integrity, and availability of sensitive files. The whole system process is further divided into separate functional layers, which are described in detail in the subsequent subsections.

3.1 System Architecture Design

The system uses a client-based security model with client-side encryption and decryption for all data stored both locally and in the cloud. This model ensures that any confidential information that is stored and backed up through cloud services never appears in its plain form to any cloud provider. The system also has four main modules. These include an authentication module, encryption and management module, secure file vault, and cloud backup.

3.2 User Registration and Authentication System

The access of the user to the file vault will be secured using a robust authentication process. The user will have his or her credentials for the purpose of registration. The user has to authenticate his/her credentials using a password for login access. Additionally, multi-factor authentication can be used. The process of using biometric details can also be included. The use of one-time passwords will also reduce attacks.

3.3 Role-Based Access Control

To prevent unauthorized access, the system uses role-based access control. Users are assigned roles with specific permissions according to their capability to upload, download, edit, or delete the file. This ensures that even if the user authenticates, he/she cannot access anything other than the file corresponding to their level of authorization.

3.4 File Encryption Process

Before storage, the files are encrypted with the Advanced Encryption Standard (AES), coupled with a secure key size. For every file, a distinct symmetric key is used, reducing the effects of a compromised key. This is done locally, so confidentiality is ensured in storage as well as while transferring the files. The files, which are encrypted, are placed in the secured vault folder.

3.5 Key Management and Secure Key Exchange

Secure key management is implemented through the use of asymmetric cryptography. Public key encryption methods like the RSA algorithm or Elliptical Curve Cryptography (ECC) are used to encrypt symmetric file keys. Through this process, the encrypted keys to the files can only be accessed or decoded by authorized personnel and not through unauthorized decryption even when the files are encrypted.

3.6 File Integrity Verification

For maintaining integrity, cryptographic hash algorithms (such as SHA-256) are used on every file prior to encrypting it. These hash results are then safeguarded, which are verified in case of file access. It helps in detecting any unauthorized change in storage files, which is not possible in a blockchain technology.

3.7 Secure File Vault Storage

Cryptographic files and their metadata are stored in a secure file vault. The file vault ensures robust security measures for access and secures the ciphertext from the operating system's universal storage of regular files. It also keeps an audit log for monitoring file activities like upload, download, or access attempts.

3.8 Encrypted Cloud Backup and Synchronization

To provide availability of data, there is synchronization of encrypted files with cloud storage. Only encrypted data is sent to cloud storage to retain confidentiality even at an untrusted platform. Secure communication channels are applied while transferring data. Automated backup schedules are implemented to avoid data loss due to failure and ransomware attacks.

3.9 Threat Model and Security Assumptions

The system assumes the presence of both external attackers as well as possible insiders. The threat model assumes attacks such as unauthorized access, key compromise, data tampering attacks, as well as cloud data exposure. The security mechanisms are designed in such a way that failure in a single layer will not lead to complete system compromise.

3.10 Performance and Security Evaluation Method

The evaluation criteria for the system are based on the encryption and decryption time, authentication delay, and cost associated with synchronizing the data in the cloud.

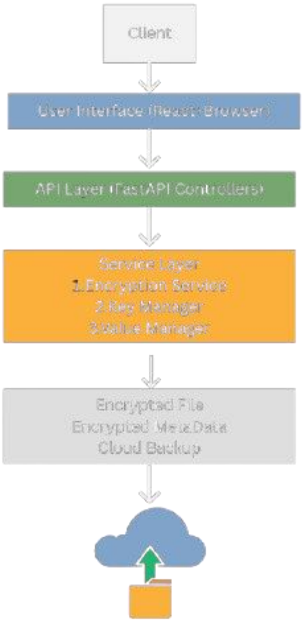


Fig. 3.2 System Architecture of the Advanced Secured File Vault

The effectiveness of the security mechanism is checked by the resilience offered by the proposed system against the attack launched through brute force attack mechanisms like replay attack and unauthorized file access.

3.11 Audit Logging and Monitoring Mechanism

The proposed system has an integrated audit logging and monitoring mechanism to ensure accountability and traceability. All critical operations regarding user login attempts, file upload, download, deletion, and access failures are logged with timestamps and user identifiers. These logs will be kept in append-only mode for tamper protection. Audit logs help in suspicious behavioral detection, forensic analysis, and adherence to security policies. Continuously monitoring logs leads to the early identification of possible attacks like brute-force attempts and unauthorized access patterns.

3.12 Secure Recovery and Disaster Management

The system has a secure mechanism for data recovery in situations of data loss due to hardware failures, accidental deletion, or ransomware attacks. As all files are encrypted before cloud syncing, data recovered will be in its encrypted form, maintaining its integrity during the process. Versioning and scheduled cloud syncing enable users to access past states of files in case the need arises. The system has a high level of data availability in disaster situations.

3.13 Scalability and System Extens

The proposed architecture is meant to be scaleable and extensible for handling an increasing number of users as well as an increasing volume of data. Decomposing for authentication, encryption, storage, and backup functionalities helps scale each component of the system independent of the others. The proposed architecture is extensible for future integrations of various security functionalities like intrusion detection systems, anomaly detection systems, and hardware security modules (HSMs).

3.14 Compliance and Security Policy Enforcement

The system has enforced securities with policies in line with general data protection and cyber security guidelines and best practices. The policies and guidelines on data encryption standards, authentication, access control, and audit processes and procedures are all managed in a way that ensures uniformity in their enforcement. The system is thus made secure for handling sensitive information through its exposition to and strict adherence to security best practices and policies.

IV. RESULT AND DISCUSSION

The performance capabilities and level of security offered by the proposed Advanced Secured File Vault with Multi-Layered Security and Cloud Backup were analyzed through systematic validation tests. This helped to ensure the robustness of the proposed system relying on the principle of layered security to ensure strong protection.

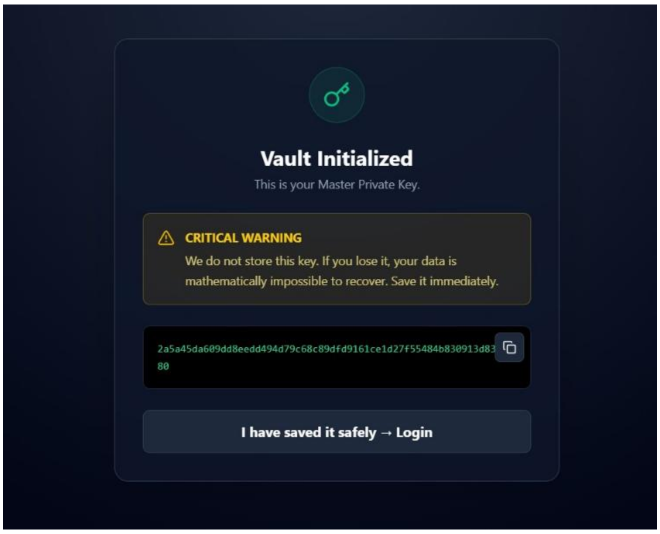
4.1 Encryption & Decryption Performance Analysis

Various tests were conducted regarding the encryption and decryption processes for files of different sizes. It was found that symmetric encryption using the AES method had efficient performance with less computational complexity. However, when it came to encrypting or decrypting small-sized files, the process happened in a matter of seconds with little delay. In the medium-sized category.

In the case of larger files, the time required for encryption and decryption directly scaled up with the file size. The linear scalability establishes the effectiveness of the chosen encryption algorithm for file storage purposes. It is pertinent to note that the encryption performed at the client-end assured the confidentiality of the text by maintaining it beyond the realm of exposure.

4.2 Authentication and Access Control Assessment

Authentication was measured by login response time and resistance to unauthorized access. Multi-factor authentication introduced some additional latency into the authentication mechanism, but it did not cross the threshold of usability. This was because merely using password-based authentication heightened the security by reducing the success probability of credential-based attacks considerably.Role-based access control further strengthened system security by enforcing permission boundaries.



Vault Initialized

This is your Master Private Key.

⚠ CRITICAL WARNING

We do not store this key. If you lose it, your data is mathematically impossible to recover. Save it immediately.

```
2a5a45da609dd8eedd494d79c68c89dfd9161ce1d27f55484b830913d83
80
```

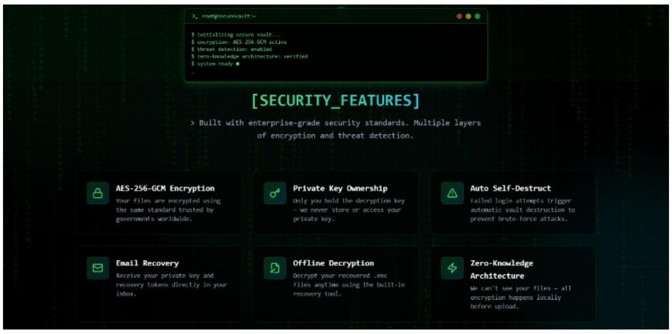
Fig. 4.1. Secure File Upload and Encryption Process

Users were only able to perform actions permitted by their assigned roles, hence preventing privilege escalations and unauthorized file operations. Audit logs captured authentication events and attempts to access files for post-event analysis and compliance requirements.

4.3 Clinching Key Management and Cryptographic Security Assessment

Secure management of keys is one of the important aspects when it comes to encrypted storage solutions. The proposed solution used asymmetric cryptography to encrypt symmetric keys used for encrypting files. This entails that every file is encrypted with a separate symmetric key that is encrypted through asymmetric cryptography.It made the effect of key compromise limited because the compromise of one key will not influence the other files that are already encrypted.

Moreover, the encryption of the keys protected the keys from being decrypted by the hackers who may have access to the files that are encrypted. These results clearly show the level of isolation between the encrypted information and the keys.



```
>_ root@securevault:~
$ initializing secure vault...
$ encryption: AES-256-GCM active
$ threat detection: enabled
$ zero-knowledge architecture: verified
$ system ready ■
```

[SECURITY_FEATURES]

> Built with enterprise-grade security standards. Multiple layers of encryption and threat detection.

AES-256-GCM Encryption Your files are encrypted using the same standard trusted by governments worldwide.

Private Key Ownership Only you hold the decryption key — we never store or access your private key.

Auto Self-Destruct Failed login attempts trigger automatic vault destruction to prevent brute-force attacks.

Email Recovery Receive your private key and recovery tokens directly in your inbox.

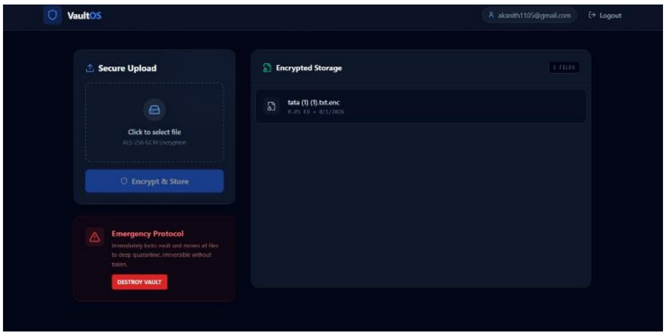
Offline Decryption Decrypt your recovered .enc files anytime using the built-in recovery tool.

Zero-Knowledge Architecture We can't see your files — all encryption happens locally before upload.

Fig. 4.2 Secure Key Management and Vault Initialization Interface

4.4 Results of File Integrity Verification

File integrity checks were assessed through simulated unauthorized alterations to encrypted file contents. The generated cryptographic hash values were validated pre- and post-encryption processes. Any change in file contents caused mismatches in hash values, thus denying unauthorized access to altered file contents.This proved to be effective for resisting tampering, unintended corruption, and replay attacks. Through integrity verification and encryption of the data stored in the environment, the users were guaranteed to access the valid as well as untampered-with information. The experiments prove the vital role of integrity protection as a supplement to encryption and access control.



tata (1) (1).txt.enc
0.05 KB • 8/1/2026

Emergency Protocol Immediately locks vault and moves all files to deep quarantine. Irreversible without token.

Fig. 4.3 Authentication and Access Control Validation Screen

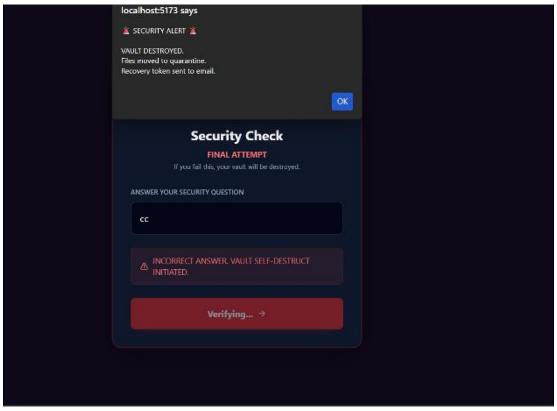
4.5 Cloud Backup Reliability and Recovery Performance

The cloud backup encryption system was also tested to determine its effectiveness in recoverability. The system ensured that cloud backups of encrypted files were performed without revealing any sensitive information. This is because only encrypted files were being transmitted to prevent any breaches in confidentiality.

The recovery tests proved that data files could be successfully recovered after system failure and data loss. Backup tasks resulted in very little network overhead, thanks to optimal synchronization mechanisms.

4.6 Comparative Security AnalysisComparison analysis has been performed for the new system with conventional single-layer file storage systems. In conventional systems, data is generally secured through passwords and single-layer encryption, thereby making it susceptible to possible compromise. In contrast, data protection in the proposed new system remained unaffected even with a possible breach of individual protection layers.

For instance, the use of compromised credentials did not lead to the exposure of plaintext data because the data was encrypted and the encryption keys safeguarded.



localhost:5173 says

SECURITY ALERT

VAULT DESTROYED.
Files moved to quarantine.
Recovery token sent to email.

Security Check

FINAL ATTEMPT

If you fail this, your vault will be destroyed.

ANSWER YOUR SECURITY QUESTION: cc

INCORRECT ANSWER. VAULT SELF-DESTRUCT INITIATED.

Fig. 4.4 Security Features Dashboard of the Proposed System

Additionally, cloud backups encrypted, thus securing the leakage of data in the event of an organization being breached through cloud storage.

4.7 Discussion and Interpretation

The extended evaluation results make it clear that there is a well-structured trade-off between the concepts of security and performance by the proposed system. Integration of several layers of security increases the computing cost, yet the level of information protection required is adequately met. Simulation results support the validity of defense-in-depth strategies for file storage systems.

The outcomes also show the importance of incorporating the mechanisms of security together. Addressing various methods such as authentication, encryption, access control, integrity verification, and cloud backup together, the proposed system covers all the aspects required to be protected through the system.

VI . REFERENCE

[1] M. Blaze, “A cryptographic file system for UNIX,” *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 9–16, 1993.

[2] M. Halcrow, “eCryptfs: An enterprise-class encrypted filesystem for Linux,” *Proceedings of the Linux Symposium*, vol. 1, pp. 201–218, 2007.

[3] Z. Wilcox-O’Hearn and B. Warner, “Tahoe: The least-authority filesystem,” *Proceedings of the ACM StorageSS Workshop*, pp. 21–26, 2008.

[4] E. Barker, “Recommendation for Key Management – Part 1: General,” *NIST Special Publication 800-57*, Rev. 5, 2020.

[5] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[6] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[7] C. Wang et al., “Toward secure and dependable storage services in cloud computing,” *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2012.

[8] R. Das and G. Tuna, “Multi-factor authentication: A

survey," *International Journal of Computer Applications*, vol. 181, no. 23, pp. 1–6, 2018.

[9] A. M. Mostafa et al., "A secure multi-layer authentication framework for cloud-based systems," *Applied Sciences*, vol. 13, no. 19, 2023.

[10] D. Ferraiolo, D. Kuhn, and R. Chandramouli, *Role-Based Access Control*, Artech House, 2003.

[11] V. Goyal et al., "Attribute-based encryption for fine-grained access control," *Proceedings of the ACM CCS*, pp. 89–98, 2006.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.

[13] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems," *NIST SP 800-37*, Rev. 2, 2018.

[14] IEEE Security & Privacy Society, "Defense-in-depth revisited," *IEEE Security & Privacy*, vol. 19, no. 3, pp. 72–75, 2021.

[15] NIST, "Secure Hash Standard (SHS)," *FIPS PUB 180-4*, 2015.

[16] NIST, "Guide to Computer Security Log Management," *NIST SP 800-92*, 2006.

[17] M. Armbrust et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[18] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[19] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," *Forrester Research*, 2010.

[20] M. da Rocha et al., "Secure cloud storage with client-side encryption using trusted execution environments," *arXiv preprint arXiv:2006.04534*, 2020.