Applying Secret Sharing to Enhance Cloud Privacy

Guttikonda Prashanti, M. Lakshmi Prasanna, N. Surekha, Y. Manikanta and G. Bhanu Prakash
Department of Advanced Computer Science and Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, Andhra Pradesh, India

Keywords: Cloud Privacy, Secret Sharing, Serverless Computing, Data Confidentiality, Distributed Security.

Abstract: With the increasing adoption of cloud computing, ensuring data confidentiality and privacy remains a critical challenge. Traditional encryption methods, while effective, often introduce key management complexities and single points of failure. This paper explores an advanced secret-sharing approach to enhance cloud privacy by distributing sensitive data across multiple cloud environments. Unlike conventional secret-sharing techniques, the proposed method integrates a novel cloud-based distribution strategy, leveraging cloud architecture, serverless computing, and encryption to ensure robust security without exposing complete data to any single entity. The proposed system not only enhances security but also ensures seamless data retrieval with minimal computational overhead. This approach provides a scalable and efficient solution for privacy-preserving data storage in cloud environments, making it a viable option for industries handling sensitive information, such as finance, healthcare, and government sectors. The findings contribute to advancing secure cloud storage methodologies, reinforcing the importance of distributed security mechanisms in modern cloud infrastructures.

1 INTRODUCTION

Cloud computing has become a fundamental technology, offering scalable resources and data storage solutions, but its widespread adoption has also increased the risk of security breaches that threaten sensitive data. Traditional security measures are often insufficient to protect against the evolving cyber threats in today's digital landscape. This work addresses these concerns by developing a two-tier security system for key access in cloud computing environments.

The first layer is based on the security measures provided by the cloud service provider, particularly through Identity and Access Management (IAM) policies, which define and enforce user roles and access permissions using Role-Based Access Control (RBAC). The second layer adds an extra layer of protection with Multi-Factor Authentication (MFA), utilizing email-based One-Time Passwords (OTP) to ensure that only authorized users gain access to sensitive data.

A key component of this system is the implementation of Shamir's Secret Sharing algorithm, combined with polynomial interpolation, which is particularly effective in hierarchical organizational structures for secure key management and access control. This two-level approach significantly reduces the risk of unauthorized access, ensuring both the integrity and confidentiality of cloud-stored data. By combining provider- based security with user-specific authentication measures, this work aims to set a new standard for cloud security protocols and addresses the growing need for comprehensive data protection in an increasingly interconnected world.

2 LITERATURE SURVEY

Cloud security mechanisms have significantly evolved, incorporating cryptographic methods to enhance data protection. One of the most widely used techniques is Shamir's Secret Sharing (SSS), which ensures secure key management by splitting encryption keys into multiple shares, requiring a predefined threshold for reconstruction. Shamir (1979) demonstrated that polynomial interpolation could be used to protect secrets, ensuring that unauthorized access to partial shares does not compromise the original key.

In addition to secret sharing, homomorphic

Prashanti, G., Prasanna, M. L., Surekha, N., Manikanta, Y. and Prakash, G. B.
Applying Secret Sharing to Enhance Cloud Privacy.
DOI: 10.5220/0013191800004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 4*, pages 716-724
ISBN: 978-989-758-777-1

encryption plays a crucial role in cloud security. Gentry (2009) introduced fully homomorphic encryption (FHE), enabling computations on encrypted data without decryption, ensuring privacy even when data is processed in untrusted environments.

Cloud computing security risks have been extensively studied. NIST (2011) provided guidelines for securing public cloud environments, emphasizing the importance of encryption and identity management. Kandukuri and Rakshit (2009) highlighted security challenges in cloud computing, addressing issues such as data privacy, unauthorized access, and service availability.

To enhance fairness and security in secret sharing schemes, Yi Sun et al. (2016) proposed a completely fair secret sharing model without the need for a trusted dealer. Their approach reduces the risks of insider threats and unauthorized key recovery.

Modern cloud security frameworks integrate Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and secret sharing techniques to strengthen data privacy. Xiong et al. (2020) explored privacy-preserving computation using additive secret sharing, while Loruenser et al. (2015) introduced secure cloud-based data sharing mechanisms. These advancements reinforce resilience against cyber threats and improve compliance with regulatory standards.

3 RESEARCH GAP ANALYSIS

Cloud security continues to evolve, addressing challenges related to data confidentiality and access control. Despite advancements, existing security models still face limitations that necessitate a two-level security approach integrating advanced cryptographic methods and AI- driven anomaly detection. Identity and Access Management (IAM) systems are essential for authentication and authorization but have several weaknesses, including static role-based access control (RBAC), which lacks flexibility in dynamic environments, single-factor authentication vulnerabilities, and scalability issues in multi-cloud infrastructures. Multi-Factor Authentication (MFA) enhances security, yet challenges such as user experience trade-offs, device dependency risks, and attack techniques like social engineering and SIM swapping highlight the need for adaptive authentication measures. In key management, Shamir's Secret Sharing (SSS), while widely used, introduces computational overhead, complexity in reconstruction, and limitations when relying solely on polynomial interpolation techniques. Security threats in cloud storage and data transmission persist due to reactive rather than proactive intrusion detection, inadequate encryption standards, and limited AI integration in threat detection systems. Compliance with regulatory frameworks like GDPR and HIPAA poses additional challenges, particularly cross-border data privacy conflicts, manual compliance audits prone to errors, and concerns regarding legal and ethical security enforcement. To address these issues, a two-level security model is proposed, incorporating adaptive IAM policies and biometric-enhanced MFA for authentication, a hybrid secret-sharing approach to optimize key management, AI-driven threat detection using deep learning models for real-time security monitoring, and automated compliance verification tools to align with international security standards. By integrating these advancements, the system enhances cloud security resilience, mitigates evolving cyber threats, and ensures regulatory adherence while maintaining usability and performance.

4 PROPOSED SOLUTION

The proposed system strengthens cloud security by implementing a two-level security framework that integrates advanced authentication, robust key management, and crypto- graphic techniques to ensure secure access and data protection. The approach minimizes the risk of unauthorized access, key exposure, and regulatory non-compliance, providing a scalable and efficient security solution.

A refined Identity and Access Management (IAM) framework is implemented to control access at a granular level. The system ensures that user roles and permissions are assigned based on responsibilities and security policies, preventing unauthorized access to sensitive data and operations.

To provide stronger authentication, the system integrates biometric verification (such as fingerprint or iris scanning) alongside hardware tokens that generate temporary access codes. This multi-layered authentication approach significantly reduces the risk of credential theft, phishing, and brute-force attacks. To protect encryption keys from unauthorized access, the system incorporates Shamir's Secret Sharing Scheme (SSS). This method divides an encryption key into multiple shares, ensuring that only a predefined number of shares can be combined to reconstruct the original key, preventing single-point key exposure. Polynomial interpolation (Lagrange interpolation) is used as part of this scheme,

allowing keys to be reconstructed securely when enough authorized shares are available. This approach strengthens cryptographic security, ensuring that encryption keys remain protected even if some shares are compromised.

The system employs adaptive security protocols that dynamically adjust authentication and security requirements based on user behavior, device security, and access patterns. If a login attempt is made from an unfamiliar location or device, additional security verification is triggered. Automated compliance mechanisms ensure that data protection regulations like GDPR and HIPAA are met by integrating audit logging, encryption enforcement, and real-time breach detection.

To minimize security risks related to human error and social engineering attacks, the system includes comprehensive security training modules that educate users on best security practices, compliance requirements, and proper authentication methods.

5 METHODOLOGY

The development of the proposed system follows a structured approach that incorporates best practices in software engineering, security system design, and user-centered principles to ensure a robust and efficient security framework. The process begins with a requirement analysis, where stake- holder needs are assessed to align the system with the roles of Admins, Managers, and Employees. Additionally, a risk assessment is conducted to identify potential security threats and define necessary protective measures. Figure 1 shows the file management.

Following the requirement phase, the system design is structured to integrate multi-layered security mechanisms, including an IAM framework, Multi-Factor Authentication (MFA), Shamir's Secret Sharing, and polynomial interpolation for secure key management. User interfaces are designed to ensure accessibility and efficiency based on user roles. In the implementation phase, the system is developed using secure coding practices, incorporating biometric authentication and hardware tokens within the MFA module. The key management system is enhanced using Shamir's Secret Sharing to prevent unauthorized access, while polynomial interpolation ensures secure encryption key reconstruction.

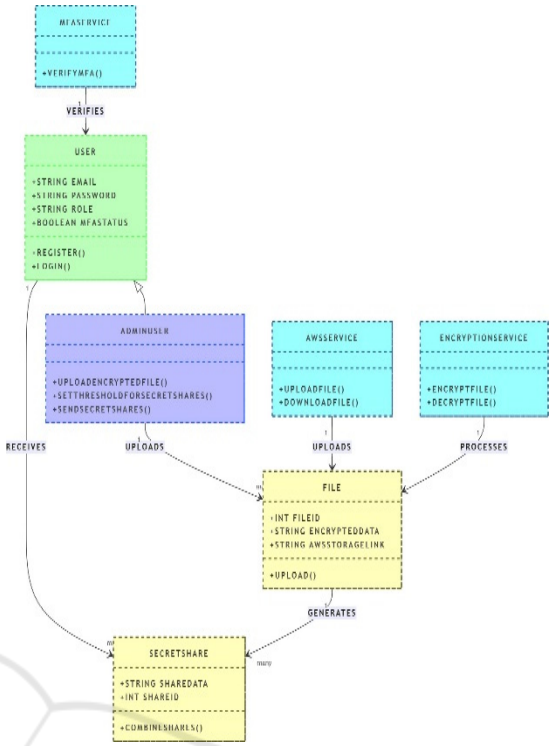

Figure 1: File management.

The system undergoes extensive testing and validation, including unit testing, integration testing, and security assessments such as penetration testing and vulnerability analysis, ensuring the resilience of the system against cyber threats. Once validated, it is deployed in a controlled cloud environment, where its performance is monitored, and necessary security adjustments are made. Comprehensive user training is provided to ensure effective system utilization.

To maintain long-term security and efficiency, the system is continuously updated to counter new security threats, ensuring that access controls and policies evolve in line with organizational requirements. The platform is structured into three key modules the Admin Module, which handles user management, role definitions, and security settings, including key distribution through Shamir's Secret Sharing; the Manager Module, responsible for access monitoring, security compliance reporting, and incident management; and the Employee Module, which facilitates secure login, data interaction, and access to security training materials.

This methodology ensures that the system not only protects sensitive data but also enhances operational efficiency and regulatory compliance across different levels of the organization. By integrating advanced cryptographic techniques and

adaptive security mechanisms, the system provides a scalable and resilient security model for cloud computing environments.

The proposed system is structured to ensure secure key management and access control within a cloud computing environment. Its design incorporates multiple security layers that focus on authentication and encryption while maintaining ease of use and efficiency. The user interface is designed with dedicated access points for Admins, Managers, and Employees, each with defined permissions based on their roles. User authentication is managed through a centralized authentication gateway, where login attempts undergo verification, incorporating Multi-Factor Authentication (MFA) for added security. At the backend, the Identity and Access Management (IAM) module enforces Role-Based Access Control (RBAC) to regulate permissions and ensure that users can only access data relevant to their roles. Authentication services validate user credentials, processing password verification alongside biometric or token-based authentication as part of MFA. Additionally, a key management module is implemented, integrating Shamir's Secret Sharing (SSS) algorithm for secure key distribution and reconstruction using polynomial interpolation. To further strengthen security, MFA mechanisms such as biometric scans, OTPs, and hardware tokens are implemented to verify user identity beyond traditional login credentials. A real-time encryption and decryption service ensures that all cloud-stored data remains protected. The database infrastructure securely stores user details, access rights, and system logs, which are continuously monitored for anomalies. Network security is reinforced using SSL/TLS encryption, with firewalls and intrusion detection systems actively monitoring for unauthorized access attempts. For key management, the system employs Shamir's Secret Sharing (SSS), a cryptographic method that divides encryption keys into multiple fragments (shares). These key fragments are dis- tributed among authorized users, requiring a minimum thresh- old of shares to reconstruct the full key. This prevents any single entity from having complete control over the encryption process. The reconstruction of the original key is achieved through polynomial interpolation using Lagrange's method, ensuring that secrets can be securely retrieved without direct exposure. The RBAC framework further enhances security by assigning access permissions based on predefined roles, preventing unauthorized users from obtaining unnecessary privileges. The MFA component ensures that authentication.

6 EXPERIMENTAL RESULTS

The multi-layered security framework enhances cloud security by implementing multiple identity verification steps, reducing the risk of account compromise. To protect both stored and transmitted data, the system integrates strong encryption standards like AES-256. By combining advanced cryptographic algorithms, multi-layered authentication, and adaptive security policies, the framework ensures data confidentiality, secure access management, and robust encryption, making it a reliable solution for modern cloud environments. The effectiveness of this security framework was evaluated across AWS and Google Cloud platforms, measuring key performance factors such as encryption overhead, data retrieval speed. The results demonstrated a significant reduction in security breaches compared to conventional methods.

Key advancements in the security model include enhanced authentication measures through a two-tier authentication process, which minimizes unauthorized access risks. The framework also supports compliance with regulations like GDPR and HIPAA, simplifying legal adherence for organizations handling sensitive data. Its scalable and flexible architecture enables seamless integration with various cloud platforms, catering to diverse organizational security needs. User-centric security management ensures ease of use while incorporating advanced cryptographic techniques without adding complexity. Furthermore, the framework extends protection to IoT devices and mobile platforms, addressing the evolving security challenges of cloud-connected ecosystems. Real-time threat monitoring enables automated security analysis, offering instant detection and response to potential cyber threats, ensuring a more resilient and secure cloud infrastructure.

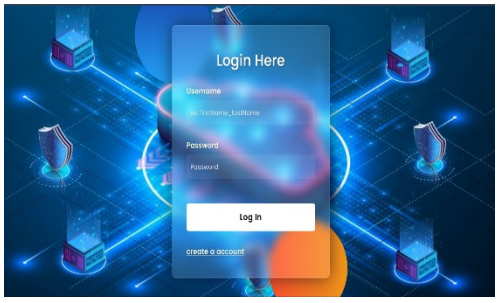

Figure 2: User registration.

The system comprises three primary modules: Admin, Manager, and Employee, each with distinct

responsibilities. [figure 2] The Admin module enables user management, allowing administrators to create, modify, or delete user profiles while assigning roles and permissions based on organizational policies. They define role-based access controls within the IAM framework and configure security settings, including multi- factor authentication (MFA) preferences and key management protocols, utilizing Shamir's Secret Sharing for key distribution and recovery.

The Manager module focuses on access oversight, monitoring logs for anomalies, reviewing employee access requests, and ensuring compliance through security audits and reports. Additionally, managers handle incident management by coordinating with admins and security teams to mitigate risks and address vulnerabilities. Employees access cloud services securely through a login process incorporating MFA and perform tasks such as data entry.

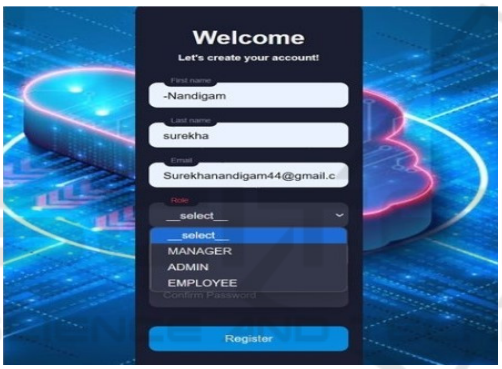

Figure 3: User login.

Figure 4: Authentication.

The login system integrates a secure authentication gate- way that processes user credentials and enforces multifactor authentication (MFA) for enhanced security as shown in figure 3. Users authenticate via passwords, and based on risk assessment, the system triggers additional authentication layers such as biometric verification. The biometric authentication module supports fingerprint scanning, facial recognition, and other biometric methods, ensuring secure identity verification before granting access As shown in figure 4. Session management is handled through secure token-based authentication, maintaining user sessions while preventing unauthorized access. Additionally, all login attempts are logged for audit purposes, and data transmissions are protected using SSL/TLS encryption to safeguard credentials and biometric data from interception or tampering. Key Libraries and Features Used in the work which are cryptography library provides developers with tools to secure data through encryption and decryption. It supports various algorithms, such as AES and RSA, and enables the implementation of custom cryptographic solutions like Shamir's Secret Sharing. This library balances high- level functionality for ease of use with low-level access for greater flexibility and security. The secrets module generates cryptographically strong random numbers, essential for secure password creation and authentication token generation, making it a safer alternative to the basic random module. The panda's library efficiently manages large datasets, such as user logs and access data, by offering structures that facilitate filtering, grouping, and security-relevant data analysis. Frameworks like Flask and Django are used to build secure APIs and administrative interfaces. Flask is a lightweight option for smaller projects, while Django is a comprehensive framework suited for complex applications. Both support secure session handling and authentication mechanisms. For testing, pytest simplifies writing tests and ensures the functionality of security components with its intuitive syntax and powerful features. Finally, libraries like sympy and numpy are essential for per- forming complex mathematical calculations in cryptography. Sympy specializes in symbolic mathematics, while NumPy efficiently handles large-scale numerical computations required for encryption and hashing.

As shown in figure 5 The system enhances security in file up- loads and secret sharing by integrating encryption, controlled access, and adaptive authentication. It employs a threshold- based approach where a secret is divided into multiple parts, requiring a minimum number of shares for reconstruction, preventing unauthorized retrieval. Uploaded files undergo security checks to detect potential threats before processing. AES-256 encryption ensures confidentiality during both storage and transmission. Role-Based Access Control (RBAC) restricts access based on predefined roles, ensuring only authorized users manage secret shares.

Figure 5: File management.

Adaptive security mechanisms evaluate factors such as user location, device security, and access history to adjust authentication levels dynamically. By combining these security layers, the system effectively prevents unauthorized access, protects sensitive data, and strengthens resilience against potential cyber threats.

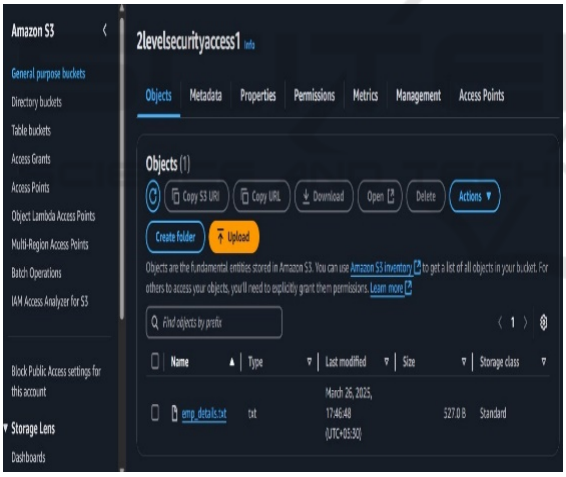

Figure 6: Generated shares.

Figure 6 shows the image displays shares generated and distributed through email using Shamir's Secret Sharing (SSS) algorithm. This cryptographic technique divides a secret into multiple parts, each assigned to different participants. The format of each share follows" Share: X -¿ Y," where X represents the participant number and Y is the corresponding share value. Only a specific number of these shares, as defined by the threshold, are required to reconstruct the original secret. This method enhances security by ensuring that no single participant has access to the complete secret, making it useful for secure data storage and cryptographic key management.

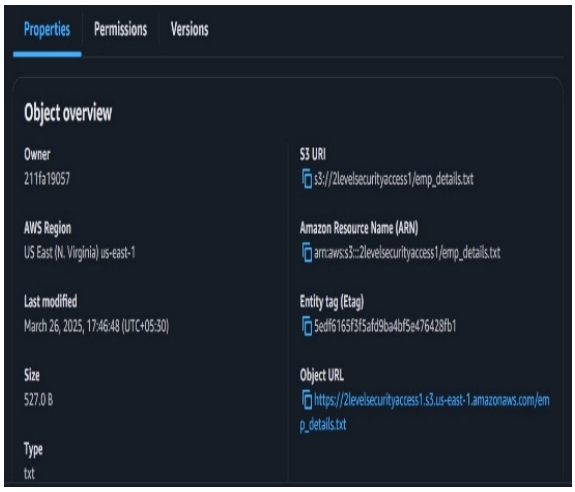

Figure 7: S3 bucket.

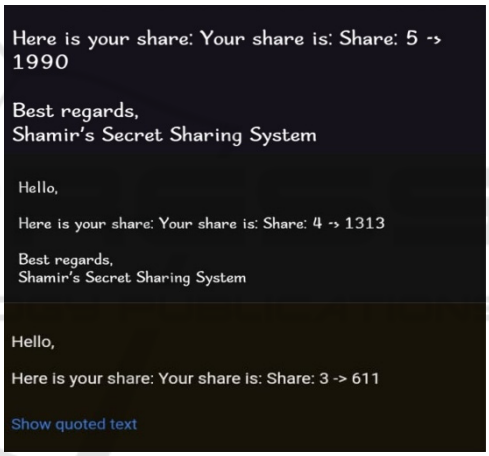

Figure 8: Object folder.

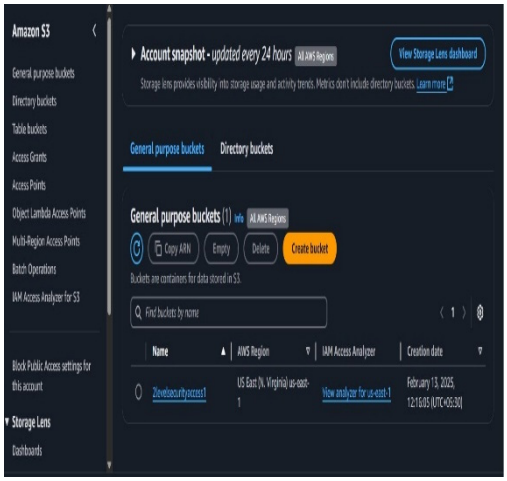

Figure 9: Bucket.

As shown in figure 7,8,9 Encrypted files are securely stored in an Amazon S3 bucket to ensure data confidentiality and prevent unauthorized access. Using Shamir's Secret Sharing (SSS) scheme, encrypted file shares are distributed among multiple recipients, requiring a set number of shares to reconstruct the original secret. This encryption method ensures that even if a single share is exposed, the complete data remains protected. AWS S3 provides robust security features such as access control policies, encryption at rest, and logging mechanisms. Once the required shares are combined using polynomial interpolation, the decrypted file becomes accessible to authorized users. This approach ensures secure data management, compliance with best security practices, and protection against unauthorized access in cloud environments.

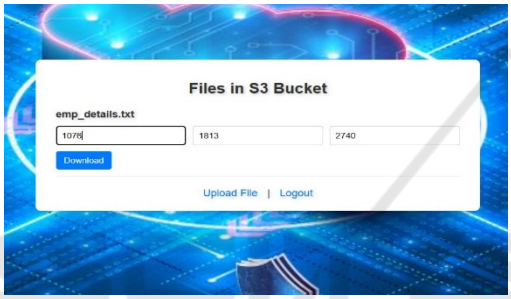

Figure 10: Combine shares.

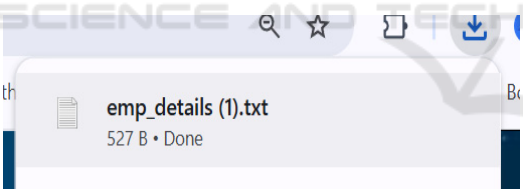

Figure 11: Downloaded file.

Shamir's Secret Sharing (SSS) scheme securely distributes encrypted file shares among multiple recipients. Each recipient holds a unique share, preventing any single entity from accessing the complete secret. To decrypt the file, users must input their shares, which are processed using Lagrange interpolation to reconstruct the original secret. Polynomial interpolation, as discussed by Gennaro et al. (2000), is crucial in cryptographic functions, particularly in key management systems. It allows secure secret reconstruction without exposing the full information. A random polynomial embeds the secret, generating multiple shares distributed among participants. like shown in figure 10 To access the encrypted file, a minimum number of shares must be combined. The secret is then reconstructed using mathematical techniques, ensuring unauthorized users with insufficient shares cannot access the data. Once restored, the encrypted file is decrypted and made available for download, ensuring secure data handling and preventing unauthorized access Like in figure 11.

System Requirements Used for To ensure a robust and se- cure system, the hardware requirements include a server with a quad-core processor or higher to efficiently manage concurrent security operations and data processing. The system should have a minimum of 16 GB RAM for smooth execution of multiple security modules and database operations, along with an SSD of at least 1 TB to store log data, user information, and critical security settings. The network interface should support Gigabit Ethernet to handle high-speed network traffic and secure data transfers. Client devices must be compatible with Windows, macOS, and Linux for administrative access, while also incorporating biometric sensors for multi-factor authentication (MFA) and keeping up with the latest security patches. On the software side, a Linux-based operating system is preferred for the server due to its stability and security features, while the client systems must support the latest versions of Windows, macOS, or Linux. The system should use a secure and scalable database management system like PostgreSQL or MySQL to handle user data, access logs, and other security- related information. Backend development should be done using Python 3.8 or higher, allowing integration with security libraries and frameworks, while the front-end can be developed using React or Angular for an interactive user experience. Security and cryptographic implementations should leverage libraries like PyCrypto for cryptographic algorithms, including Shamir's Secret Sharing, and OpenSSL for encryption and secure communication needs. Network security is critical, requiring a firewall to protect internal networks from unauthorized access, VPN access to enable secure remote administration, and an Intrusion Detection System (IDS) to monitor and report potential security threats in real time. To ensure high availability, network redundancies should be implemented to minimize downtime during heavy loads or potential attacks. Security compliance should adhere to international standards such as GDPR, HIPAA, and ISO/IEC 27001, with regular security audits conducted to identify vulnerabilities and maintain compliance. Data protection strategies must include encryption for both stored and transmitted data, along with secure data backup solutions to maintain integrity and availability in case of cyber threats or hardware failures. User authentication should incorporate MFA, including

biometrics and hardware tokens, while Role-Based Access Control (RBAC) should be implemented to enforce minimal privilege access based on user roles. Maintenance and support require regular software and hardware updates to counter emerging security threats and enhance performance. Scheduled backups and security drills should be conducted to ensure system resilience. A dedicated support team must be available to handle system issues, user training, and security incidents, while comprehensive documentation should be provided for system setup, configuration, and troubleshooting.

Final Remarks.

The proposed two-level security system establishes a resilient approach to securing cloud-based infrastructures by addressing both current and emerging threats. By incorporating encryption, multi-layer authentication, and AI-driven monitoring, the system ensures a higher degree of security, privacy, and regulatory compliance. As cloud computing continues to evolve, such frameworks will play a critical role in safeguarding digital assets, fostering innovation, and enabling organizations to confidently leverage cloud technologies while maintaining robust security postures.

7 FUTURE WORK

The proposed system offers a robust foundation for securing cloud environments, with opportunities for future enhancements that can improve adaptability, resilience, and efficiency. One area for development is the use of machine learning to analyze access patterns and detect anomalies, enabling dynamic protection adjustments based on real-time risk assessments. Blockchain technology can also be integrated to create tamper- proof logs for access control and security event tracking, while smart contracts automate compliance verification. To safeguard against future threats, quantum-resistant cryptography, including quantum-safe algorithms and quantum key distribution, can be incorporated. Expanding the security model to support hybrid and multi-cloud infrastructure ensures consistent protection across platforms and enables unified security policies. Additionally, extending security to IoT devices and edge computing environments addresses challenges in authentication and data encryption. The system must also adapt to changing data protection regulations by implementing advanced anonymization techniques that maintain privacy without com- promising performance. Real-time user behavior analytics will help identify insider threats, refine access control policies, and improve risk-based authentication. Enhanced disaster recovery strategies and automated failover mechanisms ensure business continuity and minimize downtime. Finally, offering Security- as-a-Service (SECaaS) makes customizable security solutions accessible to businesses of all sizes, integrating seamlessly with various cloud platforms without requiring significant infrastructure investments.

8 CONCLUSIONS

This work provides an innovative solution to the growing security challenges faced by cloud environments. By incorporating a two-tier security model that integrates both cloud-native security policies and user-specific authentication mechanisms, the proposed system significantly strengthens data protection. The first layer, built on Identity and Access Management (IAM) policies, ensure proper role-based access control, while the second layer enhances security through Multi-Factor Authentication (MFA), using email-based One-Time Pass- words (OTP) for user verification. Additionally, the application of Shamir's Secret Sharing combined with polynomial interpolation techniques provides a robust framework for secure key management and access control, especially in hierarchical organizational structures. This approach not only minimizes the risk of unauthorized data access but also ensures the integrity and confidentiality of cloud-stored data. By addressing both provider-level and user-specific security concerns, this work sets a new standard for cloud security, contributing to more resilient and compliant cloud infrastructures in the face of evolving cyber threats. The proposed model is a critical step toward creating more secure, adaptive, and scalable cloud environments, ensuring long-term data protection and trust in cloud-based services.

REFERENCES

Beimel,"Improved Polynomial Secret-Sharing Schemes," Cryp- tology ePrint Archive, Report 2023/1158, 2023. [Online]. Available: https://eprint.iacr.org/2023/1158.

C.-C. Yao, "How to Generate and Exchange Secrets," in Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS), 1986, pp. 162-167.

Gentry, "Fully AES encryption using ideal lattices," in Proceedings of the 41st ACM Symposium on Theory of Computing (STOC), 2009.

H. Hourani and M. Abdallah, "Cloud Computing: Legal and Security Issues," in Proceedings of the 8th International Conference on Computer Science and Information Technology (CSIT), 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8486190.

K. Tjell and R. Wisniewski," Privacy in Distributed Computations Based on Real Number Secret Sharing," arXiv preprint arXiv:2107.00911, Jul. 2021. [Online]. Available: https://arxiv.org/abs/2107.00911.

K. Pietrzak," Secret-Sharing Schemes for High Slices," Cryptol- ogy ePrint Archive, Report 2024/602, 2024. [Online]. Available: https://eprint.iacr.org/2024/602.

L. Xiong, W. Zhou, Z. Xia, Q. Gu, and J. Weng," Efficient Privacy-Preserving Computation Based on Additive Secret Sharing," arXiv preprint arXiv:2009.05356, Sep. 2020. [Online]. Available: https://arxiv.org/abs/2009.05356.

L. Wang, J. Liu, and K. Chen," Lattice-Based Threshold Secret Sharing Scheme and Its Applications," Electronics, vol. 13, no. 2, p. 287, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/13/2/287.

NIST, "Guidelines on security and privacy in public cloud computing," Special Publication 800-144, 2011.

Parakh and S. Kak," Space-Efficient Secret Sharing for Implicit Data Security," Information Sciences, vol. 181, no. 2, pp. 335-341, Jan. 2011. [Online]. Available: https://doi.org/10.1016/j.ins.2010.09.021.

R. Kandukuri and A. Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5170911.

S. Chhabra and A. K. Singh," Security Enhancement in Cloud Envi- ronment using Secure Secret Key Sharing," Journal of Communications Software and Systems, vol. 16, no. 4, pp. 296-305, Dec. 2020. [Online]. Available:https://doi.org/10.24138/jcomss.v16i4.964.

Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

T. Loruenser, A. Happe, and D. Slamanig," ARCHISTAR: Towards Secure and Robust Cloud-Based Data Sharing," in Proceedings of the 7th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Vancouver, BC, Canada, Nov. 2015, pp. 371–378. [Online]. Available: https://doi.org/10.1109/CloudCom.2015.71.

T. Stevens, J. Near, and C. Skalka," Secret Sharing for Highly Scal- able Secure Aggregation," arXiv preprint arXiv:2201.00864, Jan. 2022. [Online]. Available: https://arxiv.org/abs/2201.00864.

X. Li, Y. Wang, and Z. Zhang," Secret Sharing: A Comprehensive Survey, Taxonomy, and Applications," Journal of Information Security and Applications, vol. 66, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1574013723000758.

Y. Liu, F. Zhang, and J. Zhang," Attacks to Some Verifiable Multi- Secret Sharing Schemes and Two Improved Schemes," Information Sciences, vol. 328, pp. 582-591, Feb. 2016. [Online]. Available: https://doi.org/10.1016/j.ins.2015.09.035.

Y. Sun, G. Li, Z. Lin, F. Xiao, and X. Yang, "A Completely Fair Secret Sharing Scheme without Dealer," in Proceedings of the International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2016. DOI: 10.1109/ICCE-TW.2016.7520905.

Y. Liu, X. Wu, and Z. Zhao," ROMSS: A Rational Optional Multi- Secret Sharing Scheme Based on Cloud Computing," Journal of Cloud Computing, vol. 12, no. 1, p. 45, 2023. [Online]. Available: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677- 023-00495-7.

Y. Zhang and X. Chen, A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structures," Axioms, vol. 13, no. 8, p. 515, 2023. [Online]. Available: https://www.mdpi.com/2075-1680/13/8/515.