An Intelligent Privacy-First Anonymous Authentication System for Cloud Computing with Advanced Multi-Factor Safeguards

Bhaskar Babu Kuchanapally[1], Bollu Sairaj[2], Vemula Pavan Kalyan[2], Tholla Sampath[2], Manikayala Vinay [2], Vanga Ankitha [2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

To Cite this Article
Bhaskar Babu Kuchanapally, Bollu Sairaj, Vemula Pavan Kalyan, Tholla Sampath, Manikayala Vinay, Vanga Ankitha, "An Intelligent Privacy-First Anonymous Authentication System for Cloud Computing with Advanced Multi-Factor Safeguards", Journal of Science Engineering Technology and Management Science, Vol. 03, Issue 04, April 2026,pp: 534-543, DOI: http://doi.org/10.64771/jsetms.2026.v03.i04.pp534-543*
Submitted: 28-02-2026 Accepted: 02-04-2026 Published: 10-04-2026

Abstract

The growing dependence on cloud-based storage systems has introduced critical challenges in maintaining secure file sharing, reliable user authentication, and data confidentiality. As digital data continues to expand, protecting sensitive information from unauthorized access and cyber threats has become increasingly important. Traditional file-sharing systems typically rely on single-factor authentication and basic encryption techniques, which are often inadequate for modern security requirements. These approaches are vulnerable to data breaches, identity spoofing, and performance inefficiencies when processing large volumes of data. The primary problem addressed in this work is the design of a secure and efficient cloud-based file-sharing system that enhances authentication strength and encryption performance while ensuring controlled access to data. Existing systems lack multi-layer security mechanisms, biometric verification, and effective performance evaluation of cryptographic techniques, resulting in limited scalability and weaker protection. To overcome these limitations, the proposed system adopts a hybrid approach that integrates advanced cryptographic methods with multi-factor authentication. It utilizes Elliptic Curve Cryptography (ECC) for secure asymmetric encryption and ChaCha20 for fast and efficient symmetric encryption. The system is implemented using the Django framework with a My Structured Query Language (MySQL) database to manage user credentials, file metadata, and access control. Additionally, authentication is strengthened through password hashing combined with fingerprint-based verification. The system also compares the computational efficiency of ECC and ChaCha20, presenting the results through graphical analysis. The significance of this approach lies in its ability to provide enhanced security, efficient encryption, and scalable performance, making it a reliable solution for secure cloud-based file storage and sharing applications.

Keywords: Cloud Storage Security, Multi-Factor Authentication, Elliptic Curve Cryptography (ECC), ChaCha20 Encryption, Secure File Sharing, Data Confidentiality

1. Introduction

Cloud authentication is the process of verifying user identities within a cloud environment to determine whether a user is authorized to access applications, data, services, and resources. It ensures that only legitimate users are granted appropriate access rights and privileges. However, the absence of strong

and effective authentication mechanisms can expose cloud systems to various security threats and attacks. Common cloud security risks include information disclosure, Denial-of-Service (DoS), identity spoofing, data tampering, repudiation, account hijacking, and privilege escalation [1,2]. As shown as figure 1 In addition, cloud authentication systems are susceptible to several types of attacks such as DoS attacks, Man-in-the-Middle (MITM) attacks, replay attacks, cloud malware injection attacks, password discovery attacks, reflection attacks, customer fraud attacks, insider threats, and Known Session-Specific Temporary Information (KSSTI) attacks [3,4]. Authentication techniques serve as the primary line of defense against unauthorized access to cloud-based applications, data, and services. Various methods have been developed to strengthen authentication, including password-based authentication, Single Sign-On (SSO) [5], token-based authentication, graphical password techniques, biometric authentication, third-party authentication [6],

Figure. 1: Multifactor authentication system.

certificate-based authentication, device-based authentication, two-factor authentication, and multi-factor authentication (MFA). In recent years, organizations have increasingly adopted MFA in cloud systems to enhance security, minimize the risks associated with compromised credentials, improve compliance with regulations, and support flexible enterprise operations [7].

2. Literature Survey

Mostafa, et al. [8] developed an adaptive multi-factor and multi-layer authentication framework for cloud platforms, aiming to significantly enhance security and reduce false positive alarms for unauthorized access. They implemented a dynamic authentication approach that utilized several factors for identity verification, which included examining the length and validity of the user's credential, along with checks based on the user's geolocation and browser confirmation method. Alatawi, et al. [9] researched critical challenges in cloud security by proposing a novel framework that integrated blockchain-based smart contracts to enhance authorization and authentication processes, and leveraged smart contracts to enable decentralized, transparent, and tamper-proof mechanisms for managing access control in cloud environments. The proposed system mitigated prevalent threats like unauthorized access and identity theft by providing an immutable and auditable security framework. A prototype system, developed using the Ethereum blockchain and Solidity programming, demonstrated the feasibility of this decentralized security approach, although the work did not specify the use of multi-factor protection or anonymous credentialing. Tanveer, et al. [10] presented in CMAF-IIoT is built on the ASCON authenticated encryption (AE) system, which combines encryption and decryption with authentication to provide secrecy, integrity, and authenticity. As a result, designing an authentication framework requires fewer cryptographic procedures.

Qui, et al. [11] presented a 3FA protocol is applied to provide secure, efficient, and practical for mobile lightweight devices. The extended chaotic maps component of the protocol is used to generate random

numbers. The fuzzy verifier's component of the protocol is used to verify the users' identity. Alsirhani, et al. [12] the main methodology is based on applying different layers of authentications to verify cloud users and reduce false alarms. Furthermore, different methods applied to check cloud user identity and maintain the secrecy of data. The key threats in different cloud computing applications and environments include data loss, hijacking of accounts, malicious users, and leakage of data. Wang, et al. [13] defined explaining failures in MFA. One of these factors is the incomplete definition of an adversary, in which the capabilities and goals of an attacker and difficulties in defining cryptographic primitives must be defined. In addition, the provided MFA frameworks may be complex or unable to identify vulnerabilities. These factors are checked with eight proof failures to examine vulnerabilities. Wu, L., et al. [14] They researched on securing the encryption key in remote data backup by proposing a User-Centric Design (UCD) scheme based on multi-factor authentication. Recognizing that remote channels and backup servers are untrustworthy, the scheme employed a secret sharing mechanism to divide the encryption key into three parts, which were securely stored across the user's laptop, smart card, and the server. This key could then be reconstructed using any two of these shares, combined with the user's private information, including their password, identity, and biometrics.

Hu, et al. [15] found that the design of Liu et al.'s scheme in the authentication phase is unreasonable, as their scheme cannot resist offline password-guessing attacks, server/user camouflage attacks, and so on. Then, they presented an enhanced secure data backup scheme to overcome all above-mentioned security threats. Yi, et al. [16] found that Hu et al.'s scheme cannot achieve their claimed security. Their scheme could not resist offline guessing attacks, replay attacks, and denial of service attacks. They also did not consider the situation of users rebuilding an incorrect key. Then, they proposed an enhanced scheme to address the aforementioned issues. Chang, et al. [17] proposed a data protection scheme based on Shamir's (2,3)-threshold secret sharing scheme to protect sensitive data. In their scheme, the server chooses the encryption key, and divides the key into three shares, which are stored in the laptop, the USB device, and the server, respectively. The user can reconstruct the key on the laptop with the help of the USB offline after the user obtains the authentication of the USB device via their identity and password.

Bamashmos, et al. [18] proposed, two-layered multi-factor authentication (2L-MFA) framework based on blockchain to enhance the security of IoT devices and users. In their work, the first level of authentication was implemented for IoT devices, considering secret keys, geographical location, and physically unclonable functions (PUFs). They utilized Proof-of-Authentication (PoAh) and elliptic curve Diffie–Hellman to achieve lightweight and low-latency communication. The second level of authentication was designed for IoT users, which were further divided into four sub-levels, each defined by specific factors such as identity, password, and biometrics. Wu, Y., et al. [19] They presented an identity management scheme based on multi-factor authentication and dynamic trust evaluation for telemedicine applications. Their authentication mechanism combined iris recognition for secure biometric verification, smart cards for encrypted credential storage, and static passwords for supplementary verification, effectively addressing scenarios such as facial coverage in medical environments. The proposed scheme dynamically adjusted the authentication process based on factors like attack rates, login anomalies, and service durations.

3. Proposed System

The system is designed to provide a secure and efficient platform for cloud-based file sharing by integrating advanced authentication and encryption techniques. It focuses on protecting sensitive data during upload, storage, and download processes while ensuring that only authorized users can access the files. The application is developed using a web-based framework with a structured database to manage user information, file details, and access permissions effectively. The system incorporates a

hybrid cryptographic approach to enhance data security and performance. It utilizes both asymmetric and symmetric encryption methods to ensure strong protection and faster processing. Additionally, a multi-factor authentication mechanism is implemented, combining password verification with biometric validation to strengthen user identity verification, as shown in figure 2. An access control mechanism is also included to regulate file sharing based on user permissions, ensuring privacy and security. Furthermore, the system evaluates the performance of encryption techniques by measuring computation time and presenting the results through graphical visualization, providing insights into efficiency and reliability.

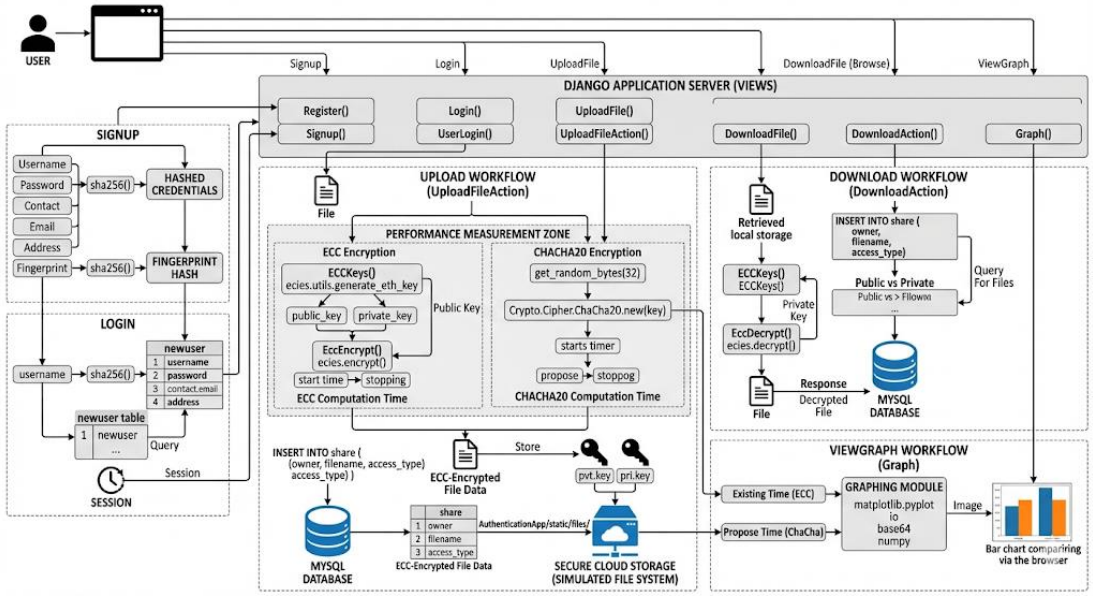


Figure. 2: Proposed system architecture.

3.1 Elliptic Curve Cryptography (ECC)

ECC is an asymmetric cryptographic technique that uses the mathematical properties of elliptic curves to generate public and private key pairs. It provides high security with smaller key sizes compared to RSA, making it computationally efficient. ECC encrypts files uploaded by users, ensuring confidentiality during cloud storage. Only the user with the correct private key can decrypt files, maintaining secure access illustrated Figure 3.

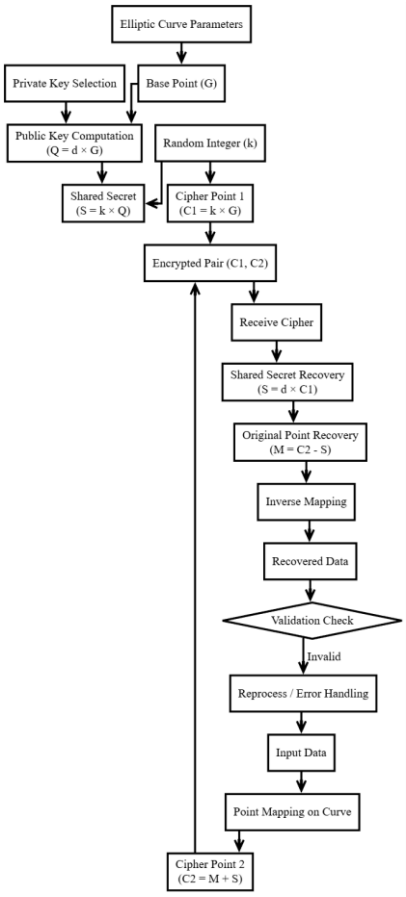


Figure. 3: Internal work flow of ECC.

Elliptic Curve Parameter Initialization: ECC begins by defining domain parameters including the elliptic curve equation, finite field, base point (G), and curve order. These parameters establish the mathematical structure used for secure key operations.

Key Generation: A private key is selected as a random integer within the curve's valid range. The public key is derived by performing scalar multiplication of the base point with the private key, creating a one-way relationship that is computationally hard to reverse

Shared Secret / Encryption Computation: During encryption or key exchange, an ephemeral random value is generated and used with elliptic curve point multiplication. This produces a shared secret derived from combining the sender's temporary value and the receiver's public key.

Cipher Construction or Key Derivation: The shared secret is converted into a usable cryptographic key or combined with mapped data points to produce encrypted output. This stage ensures that only someone with the corresponding private key can recover the original information.

Decryption / Shared Secret Recovery: The receiver uses their private key with received elliptic curve points to recompute the same shared secret. Due to elliptic curve properties, both parties derive identical secrets without directly transmitting them.

Validation and Integrity Checks: Final validation confirms that curve points are valid and operations were performed within allowed parameters. This prevents invalid-curve attacks and ensures secure reconstruction of the original data

4. Result Description

The results demonstrate the effectiveness of the system in providing secure and efficient file sharing through integrated encryption and authentication mechanisms. The implementation successfully ensures controlled access to files while maintaining data confidentiality during upload and download processes. Performance analysis indicates that symmetric encryption achieves faster computation compared to asymmetric encryption, while the latter provides stronger security for key management. The graphical representation of computation time clearly highlights the efficiency differences between the techniques. The system achieves a balance between security and performance, validating the reliability of the proposed approach in real-time applications.

Figure 4 illustrates the home page screen of the hybrid identity protection and multi-factor authentication framework for cloud security, representing the initial interface through which users access authentication and cloud storage functionalities. It depicts the starting point of the system where identity verification and secure access workflows are introduced. The figure reflects the integration of multi-factor authentication concepts with cloud-based resource management. It represents the foundational stage that connects users to registration, login, and secure operations.

Figure. 4: Home page screen.

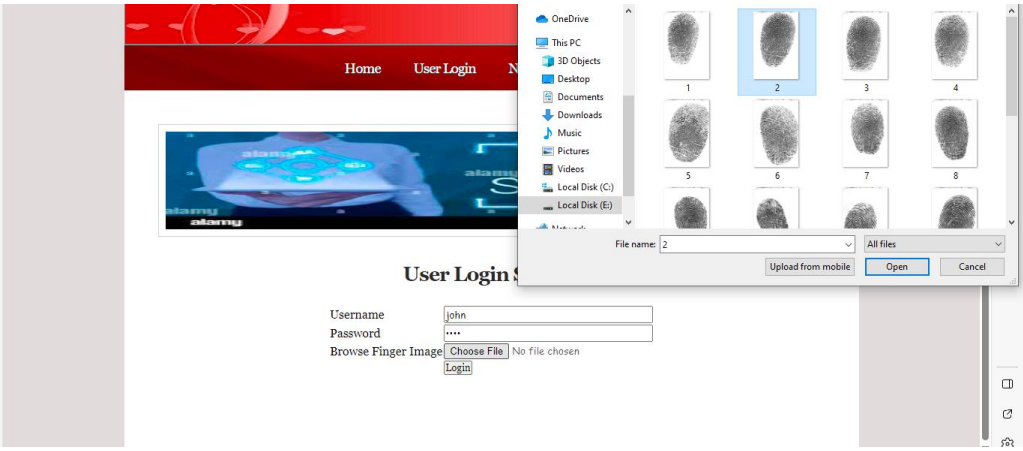


Figure. 5: User login screen.

Figure 5 illustrates the user login screen, representing the authentication stage where registered users verify their identity through multiple authentication factors. It depicts the integration of biometric validation alongside standard login credentials. The figure reflects how multi-layered authentication mechanisms reduce the risk of unauthorized access. It demonstrates the process of validating identity before granting access to cloud services.

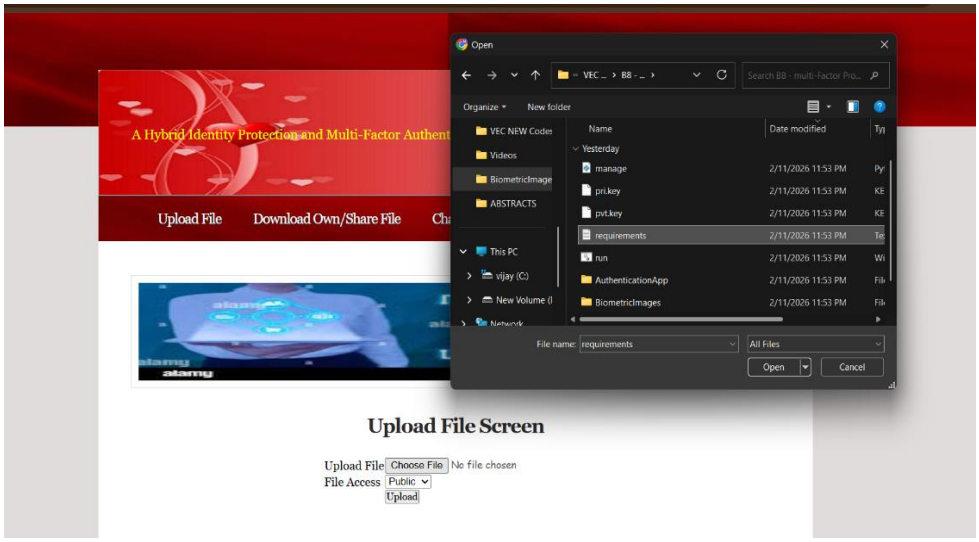
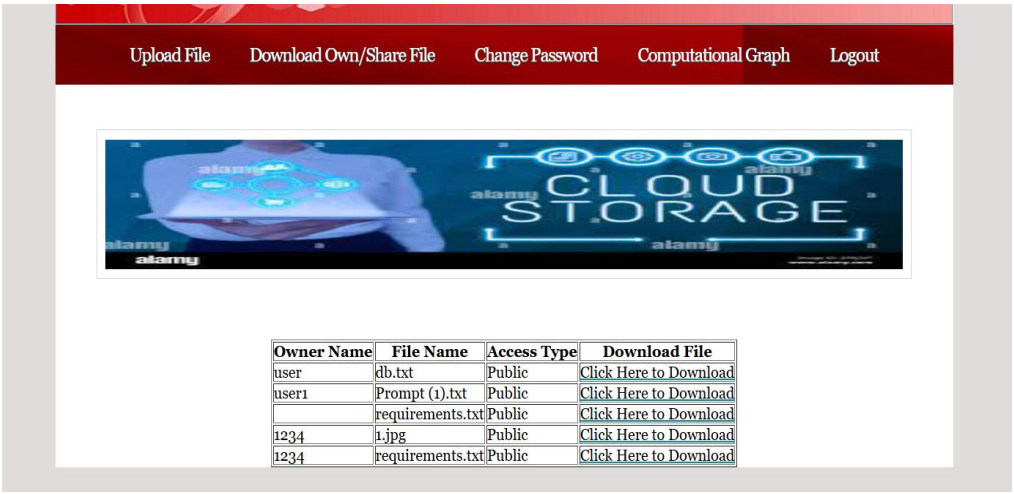


Figure. 6: Upload file screen.

Figure 6 depicts the upload file screen, representing how authenticated users securely upload files to cloud storage under controlled access policies. It illustrates the system's capability to manage file permissions and enforce secure storage operations. The figure reflects the integration of access control mechanisms with cloud-based data management.



Owner Name	File Name	Access Type	Download File
user	db.txt	Public	Click Here to Download
user1	Prompt (1).txt	Public	Click Here to Download
	requirements.txt	Public	Click Here to Download
1234	1.jpg	Public	Click Here to Download
1234	requirements.txt	Public	Click Here to Download

Figure. 7: Download screen.

Figure 7 depicts the download screen, representing how users retrieve stored files while maintaining controlled access permissions. It illustrates the availability of uploaded resources along with associated access types and download options. The figure reflects how cloud storage integrates sharing and retrieval within a secure identity framework. It demonstrates how authenticated users access files based on predefined permissions.

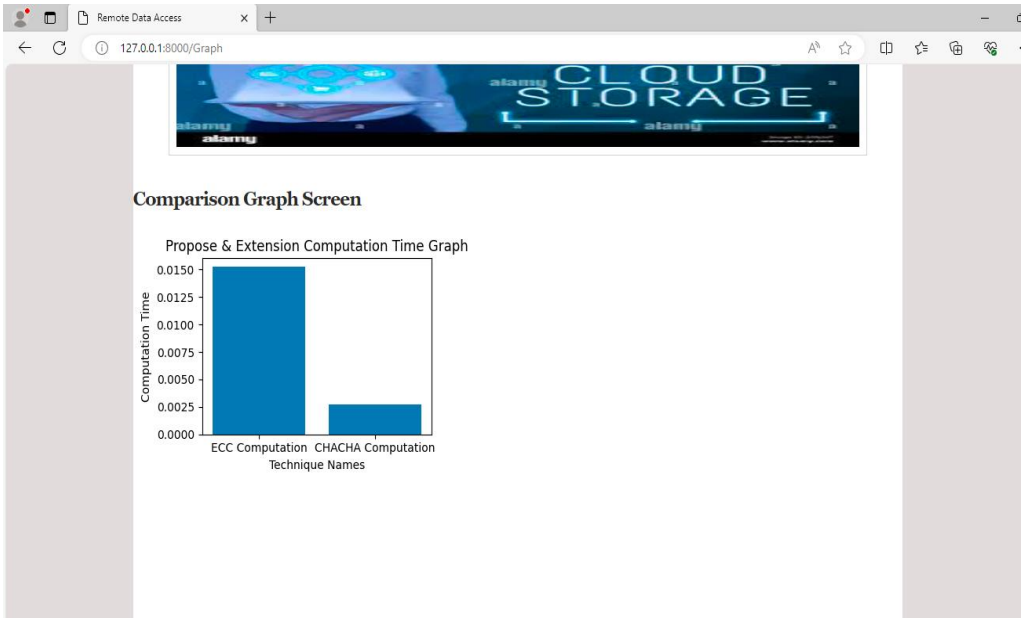


Figure. 8: Model Comparison Screen.

Figure 8 illustrates the model comparison screen, representing graphical analysis used to compare computational performance within the framework. It depicts how computation time or performance metrics are visualized to evaluate different techniques. The figure reflects the analytical component supporting system evaluation and optimization. It demonstrates how visual comparison assists in understanding performance differences between methods.

5. Conclusion

The developed system successfully addresses the challenges of secure cloud-based file sharing by integrating advanced authentication and encryption mechanisms. It ensures data confidentiality, integrity, and controlled access through a combination of strong cryptographic techniques and multi-factor authentication. The use of both asymmetric and symmetric encryption methods enhances overall security while maintaining efficiency during file operations. By incorporating biometric verification along with password-based authentication, the system significantly strengthens user identity validation and reduces the risk of unauthorized access. A key outcome of the system is the performance evaluation of encryption techniques, where computational efficiency is analyzed and compared. The results indicate that symmetric encryption demonstrates faster processing time, while asymmetric encryption provides stronger key-based security, thereby achieving a balance between security and performance. This comparison highlights the effectiveness of combining both techniques in a hybrid approach to optimize system performance. The system also implements access control mechanisms to ensure that only authorized users can access specific files, thereby improving data privacy and reliability. The graphical representation of performance metrics further enhances the understanding of system efficiency and supports better decision-making. In the future, the system can be enhanced by integrating more advanced biometric techniques, improving scalability for large-scale deployments, and incorporating real-time threat detection mechanisms. Additionally, the adoption of distributed storage and blockchain-based auditing can further strengthen data security, transparency, and trust in cloud environments.

References

[1] abrizchi, H.; Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: Issues, threats, and solutions. J. Supercomp. 2020, 76, 9493–9532.

[2] Yeng, P.K.; Wulthusen, S.D.; Yang, B. Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. Int. J. Adv. Comp. Sci. Appl. (IJACSA) 2020, 11, 772–784.
[3] Panda, D.R.; Behera, S.K.; Jena, D. A Survey on Cloud Computing Security Issues, Attacks and Countermeasures. Advances in Machine Learning and Computational Intelligence; Patnaik, X.-S., Yang, I.K., Sethi, S., Eds.; Springer: Singapore, 2021; pp. 513–524.
[4] Sumitra, B.; Pethuru, C.; Misbahuddin, M. A survey of cloud authentication attacks and solution approaches. Int. J. Innov. Res. Comp. Commun. Eng. (IJIRCCE) 2014, 2, 6245–6253.
[5] Ghasemisharif, M.; Kanich, C.; Polakis, J. Towards automated auditing for account and session management flaws in single sign-on deployments. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–26 May 2022; pp. 1774–1790.
[6] Wang, C.; Wang, D.; Duan, Y.; Tao, X. Secure and lightweight user authentication scheme for cloud-assisted internet of things. IEEE Trans. Inf. Forensics Secur. 2023, 18, 2961–2976.
[7] Li, Z.; Wang, D.; Morais, E. Quantum-safe round-optimal password authentication for mobile devices. IEEE Trans. Dependable Secur. Comp. 2020, 19, 1885–1899.
[8] Mostafa, A.M.; Ezz, M.; Elbashir, M.K.; Alruily, M.; Hamouda, E.; Alsarhani, M.; Said, W. Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Appl. Sci. 2023, 13, 10871. https://doi.org/10.3390/app131910871
[9] Alatawi, M.N. Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security. Electronics 2025, 14, 3104. https://doi.org/10.3390/electronics14153104
[10] Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81.
[11] Qui, S.; Wang, D.; Xu, G.; Kumari, S. Practical and provably secure three-factor authentication protocol based on extended chaotic maps for mobile lightweight devices. IEEE Trans. Dependable Secur. Comp. 2022, 20, 1338–1351.
[12] Alsirhani, A.; Ezz, M.; Mostafa, A.M. advanced authentication mechanisms for identity and access management in cloud computing. Comp. Syst. Sci. Eng. 2022, 43, 967–984.
[13] Wang, Q.; Wang, D.; Cheng, C.; He, D. Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices. IEEE Trans. Dependable Secur. Comp. 2021, 20, 193–208.
[14] Wu, L.; Wen, Y.; Yi, J. A Higher Performance Data Backup Scheme Based on Multi-Factor Authentication. Entropy 2024, 26, 667. https://doi.org/10.3390/e26080667
[15] Hu, H.; Lin, C.; Chang, C.C.; Chen, L. Enhanced secure data backup scheme using multi-factor authentication. IET Inf. Secur. 2019, 13, 649–658.
[16] Yi, J.; Wen, Y. An Improved Data Backup Scheme Based on Multi-Factor Authentication. In Proceedings of the 9th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 6–8 May 2023.
[17] Chang, C.C.; Chou, Y.C.; Sun, C.Y. Novel and practical scheme based on secret sharing for laptop data protection. IET Inf. Secur. 2015, 9, 100–107.
[18] Bamashmos, S.; Chilamkurti, N.; Shahraki, A.S. Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. Sensors 2024, 24, 3575. https://doi.org/10.3390/s24113575

[19] Wu, Y.; Pang, M.; Ma, J.; Ou, W.; Yue, Q.; Han, W. An Identity Management Scheme Based on Multi-Factor Authentication and Dynamic Trust Evaluation for Telemedicine. Sensors 2025, 25, 2118. https://doi.org/10.3390/s25072118