I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

A Secure and Lightweight Cryptographic Framework for Smartphone Authentication and Password Recovery Via Secret Sharing

Vikas Kumar [1*], Manjeet Singh [2], Lokesh Kumar [3]
[1-3] Department of Mathematics, L.R.(P.G.) College Sahibabad, Ghaziabad, Uttar Pradesh, India

Corresponding Author: * Vikas Kumar

DOI: https://doi.org/10.5281/zenodo.20927406

Abstract

Secure authentication and dependable password recovery are imperative as smartphones store utterly sensitive personal and financial data. The recovery methods offered by traditional password-based systems are limited and vague in cases of authorised users losing their devices or failing to remember their credentials. In this study, a cryptography-based framework for password recovery and authentication is proposed to provide safe and private access restoration. It integrates lightweight cryptographic primitives, multi-factor authentication and recovery based on secret sharing. The scheme we suggest distributes the recovery secrets among several trusted entities in various shares, such that no single entity can compromise the system. The low computational and communication overhead of the framework permits it to endure popular assaults including brute-force, replay, impersonation and man-in-the-middle attacks. This research aims to create a safe and effective solution for next-generation mobile authentication systems.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 11-05-2026
- **Accepted:** 22-06-2026
- **Published:** 26-06-2026
- **IJCRM:**5(SP1); 2026: 34-39

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Kumar V, Singh M, Kumar L. A Secure and Lightweight Cryptographic Framework for Smartphone Authentication and Password Recovery Via Secret Sharing. Int J Contemp Res Multidiscip. 2026;5(SP1):34-39.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Multi-Factor Authentication, Secret Sharing, Secure Access Control, Mobile Device (MD), Multi-factor authentication (MFA).

1. INTRODUCTION

Smartphones have become multi-functional computing platforms that enable communication, healthcare monitoring, digital identity management, financial transactions and cloud-based services, and they store utterly sensitive personal, biometric, and financial data. That's why secure authentication mechanisms have become crucial to protect user privacy and restrict unauthorised access. Despite the growth of smartphone functionality, they continue to be resource-constrained devices that are limited in battery capacity, computer processing power, and memory availability. Because of their resource constraints, authentication protocols that have been developed for use on desktops or servers cannot be readily implemented on mobile devices because the protocols are computationally complex and require a high degree of communication overhead. So, lightweight security mechanisms are required to ensure strong security with efficient performance [1].

Traditional password-based authentication systems persist in widespread adoption due to their simplicity and ease of deployment. However, password-based authentication systems have a number of well-known vulnerabilities, such as weak password selection, repeated passwords, phishing attacks, brute-force attacks, replay attacks, and credential leakage. In addition, password recovery methods are commonly considered the weakest part of an authentication system. Most password recovery methods depend upon centralised servers, sending email verification links, or SMS one-time password messages, all of which provide a single point of failure and are also subject to social engineering, SIM swap, and man-in-the-middle attacks [2].

By combining knowledge factors (passwords), possession factors (tokens or devices), and inherence factors (biometrics), multi-factor authentication (MFA) has been introduced to improve security. Password recovery procedures are often still centralised and unsafe, despite the fact that MFA increases login security. Attackers might have total control over user accounts if the recovery server is hacked [3].

Distributed cryptography methods like secret sharing have been investigated in safe systems to overcome these constraints. A secret is divided into multiple parts and allocated among trusted parties in threshold secret sharing techniques. The secret can only be regenerated with a predetermined number of shares (threshold value). This strategy develops resistance to compromise and discards single points of failure [4-5].

Although there is still an inadequacy of research on the integration of secret sharing techniques into frameworks for password recovery and smartphone authentication. Many existing authentication protocols significantly lean on computationally expensive public-key cryptographic operations, which raise mobile device latency and energy usage. A framework that is lightweight, scalable, and resistant to attacks is imperative, especially for smartphone contexts [6-7].

Research Gap

The following research gaps can be inferred from the existing literature:

1. Most smartphone authentication systems depend on centralised password recovery mechanisms [8].
2. Existing methods for recovering passwords are susceptible to impersonation, replay, or brute-forcing [9].
3. Highly complex cryptographic protocols were not designed with resource-limited smartphones in mind [10].
4. There are limited frameworks that assimilate lightweight authentication with distributed secret sharing for secure password recovery [11-12].

These limitations motivate the development of a lightweight cryptographic framework that ensures both secure authentication and robust password recovery without increasing computational overhead.

Contributions of the Paper

This paper proposes A Lightweight Cryptographic Framework for Secure Smartphone Authentication and Secret Sharing–Based Password Recovery. The main contributions are summarised as follows:

1. We design a lightweight multi-factor authentication mechanism suitable for resource-constrained smartphones.
2. We integrate a threshold-based secret sharing scheme to securely distribute password recovery secrets across multiple trusted entities.
3. We eliminate single points of failure in password recovery processes.
4. We provide resistance against common attacks, including replay, brute-force, impersonation, and man-in-the-middle attacks.
5. We analyse computational and communication overhead to demonstrate the framework's efficiency in mobile environments.
6. We present a scalable architecture suitable for next-generation mobile and cloud-based authentication systems.

Comparative Analysis

Feature	Traditional System	Proposed Framework
MFA	Limited	Yes
Secret Sharing	No	Yes
Replay Protection	Weak	Strong
Single Point Failure	Yes	No
Lightweight	Yes	Yes
Secure Recovery	No	Yes

The proposed framework improves security without significant performance degradation.

2. RELATED WORK

Smartphone authentication techniques generally include:
1. Password-based authentication 2. Biometric authentication 3. Token-based authentication (OTP) 4. Multi-factor authentication (MFA) [13-14].
Although MFA improves security, password recovery mechanisms remain weak. Most systems rely on centralised servers or email-based resets. Secret sharing schemes, such as Shamir's Secret Sharing, divide a secret into multiple shares. Only a threshold number of shares can reconstruct the secret. However, their integration into smartphone password recovery remains underexplored. Unlike existing systems, our framework integrates lightweight authentication with threshold-based secret reconstruction for secure recovery [15].

3. PROPOSED FRAMEWORK

The proposed framework consists of:
User (U) – Smartphone owner,
Mobile Device (MD) – User's smartphone,
Authentication Server (AS) – Verifies credentials,

Trusted Recovery Authorities (TRA_1, TRA_2, …, TRA_n) – Store secret shares
The framework includes three main phases:
1. Registration Phase
2. Authentication Phase
3. Password Recovery Phase

1. Registration Phase

Step 1: User selects identity ID and password PW.
Step 2: Password is hashed using lightweight hashing:

$$HPW = H(PW \,||\, Salt)$$

Step 3: A recovery master secret S is generated.
Step 4: Secret S is divided into n shares using threshold secret sharing:

$$S \rightarrow (S_1, S_2, \ldots, S_n)$$

Step 5: Each share is securely stored by a trusted recovery authority.
Step 6: Authentication server stores only hashed password and metadata.

2. Authentication Phase

Step 1: User enters ID and PW.
Step 2: Device computes:

$$AuthToken = H(HPW \,||\, N \,||\, DeviceID)$$

Where:

- N = timestamp-based nonce

Step 3: Server verifies token.
Step 4: Mutual authentication is performed.
Step 5: Secure session key is generated using lightweight symmetric encryption (e.g., AES-128).

3. Password Recovery Phase

If password is forgotten:
Step 1: User requests recovery.
Step 2: At least k out of n recovery authorities provide shares.
Step 3: Secret reconstructed:

$$S = Combine(S_1, S_2, \ldots, S_k)$$

Step 4: User identity verified via additional factor (OTP/biometric).
Step 5: User resets password securely.
This ensures:

- No single authority can recover the secret
- Server compromise does not expose recovery mechanism

4. SECURITY ANALYSIS

A. Replay Attack Resistance

To ensure message freshness, the proposed framework uses nonces and timestamps in each [16]. Since these values change for every login attempt, previously intercepted messages cannot be reused. This prevents replay attacks effectively.

B. Brute-Force Resistance

Passwords are protected using salted hashing, which prevents dictionary and rainbow table attacks. The combination of limiting the number of login attempts along with multi-factor authentication can significantly reduce the possibility that a brute-force attack will be successful.

C. Impersonation Attack Resistance

The framework integrates multi-factor authentication and device-specific parameters during token generation [17]. An attacker cannot impersonate an authenticated legitimate user without having access to all of the relevant factors required to authenticate with the system.

D. Man-in-the-Middle Resistance

Mutually authenticated sessions are encrypted using session keys, which prevent an assailant from being able to verify or alter a message between the smartphone and the server [18]. Any modified or intercepted message fails verification, providing protection against MITM attacks.

E. Server Compromise Protection

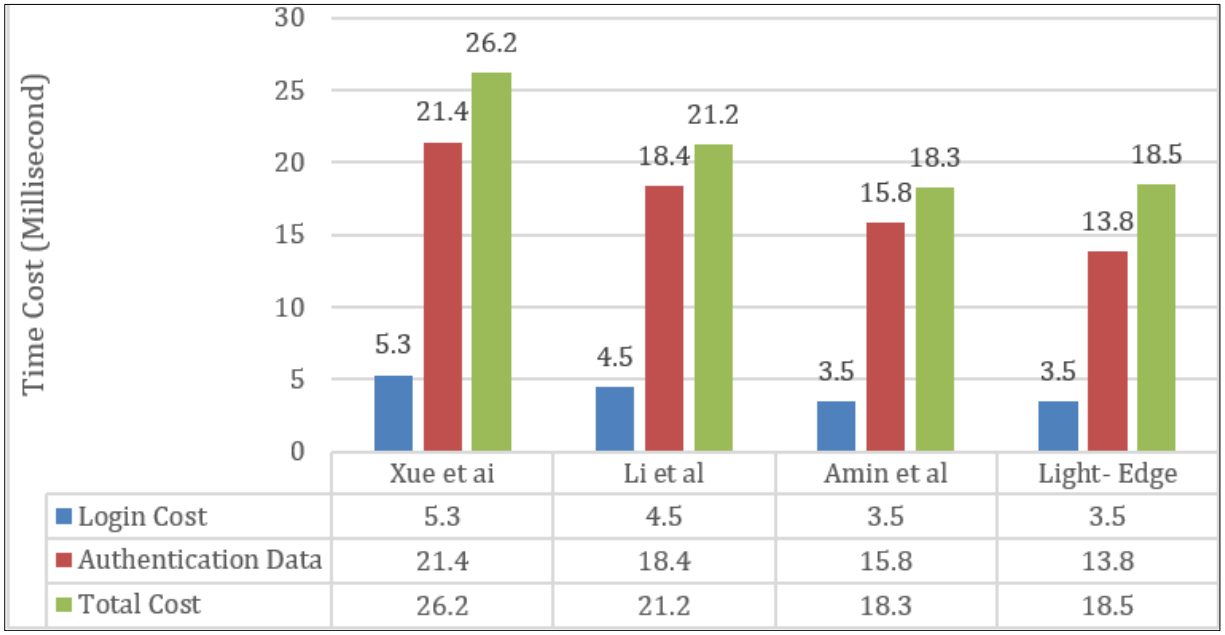
The use of threshold-based secret sharing to recover passwords allows compromised servers to provide no more than a partial password recovery secret. This sharing avoids any risk of a single point of failure, because the password recovery secrets are distributed among multiple trusted parties.

5. Performance Analysis

A. Computational Cost

The amount of processing effort required to execute security-related operations represents the computational cost of an authentication framework. In the proposed framework, the primary computing operations consist of XOR operations, hash

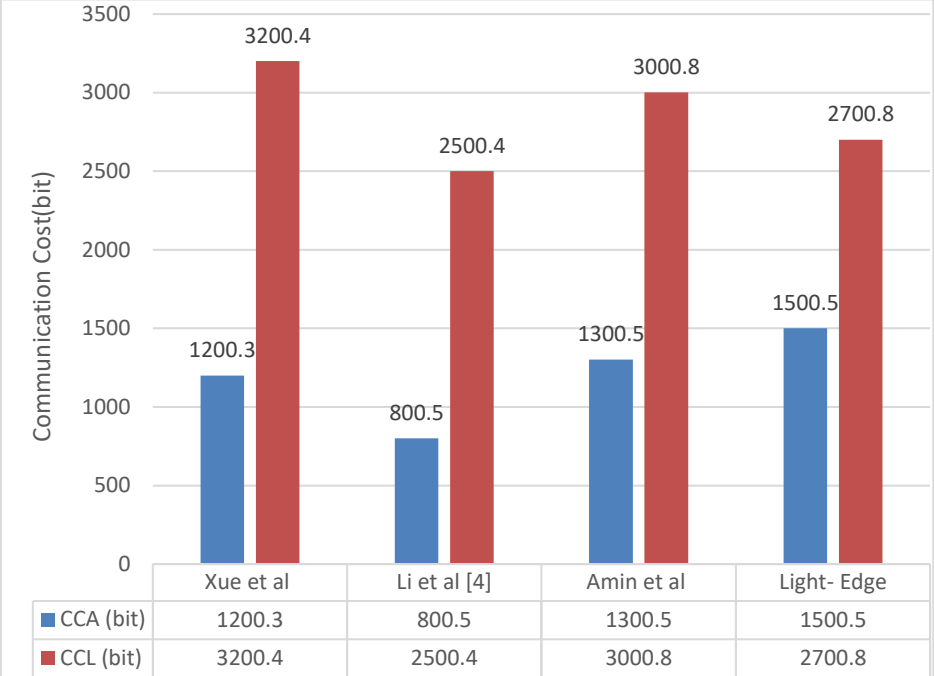
computations, and symmetric encryption. Hash functions are used to transform sensitive inputs like identity parameters and passwords into fixed-length outputs. These operations are computationally efficient and mathematically secured. Modern hash algorithms are designed to execute quickly even on low-power devices. This characteristic makes them suitable for mobile phones and IoT systems. XOR (Exclusive OR) operations are lightweight bitwise computations that require minimal processing overhead [19,20]. They are simple enough to be performed almost instantaneously, which reduces the overall computational burden of the authentication process. To ensure secure communication symmetric encryption is used. between the user and the server. Symmetric encryption techniques require lower computational resources and are faster in the process of both encryption and decryption than asymmetric cryptographic techniques [21]. The encryption and decryption process are faster and more efficient because both parties share a secret key. Because the proposed framework is mainly based on lightweight cryptographic operations, it attains reduced processing delay, low energy consumption, and efficient authentication performance [22]. Therefore, the framework is compatible for resource-constrained environments, including IoT devices, smartphones and embedded systems.



B. Communication Cost

Communication cost represents the amount of exchanged data among the user and the server all along the authentication process. The communication procedure is very simple and efficient in the proposed framework. The authentication phase needs only a single login request from the user followed by a response from the server [23,24]. This type of two-message interaction significantly minimizes the network traffic and communication latency. Moreover, recovery-related communication such as account recovery procedures or password reset, is performed only when necessary and does not impose continuous overhead on the system. The protocol does not require multiple rounds of message transmission and also does not rely on the exchange of large cryptographic parameters. As a result, the overall communication overhead remains relatively low, which makes the system relevant to bandwidth-constrained environments such as mobile networks and IoT-based applications [25].

Finally, both computational and communication costs of the proposed framework are effectively optimized. The system achieves efficient performance, scalability, and practical applicability in real-world deployment scenarios due to the combination of lightweight cryptographic operations with minimal message exchange.



6. FUTURE DIRECTIONS

A. Integration with biometric authentication

The integration of biometric authentication factors such as fingerprints, facial recognition, or iris scanning into password-based systems will strengthen the security of the system. In this an additional layer of identity verification is added, which makes unauthorised access more difficult while providing users with continued convenience.

B. Blockchain-based decentralized recovery

The use of blockchain to recover passwords can decentralise the control of password recovery and allow the distribution of password recovery data among multiple trusted nodes [27]. This elevates transparency, avoids single points of failure, and enhances resistance against server compromise.

C. post-quantum lightweight cryptography

The threat posed by quantum computers in the future may make traditional cryptographic algorithms insecure [28]. Post-quantum lightweight cryptography ensures security against quantum attacks while remaining efficient enough for smartphones and IoT devices.

D. AI-based anomaly detection for authentication

Artificial Intelligence can analyze user behaviour patterns such as typing speed, login time, or location [29]. If an anomaly is detected by analysing user behaviour patterns, an additional verification step can be triggered in order to provide stronger protection against impersonation and fraud.

E. Secure implementation in 5G/6G mobile ecosystems

As 5G and future 6G networks enable faster and more connected environments, authentication systems must be optimized for these networks. Secure implementation of authentication systems within mobile ecosystem will allow for rapid communication with strong encryption and increased security across multiple devices and connected networks.

7. CONCLUSION

This study proposed a secure and efficient cryptography-based framework for smartphone authentication and password recovery. By combining multi-factor authentication, lightweight cryptographic techniques, and secret sharing–based recovery, the system eliminates single points of failure and strengthens overall security.

The framework maintains low computational and communication overhead, making it suitable for mobile devices while effectively resisting replay, impersonation, brute-force, and man-in-the-middle attacks. Overall, it provides a reliable and practical solution for next-generation mobile authentication systems.

REFERENCES

1. Shariq M, Jamil N, Rawat GS, Chaudhry SA, Masud M, Cangelosi A. An anonymous and privacy-preserving lightweight authentication protocol for secure communication in UAV-assisted IoAV networks. Comput Commun. 2025. doi: 10.1016/j.comcom.2025.108192.
2. Shariq M, Conti M, Singh K, Lal C, Das AK, Chaudhry SA, et al. Anonymous and reliable ultralightweight RFID-enabled authentication scheme for IoT systems in cloud computing. Comput Netw. 2024. doi: 10.1016/j.comnet.2024.110678.
3. Javadi A, Sadeghi S, Pahlevani P, Bagheri N, Rostampour S, Bendavid Y. Secure and efficient lightweight authentication protocol (SELAP) for multi-sector IoT applications. Internet Things. 2025. doi: 10.1016/j.iot.2025.101499.

4. Barati A, Movaghar A, Sabaei M. RDTP: Reliable data transport protocol for wireless sensor networks. Telecommun Syst. 2016; 62:611-623.
5. Zaslavsky A, Perera C, Georgakopoulos D. Sensing as a service and big data. arXiv. 2013; arXiv:1301.0159.
6. Kassab W, Darabkh KA. A-Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. J Netw Comput Appl. 2020; 163:102663.
7. Al-Emran M, Malik SI, Al-Kabi MN. A survey of Internet of Things (IoT) in education: Opportunities and challenges. In: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. Cham: Springer; 2020. p. 197-209.
8. Chaudhry SA, Farash MS, Kumar N, Alsharif MH. PFLUA-DIoT: A pairing-free, lightweight, and unlinkable user access control scheme for distributed IoT environments. IEEE Syst J. 2022;16(1):309-316.
9. Jia X, Feng Q, Ma C. An efficient anti-collision protocol for RFID tag identification. IEEE Commun Lett. 2010;14(11):1014-1016.
10. Jia X, Feng Q, Fan T, Lei Q. RFID technology and its applications in Internet of Things (IoT). In: Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet). Piscataway (NJ): IEEE; 2012. p. 1282-1285.
11. Pakniat N, Eslami Z. Cryptanalysis and improvement of a group RFID authentication protocol. Wireless Netw. 2020;26(5):3363-3372.
12. Vasudev H, Shariq M, Dwivedi SK, Conti M. LightKey: Lightweight and secure key agreement protocol for effective communication in Internet of Vehicles. In: Proceedings of the 25th International Conference on Distributed Computing and Networking. 2024. p. 209-216.
13. Shariq M, Singh K, Maurya PK, Ahmadian A, Taniar D. AnonSURP: An anonymous and secure ultralightweight RFID protocol for deployment in Internet of Vehicles systems. J Supercomput. 2022; 78:1-26.
14. Hui Y, Huang Y, Su Z, Luan TH, Cheng N, Xiao X, et al. BCC: Blockchain-based collaborative crowdsensing in autonomous vehicular networks. IEEE Internet Things J. 2022;9(6):4518-4532.
15. Martínez-Díaz M, Soriguera F. Autonomous vehicles: Theoretical and practical challenges. Transp Res Procedia. 2018; 33:275-282.
16. Anderson JM, Kalra N, Stanley KD, Sorensen P, Samaras C, Oluwatola OA. Autonomous Vehicle Technology: A Guide for Policymakers. Santa Monica (CA): RAND Corporation; 2014.
17. Xing R, Su Z, Xu Q, Benslimane A. Truck platooning aided secure publish/subscribe system based on smart contract in autonomous vehicular networks. IEEE Trans Veh Technol. 2021;70(1):782-794.
18. IoT Analytics. 5 things to know about IoT protocols [Internet]. Available from: https://iot-analytics.com/iot-protocols/
19. Pourrahmani H, Yavarinasab A, Monazzah AMH, Van Herle J. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the blockchain. Internet Things. 2023; 23:100888.
20. Williams P, Dutta IK, Daoud H, Bayoumi M. A survey on security in Internet of Things with a focus on the impact of emerging technologies. Internet Things. 2022; 19:100564.
21. Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. J Netw Comput Appl. 2023; 209:103540.
22. Mishra N, Islam SH, Zeadally S. A survey on security and cryptographic perspectives of Industrial Internet of Things. Internet Things. 2024; 25:101037.
23. Hernandez-Jaimes ML, Martinez-Cruz A, Ramírez-Gutiérrez KA, Feregrino Uribe C. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet Things. 2023;23:100887.
24. Gupta R, Saxena D, Gupta I, Singh AK. Differential and tri-phase adaptive learning-based privacy-preserving model for medical data in a cloud environment. IEEE Netw Lett. 2022;4(4):217-221.
25. Panahi Rizi MH, Hosseini Seno SA. A systematic review of technologies and solutions to improve the security and privacy protection of citizens in the smart city. Internet Things. 2022; 20:100584.
26. Chamola V, Hassija V, Gupta V, Guizani M. A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access. 2020; 8:90225-90265.
27. Singh M, Aujla GS, Bali RS. A deep learning-based blockchain mechanism for a secure Internet of Drones environment. IEEE Trans Intell Transp Syst. 2021;22(7):4404-4413.
28. Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M. Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of Drones environment. IEEE Trans Veh Technol. 2020;69(8):9097-9111.
29. Valavanis KP, Vachtsevanos GJ. Handbook of Unmanned Aerial Vehicles. New York: Springer; 2014.
30. Li B, Fei Z, Zhang Y. UAV communications for 5G and beyond: Recent advances and future trends. IEEE Internet Things J. 2019;6(2):2241-2263.