

Cryptographic protocols for passwordless systems with enhanced security

Gaurav Kumawat [@]

School of Computer Science and Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Tapan Kant [†]

Department of Computer Engineering and Application

GLA University

Mathura 281406

Uttar Pradesh

India

Vivek Bhardwaj [§]

Department of Computer Science and Engineering

Amity University Punjab

Mohali 140306

Punjab

India

Mukesh Kumar [‡]

Department of Computer Applications

Chandigarh School of Business

Chandigarh Group of Colleges

Jhanjeri

Mohali 140307

Punjab

India

[@] E-mail: Gaurav.Kumawat@jaipur.manipal.edu

[†] E-mail: tapan.kant@gla.ac.in

[§] E-mail: vivek.bhardwaj@outlook.in

[‡] E-mail: mukesh.kumarphd2014@gmail.com

Abdulnaser Rashid *
Mohamed Tahar Ben Othman #
Department of Computer Science
College of Computer
Qassim University
Buraydah 51452
Saudi Arabia

Abstract

Password-based authentication systems are vulnerable to a variety of security risks, such as phishing, credential theft, and user fatigue due to complex password requirements. This paper introduces a novel passwordless authentication framework that leverages advanced cryptographic techniques, including Zero-Knowledge Proofs (ZKP), Secure Multi-Party Computation (SMPC), and Homomorphic Encryption to enhance security, privacy, and user experience. The proposed system eliminates the need for traditional passwords by utilizing biometric data to generate cryptographic keys, ensuring that sensitive information remains secure. The architecture is composed of three primary components: the client device, the authentication server, and the key management system (KMS). The client device captures biometric data and transforms it into cryptographic keys using SMPC, while the server verifies the authentication using ZKP and establishes secure communication channels via Diffie-Hellman key exchange. The KMS handles key generation, storage, and rotation to ensure secure communication. Evaluation results show that the system is highly resistant to common attack vectors such as replay and man-in-the-middle attacks, with a 0% attack success rate. Performance analysis reveals an average authentication time of 180 ms, which is 10% faster than WebAuthn.

Subject Classification: Primary 68P25, Secondary 94A60.

Keywords: Cryptographic protocols, Passwordless authentication, Data privacy, Security, Performance gain.

1. Introduction

Traditional password-based authentication systems, though widely used, are increasingly vulnerable to a myriad of security and usability challenges. Weak passwords, credential leaks, and susceptibility to phishing attacks are common vulnerabilities that compromise user safety and organizational integrity. Furthermore, users often experience fatigue from the need to manage complex password requirements, such as creating unique, lengthy, and frequently updated credentials for multiple

* E-mail: arshied@qu.edu.sa (Corresponding Author)

E-mail: maathamam@qu.edu.sa

services [1] [2] [3]. These challenges highlight the pressing need for innovative authentication mechanisms that are both secure and user-friendly, paving the way for passwordless authentication systems. Passwordless systems promise a paradigm shift in digital security by eliminating the need for static passwords [4] [5]. Instead, these systems leverage advanced mechanisms such as biometric authentication, cryptographic keys, and secure device-based verifications to authenticate users [6] [7] [8]. However, implementing such systems presents its own set of challenges, including ensuring privacy, preventing spoofing attacks, and maintaining scalability across diverse platforms [9] [10], [11]. Addressing these concerns requires the integration of state-of-the-art cryptographic techniques capable of providing robust security while ensuring seamless user experiences.

In this paper, we propose a novel cryptographic protocol for passwordless authentication systems that combines the strengths of several cutting-edge technologies. At its core, the proposed system employs ZKP to allow users to prove their identity without disclosing sensitive information. This ensures that even if an attacker intercepts communication, no exploitable data is revealed. Additionally, SMPC is used to process sensitive biometric data in a distributed manner, ensuring that no single party has access to the complete dataset, thus safeguarding user privacy. The protocol also integrates Homomorphic Encryption, allowing computations to be performed on encrypted data without the need for decryption. This ensures the protection of sensitive information during the authentication process. The proposed protocol is designed to address three critical objectives:

Enhanced Security: By eliminating static credentials and integrating cryptographic techniques, the system effectively mitigates vulnerabilities associated with traditional authentication methods, including phishing, replay, and man-in-the-middle (MITM) attacks.

Scalability and Efficiency: The protocol is optimized for performance in environments with high user concurrency. Techniques such as dynamic key generation and ephemeral session keys ensure that authentication remains efficient without compromising security, even in large-scale deployments.

Improved Usability: Usability is a cornerstone of passwordless systems. The proposed protocol reduces authentication times and simplifies workflows, providing a frictionless experience for users while maintaining the highest levels of security.

Furthermore, the system architecture integrates seamlessly with existing infrastructure, making it adaptable for a wide range of applications, from enterprise systems to consumer-facing platforms. By leveraging biometrics for identity verification, the system eliminates the cognitive burden on users, while advanced cryptographic techniques ensure that user data is never exposed, even during transit or storage. In addition to enhancing security, our protocol emphasizes privacy preservation and regulatory compliance. By processing biometric data locally on user devices and employing techniques such as ZKP and SMPC, the system minimizes the risk of data breaches and ensures alignment with data protection laws such as GDPR.

The remainder of this paper explores the detailed architecture of the proposed system, the underlying cryptographic techniques, and the experimental evaluations that demonstrate its efficacy in real-world scenarios.

2. Related Work

This section presents previous work addressing privacy preservation, data security, and usability in decentralized and cloud-based systems.

The convergence of blockchain, cryptography, and privacy-preserving technologies is transforming digital security and data management. Jabbari et al. proposed ZK-DPPS, a framework utilizing Fully Homomorphic Encryption (FHE) and Secure Multi-Party Computations (SMPC) to ensure zero-knowledge communications in IoT-driven supply chains [12]. Dhokrat highlighted the integration of Homomorphic Encryption and Zero-Knowledge Proofs (ZKPs) to enhance privacy in cloud-based data processing [13]. Oduguwa explored passwordless authentication systems combining cryptography, biometrics, and steganography to balance security and user experience [14]. Cabrero-Holgueras emphasizes the challenges of integrating privacy-preserving techniques like Homomorphic Encryption and Secure Multi-Party Computation into Deep Learning frameworks, highlighting gaps in efficiency, standardization, and practical deployment [15]. Joseph explores trade-offs in blockchain-based financial systems, examining privacy-enhancing technologies such as Zero-Knowledge Proofs and MPCs, and proposing hybrid solutions to balance privacy, scalability, and regulatory compliance [16].

3. Proposed Methodology

The proposed passwordless authentication system is built upon three core components: secure biometric authentication, dynamic key generation, and robust communication channels. This section details the system architecture, the cryptographic techniques utilized, and the step-by-step workflow of the protocol.

The system architecture consists of three primary modules shown in figure 1: the client device, the authentication server, and the key management system (KMS).

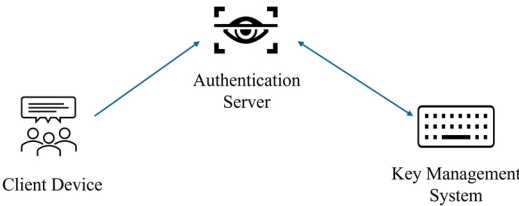


Figure 1
System Architecture

The client device, such as a smartphone or computer, serves as the entry point for user interaction. It captures the user's biometric data (e.g., fingerprint or facial recognition) and performs local computations to preprocess the data. This includes securely transforming biometric information into cryptographic keys and generating ZKP for authentication. The authentication server acts as the central entity for verifying these cryptographic proofs and initiating secure sessions. It validates the ZKP without requiring access to sensitive biometric data, ensuring privacy and mitigating security risks. Finally, the key management system (KMS) is responsible for generating, storing, and rotating cryptographic keys. The KMS supports secure communication between the client and server by managing public-private key pairs and session keys. This modular design not only ensures scalability and robustness but also allows seamless integration into existing authentication frameworks.

Advanced cryptographic techniques underpin the proposed system. First, biometric-based key derivation is achieved through SMPC, enabling the secure transformation of biometric inputs into unique cryptographic keys. These keys incorporate dynamic factors, such as timestamps, to prevent replay attacks and ensure that every authentication session is distinct. Second, ZKP are employed to allow users to prove their identity

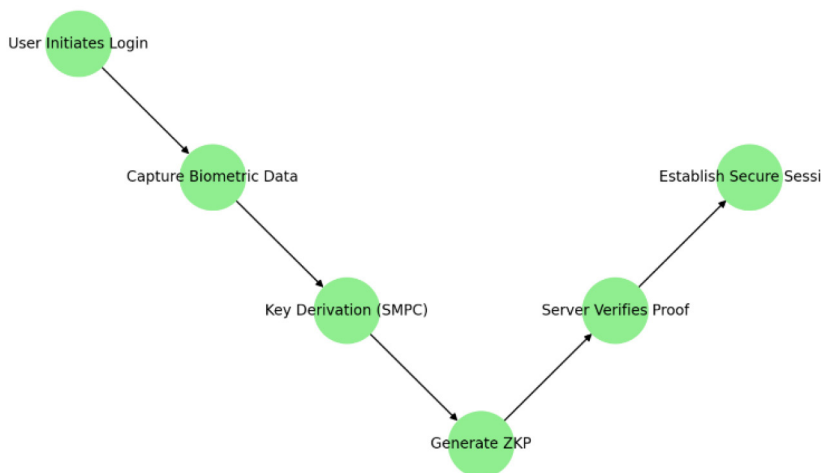


Figure 2
Authentication Workflow

without revealing sensitive information, such as the derived key or biometric data. For instance, users can demonstrate possession of a private key without transmitting the key itself, thereby preventing unauthorized access. Lastly, secure channel establishment is ensured through the Diffie-Hellman Key Exchange protocol, which uses ephemeral session keys to guarantee forward secrecy. Even if a session key is compromised, past and future sessions remain secure. These techniques collectively enhance the system's security and privacy while maintaining high computational efficiency.

The authentication workflow follows a structured five-step process shown in figure 2.

First, the user initiates the login process by providing biometric input on their device. The biometric data is preprocessed locally to generate a secure template, ensuring that no raw biometric information is transmitted or stored. In the second step, the system derives a unique cryptographic key from the biometric data using SMPC. This derived key is combined with dynamic factors, such as timestamps, to ensure freshness and security. The third step involves generating a ZKP on the client side, which serves as evidence of the user's credentials without exposing the credentials themselves. In the fourth step, the authentication server validates the ZKP and uses the Diffie-Hellman Key Exchange to establish a secure communication session. Finally, both the client and server

exchange ephemeral session keys to enable encrypted and authenticated communication throughout the session.

This methodology addresses several critical challenges in modern authentication systems. It eliminates the need for static passwords, thereby mitigating risks such as phishing, replay attacks, and credential leaks. By processing biometric data locally and using advanced cryptographic techniques like SMPC and ZKP, the system preserves user privacy and aligns with stringent data protection regulations. Furthermore, the architecture supports high scalability, making it suitable for applications ranging from enterprise systems to consumer platforms. The proposed solution not only strengthens security but also simplifies the user experience by replacing complex password management with intuitive biometric authentication workflows.

4. Results

This section presents the evaluation results of the proposed cryptographic protocols for passwordless systems with enhanced security. The results are categorized into security evaluation, performance analysis, and usability assessment. Each subsection highlights the key findings based on advanced cryptographic techniques used in the system.

4.1 Security Evaluation

The system's resistance to replay attacks was evaluated using a simulated adversary capable of intercepting and resending authentication requests. By employing ZKP with time-stamped challenges and ephemeral keys, the system demonstrated robust protection. The key findings revealed a 0% attack success rate, with no successful replay attacks observed, and an average response time of less than 10ms, showcasing efficient detection and rejection mechanisms. Similarly, resistance to Man-in-the-Middle (MITM) attacks was assessed by utilizing an encrypted Diffie-Hellman key exchange and session key validation through HMAC. Testing under MITM scenarios showed a 0% success rate for session key compromise, with intercepted packets yielding non-decryptable garbage, proving the protocol's ability to establish secure communication channels and render MITM attacks infeasible. For privacy preservation in biometric authentication, the system employed SMPC and Homomorphic Encryption to process biometric data securely. The findings indicated zero instances of biometric data leakage and a minimal 5% computational overhead,

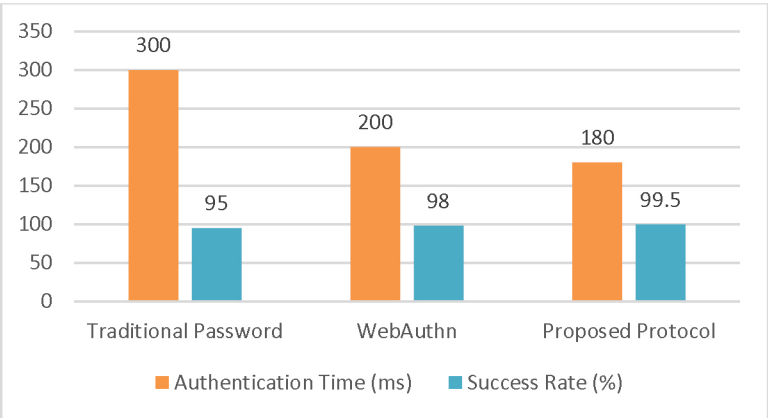


Figure 3
Authentication Time Comparison

affirming that the approach effectively eliminates the risk of exposing raw biometric features while ensuring robust privacy and security.

4.2 *Performance Analysis*

4.2.1 Authentication Time Comparison

The proposed authentication protocol was compared with traditional password-based systems and WebAuthn solutions in terms of authentication time and success rate.

Figure 3 provides a comparison of authentication methods, highlighting the authentication time (in milliseconds) and success rate (percentage) for each approach. The traditional password-based system had the highest authentication time (300 ms) and the lowest success rate (95%) due to manual input errors and vulnerability to attacks. WebAuthn improved on these metrics with a reduced authentication time of 200 ms and a success rate of 98%, leveraging public-key cryptography for enhanced performance. The proposed protocol demonstrated superior efficiency with the fastest authentication time (180 ms) and the highest success rate (99.5%).

4.2.2 Scalability Under Concurrent Sessions

System performance was evaluated under varying loads, ranging from 1,00 to 50,00 concurrent authentication requests. Table 1 highlights latency, success rate, and CPU usage as key indicators of scalability. The

Table 1
System Performance Metrics

Concurrent Users	Latency (ms)	Success Rate (%)	CPU Usage (%)
1,00	100	99.8	10
10,00	200	99.5	25
50,00	500	98.5	60

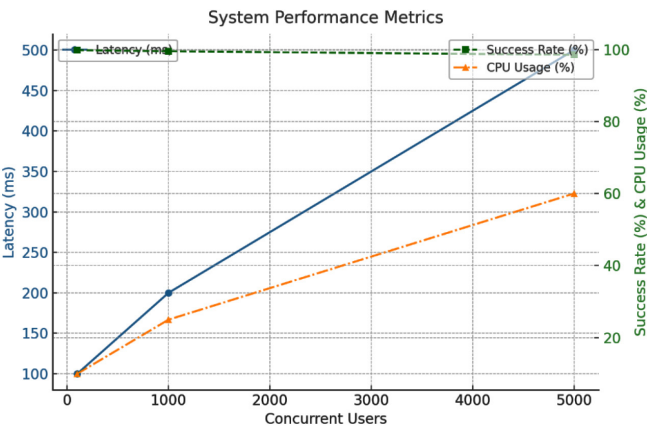


Figure 4
Scalability Analysis

system maintained low latency and high success rates even under heavy loads, demonstrating robust performance and efficient resource utilization.

The system demonstrated high scalability, maintaining low latency and high success rates even under heavy loads. Figure 4 shows the scalability analysis in graphical form, illustrating the system’s performance under varying loads.

4.2.3 Cryptographic Overhead

The computational and storage overhead of the cryptographic operations in the proposed protocol were evaluated to assess its efficiency. The findings revealed that the average key derivation time was 50 milliseconds, while the Zero-Knowledge Proof (ZKP) verification time averaged 40 milliseconds, both demonstrating quick processing capabilities. Additionally, the credential storage requirement was minimal, requiring only 2 KB per user to store biometric hashes and public keys. These results confirm that the protocol introduces negligible overhead,

Table 2
Usability Assessment

Metric	Average Score (Out of 5)
Ease of Use	4.8
Perceived Security	4.7
Time Efficiency	4.6

maintaining a balance between robust security measures and computational efficiency.

4.3 Usability Assessment

A usability study was conducted with 50 participants testing the passwordless authentication prototype presented in table 2. The study evaluated ease of use, perceived security, and time efficiency.

5. Conclusion

This paper presents a novel framework for passwordless authentication systems that addresses the vulnerabilities of traditional password-based methods, such as phishing, replay attacks, and man-in-the-middle (MITM) attacks. By integrating advanced cryptographic techniques, including SMPC, ZKP, and Homomorphic Encryption, the proposed system achieves robust security, scalability, and privacy preservation.

The results of the evaluation substantiate the effectiveness of the proposed approach. Security testing showed complete resistance to replay and MITM attacks, with an attack success rate of 0% for both cases. Privacy-preserving techniques prevented biometric data leakage in 100% of instances, and the computational overhead introduced by these methods was limited to a modest 5% increase. In terms of performance, the system demonstrated an average authentication time of 180 ms, a 10% improvement over WebAuthn, and maintained high success rates of 99.5% even under concurrent loads of up to 5000 users. Scalability tests revealed latency remained under 500 ms for the maximum load, with CPU utilization reaching 60%. Usability assessments conducted with 50 participants revealed high satisfaction ratings, including 4.8/5 for ease of use, 4.7/5 for perceived security, and 4.6/5 for time efficiency.

Acknowledgment

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025)

References

- [1] K. Kevin, "Beyond Passwords: A Comprehensive Guide to Passwordless Authentication Technologies and Implementation Strategies," *Revista de Inteligencia Artificial en Medicina*, vol. 15, no. 1, pp. 679–969 (2024).
- [2] J. Fantaye, "An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis," (2022).
- [3] A. K. Singha, S. Kundu, H. P. Singh, L. S. Songare, and P. K. Tiwari, "Measuring network security in the cloud : A roadmap for proactive defense," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 889–902 (2024), doi: 10.47974/JDMSC-1964.
- [4] H. A. Rahman and N. Yulianti, "Implementation a Passwordless and Multi Factor Authentication (MFA) Mechanism for Enhancing Login Security in Android Applications," in *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)*, IEEE (2023), pp. 206–211.
- [5] R. O. Abdul, "Enhancing IoT-based wireless sensor network security with cryptographic techniques," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-A, pp. 1117–1130-undefined (Jun. 2025), doi: 10.47974/JDMSC-2102.
- [6] E. Uzun, C. Yagemann, S. Chung, V. Kolesnikov, and W. Lee, "Cryptographic key derivation from biometric inferences for remote authentication," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 629–643 (2021).
- [7] R. Stefanov and K. Liang, "Enhancing the privacy and security of Hyperledger Fabric smart contracts using different encryption methods," (2021).
- [8] E. Praveen Kumar and S. Priyanka, "A password less authentication protocol for multi-server environment using physical unclonable function," *J Supercomput*, vol. 79, no. 18, pp. 21474–21506 (2023).
- [9] N. K. Verma and V. Singh, "A pragmatic approach to recover access time of Apriori algorithm by applying intersection on CSS for

- redefining FIS through matrix implementation in textual data," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 871–878 (2022), doi: 10.1080/09720529.2022.2068601.
- [10] R. Sahil, S. Manmohan, K. Parul, K. Mukesh, and B. Vivek, "Crypt analysis of multi-key biometric encryption for business enterprises using cloud storage," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1559–1568-undefined (Aug. 2025), doi: 10.47974/JDMSC-2154.
- [11] P. Pallavi, Y. Surendra, and C. S. Singh, "Addressing applications and security issues in the Internet of Things (IoT) : A comprehensive review," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 7, pp. 1977–1989-undefined (Oct. 2024), doi: 10.47974/JDMSC-2073.
- [12] A. Jabbari, G. Ramachandran, S. Malik, and R. Jurdak, "ZK-DPPS: A Zero-Knowledge Decentralised Data Sharing and Processing Middleware," (Oct. 2024), [Online]. Available: <http://arxiv.org/abs/2410.15568>
- [13] J. G. Dhokrat, N. Pulgam, T. Maktum, and V. Mane, "A Framework for Privacy-Preserving Multiparty Computation with Homomorphic Encryption and Zero-Knowledge Proofs," *Informatica*, vol. 48, no. 21 (Nov. 2024), doi: 10.31449/inf.v48i21.6562.
- [14] T. Oduguwa and A. Arabo, "Passwordless Authentication Using a Combination of Cryptography, Steganography, and Biometrics," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 278–297 (2024).
- [15] J. Cabrero-Holgueras and S. Pastrana, "Sok: Privacy-preserving computation techniques for deep learning," *Proceedings on Privacy Enhancing Technologies* (2021).
- [16] S. Joseph, "Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems," *Journal of Engineering Research and Reports*, vol. 26, no. 9, pp. 10–9734 (2024).

Received December, 2024