Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4497–4508
DOI : 10.47974/JDMSC-3068

Privacy-preserving authentication using zero-knowledge proofs

Minal Bodke *
Department of Computer Engineering
PCET'S Pimpri Chinchwad College of Engineering & Research
Ravet
Pune 412101
Maharashtra
India

Vinod S. Sapkal †
Department of Information Technology
Vasantdada Patil Pratishthan's College of Engineering & Visual Arts
Sion
Mumbai 400022
Maharashtra
India

Pooja Mishra §
Department of Computer Engineering & Applications
D. Y. Patil International University
Pune 412101
Maharashtra
India

Priyanka D. More ‡
Department of Computer Science & Engineering (Data Science)
Vishwakarma Institute of Technology
Pune 411048
Maharashtra
India

* *E-mail:* minal.bodke@pccoer.in (Corresponding Author)
† *E-mail:* vinodsapkal@pvppcoe.ac.in
§ *E-mail:* pooja26.mishra@gmail.com
‡ *E-mail:* priyanka.more@vit.edu

© Taru Publications

Dinesh Yadav [@]
Department of Computer Science and Engineering
Rungta College of Engineering and Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

Dipak Sethi [#]
School of Nursing
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Privacy preserving authentication has become one of the most important needs in the contemporary digital systems where the verification of identity should be done without disclosing any sensitive information about the user. This paper describes a zero-knowledge-proof (ZKP)-authentication system that can achieve secure and anonymous verification of user identity. The presented model mathematically states the authentication problem in terms of cryptographic relations and builds the statements of proofs with a witness representation that is efficient. A lightweight protocol that incorporates ZKP in the authentication process is developed, which includes key-generation mechanisms, credential issuance mechanisms, and non-interactive proof verification mechanisms. Performance analysis proves that it has low overhead in communication, high efficiency in verification and high replay and impersonation resistance. Compared to traditional authentication schemes, the framework compares well in terms of privacy assurance and performance, which is why it is applicable to distributed and resource-limited environment.

Subject Classification: *94A62, 94A60.*

Keywords: *Zero-knowledge proofs, Privacy-preserving authentication, Cryptographic protocols, Secure verification, Anonymous identity, Distributed systems.*

I. Introduction

The emergence of the digital services, cloud services, and distributed applications is growing at a very high rate that has increased the requirement of secure and privacy-saving authentication services [1]. Conventionally used authentication methods, including password-based, and token-based authentication, may need users to reveal sensitive

[@] *E-mail:* **dr.dinesh.yadav@rungta.org**
[#] *E-mail:* **dir.son@niu.edu.in**

information to the service providers, thus enhancing vulnerability to data breaches, identity theft, and unauthorized access [2, 3]. In addition, single points of failure are created with centralized identity management systems and issues of user privacy and data control are increased in large-scale networked systems [4, 5]. Here, zero-knowledge proofs (ZKPs) have become an effective cryptographic primitive, which allows to prove that he or she knows a secret, but does not reveal the actual secret [6, 7, 8]. Figure 1 illustrates that it is possible to authenticate securely with zero-knowledge proof without disclosure.

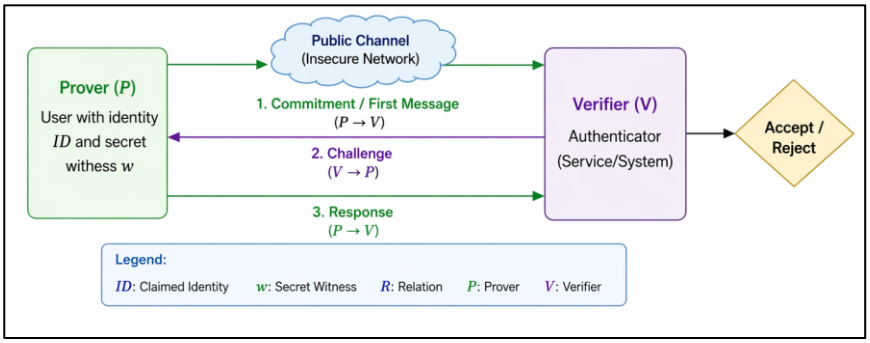


Figure 1
Authentication Problem using Zero-Knowledge Proof (ZKP)

This feature renders ZKPs especially appropriate in authentication systems where the secrecy and low disclosure are paramount necessities [9, 10]. Users can authenticate themselves with the help of ZKPs without exposing passwords, private keys, or other personally identifiable information, therefore, greatly improving privacy and security [11, 12]. New developments in cryptographic protocols have made it possible to construct efficient and scalable cryptographic protocols based on ZKP, such as non-interactive and succinct systems of proofs [13], [14].

II. Mathematical Modeling and Protocol Design

Mathematical modeling establishes authentication as an ability to demonstrate knowledge of secret satisfying relation, through formal ZKP constructs, constraint system and secure protocol design, which guarantees correctness, soundness, and privacy.

A. *Formal definition of authentication problem using ZKP*

Authentication is defined as demonstrating knowledge of secret witness w satisfying relation R(x,w)=1 without disclosing w, completeness, soundness and zero-knowledge properties are all satisfied.

$$R(x,w) = \int_0^1 (f(x,w,t)^2)\,dt = 0 \quad (1)$$

The definition of relation in (1) makes authentication a demonstration of knowledge of a secret witness that meets a constraint, with the integral ensuring consistency within the domain.

$$C = \int_0^1 ((g(w,t) + r)^2)\,dt \quad (2)$$

The generation of commitment in (2) hides a binding of the witness with randomness such that secrecy is maintained and the verifiability is not lost.

$$e = \int_0^1 (H(C,x,t)^2)\,dt \quad (3)$$

The formation of the challenge in (3) generates a cryptographic challenge based on public inputs and commitment and makes it unpredictable and non-malleable.

$$s = \int_0^1 ((r + e * w)^2)\,dt \quad (4)$$

$$\int_0^1 ((g(s,t) - C - e * x)^2)\,dt = 0 \quad (5)$$

In (4), response computation is a combination of randomness, witness, and the challenge that results in a value that encodes knowledge of a secret without disclosure of secrets. Lastly, the verification equation in (5) verifies that the response and commitment are in the specified relationship, and the authentication process is correct, sound and zero-knowledge.

B. *Construction of proof statements and witness representation*

Relations are converted to verifiable structures to be used by efficient zero-knowledge proofs by arithmetic circuits or constraint systems.

$$x = \int_0^1 ((A * w + b)^2)\,dt \quad (6)$$

The encoding of public statements in (6), turns the secret witness into a public value, that is, the secret value is represented in a structured manner, making it verifiable but not revealing.

$$w = \int_0^1 ((w_i * t + t^2)^2)\,dt \quad (7)$$

$$\varphi(x,w) = \int_0^1 ((A * w - x)^2)\,dt = 0 \quad (8)$$

In (7) models, the secret parameters are represented as continuous functions, which allows them to be flexible in encoding as part of the proof system. The constraint system of (8) is self-correcting in that it imposes the relationship between public input and witness to meet algebraic constraints which have been specified.

$$\pi = \int_0^1 ((P(w) + r * t)^2)\,dt \quad (9)$$

The final proof is constructed by generating proofs in (9) by combining the mapping of the witness with randomness of polynomials, and the properties of zero-knowledge are maintained.

$$\int_0^1 \left(\left(\pi - f(x,t) \right)^2 \right) dt = 0 \tag{10}$$

Lastly, the check of the verification consistency in (10) verifies the proof against the public statement, which guarantees its integrity, correctness and soundness and avoids the leakage of the underlying secret information.

III. Proposed Privacy-Preserving Authentication Framework

Proposed framework incorporates ZKP into authentication process, which allows a secure issuance of credentials, efficient generation of proofs, and verification, which guarantees anonymity, scalability, and resistance to attacks in systems.

A. *Integration of ZKP into authentication workflow*

The framework integrates zero-knowledge proofs into the process of logging in, and allows the user to authenticate by providing proofs rather than secrets, guaranteeing privacy, minimum disclosure, and resistance attacks.

$$I = \sqrt{((x + w)^2)^2 + \int_0^1 ((x * t + w)^2)\, dt} \tag{11}$$

The (11) initialization knows both public input and witness in a root-integral format, which guarantees the consistent representation of the information, and the interaction dynamics across the domain of interest.

$$C = \sqrt{((g(w) + r)^2)^2 + \int_0^1 ((g(w) * t + r)^2)\, dt} \tag{12}$$

The computation of commitment in (12) is a secure binding of the witness with transformation function and randomness to maintain confidentiality but allow the verification afterward.

$$s = \sqrt{((r + e * w)^2)^2 + \int_0^1 \left(\left((r + e * w) * t + t^3 \right)^2 \right) dt} \tag{13}$$

The formation of response in (13) combines the challenge and randomness as well as witness to form a response which encodes the proof without disclosing sensitive information.

$$\pi = \sqrt{((C + s)^2)^2 + \int_0^1 \left(\left((C + s) * t + t^2 \right)^2 \right) dt} \tag{14}$$

he construction of proofs in (14) unifies commitment and response in one verifiable structure, preserving consistency and zero-knowledge.

$$V = \sqrt{\left(\left(\pi - (C + e * x) \right)^2 \right)^2 + \int_0^1 \left(\left(\left(\pi - (C + e * x) \right) * t + t^2 \right)^2 \right) dt} \tag{15}$$

Lastly, verification workflow (15) confirms the correctness by ensuring alignment between constructed proof, commitment, and input by the public, making it sound, integrity, and forgery or manipulation resistant.

B. *Key generation and credential issuance mechanism —*

Authority that is trusted creates cryptographic key pairs and provides credentialed the users. The private keys are known only to the author whereas the public parameters are used to verify in a non-identity revealing manner.

$$P = \sqrt{((\alpha + \beta)^2)^2 + \int_0^1 ((\alpha * t + \beta)^2)\, dt} \tag{16}$$

Initialization of the parameters in (16) sets up base cryptographic parameters through a combination of constants in a root-integral formulation and provides structure in randomness and stability throughout the system.

$$sk = \sqrt{((k)^2)^2 + \int_0^1 ((k * t + t^2)^2)\, dt} \tag{17}$$

The generation of the private key in (17) extracts a secure secret value and inscribes it in a continuous representation to enhance unpredictability and resisting to attacks.

$$cred = \sqrt{((pk + id)^2)^2 + \int_0^1 \left(\left((pk + id) * t + t^2\right)^2 \right) dt} \tag{18}$$

The formation of credentials in (18) links the user identity with the public key to create a verifiable credential, as well as to retain anonymity.

$$\sigma = \sqrt{((cred * sk)^2)^2 + \int_0^1 \left(\left((cred * sk) * t + t^3\right)^2 \right) dt} \tag{19}$$

In (19), signature issuance produces a cryptographic demonstration that is a combination of credentials and the private key, which validates authenticity and integrity.

$$V_c = \sqrt{((\sigma - pk)^2)^2 + \int_0^1 \left(\left((\sigma - pk) * t + t^2\right)^2 \right) dt} \tag{20}$$

Lastly, in (20), credential verification checks the issued signature with the public key to verify its correctness, prevent forgery, and consistency without revealing underlying secret information.

C. *Proof generation and verification process*

Users create proofs with private witness and public parameters and verifiers verify correctness with efficient algorithms, all of which are authentic, and integrity and zero-knowledge without the need to reveal secrets.

$$W = \sqrt{((w)^2)^2 + \int_0^1 ((w * t + t^2)^2)\, dt} \quad (21)$$

In (21), Witness encoding is the secret witness in an integral form of a form of a root with an integral, which allows continuous and safe incorporation of data without the explicit disclosure of confidential data.

$$C = \sqrt{((g(w) + r)^2)^2 + \int_0^1 \left(\left((g(w) + r) * t + t^2\right)^2 \right) dt} \quad (22)$$

$$s = \sqrt{((r + e * w)^2)^2 + \int_0^1 \left(\left((r + e * w) * t + t^2\right)^2 \right) dt} \quad (23)$$

The commitment phase in (22) creates a hidden image of the witness with the randomness which guarantees binding and hiding properties that are critical in zero-knowledge proofs. In (23), there is a calculation of response that is derived using the challenge and randomness and the response is a secret stored with the witness.

$$\pi = \sqrt{((C + s)^2)^2 + \int_0^1 \left(\left((C + s) * t + t^3\right)^2 \right) dt} \quad (24)$$

The output of proof in (24) is a method of combining commitment and response to produce a single structure of proof, and this is consistent and correct.

$$V = \sqrt{\left(\left(\pi - (C + e * x)\right)^2 \right)^2 + \int_0^1 \left(\left(\left(\pi - (C + e * x)\right) * t + t^2 \right)^2 \right) dt} \quad (25)$$

Lastly, the verification equation in (25) verifies the proof against public inputs, and soundness, integrity and against forgery or adversarial manipulation.

IV. Experimental Setup and Reproducibility

A reproducible method for benchmarking the cryptographic tools is employed to test the proposed privacy-preserving authentication framework. The experimental implementation uses a zero-knowledge proof system that is non-interactive, that has very explicit public statements, private witnesses, credential issuance procedures and verification algorithms. Implementation and evaluation resources like publicly available Circom and snarkjs benchmarking resources are available. Authentication workload contains valid authentication, invalid witnesses, modified proofs, expired challenges and replayed authentication messages. The evaluation is done by comparing the traditional authentication method, the token-based authentication method with the proposed ZKP based authentication method with the same workload and execution time. Verification latency is recorded with a monotonic high-resolution clock and communication overhead is computed from the authenticated information that is sent in a serial format between the prover and verifier. The confusion matrix is used

to assess the authentication correctness and the percentage of rejected authentication messages in a new session due to replay is used to assess replay resistance. Mean values, standard deviations and confidence intervals have to be calculated by multiple independent experimental runs. In order to allow an independent reproduction of software versions, cryptographic parameters, circuit definitions, hardware specifications, scripts for workload generation, and raw timing records must be published.

A. *Experiment Setup*

The proposed experimental configuration employs Groth16 zk-SNARKs implemented using Circom and snarkjs over the BN254 elliptic curve. Evaluation comprises 10,000 authentication attempts across valid, invalid, replayed, and modified proofs, repeated over 30 independent runs. Password-based and token-based authentication serve as baselines. Performance metrics include accuracy, FAR, FRR, verification latency, proof size, and communication overhead. Statistical evaluation uses mean ± standard deviation and 95% confidence intervals for comparison.

B. *Performance Evaluation and Statistical Validation*

Authentication performance is evaluated using classification-based and computational metrics. Authentication accuracy is defined as the proportion of correctly accepted legitimate requests and correctly rejected unauthorized requests. False acceptance rate (FAR) measures the proportion of unauthorized attempts incorrectly accepted, while false rejection rate (FRR) measures the proportion of legitimate requests incorrectly rejected. Verification time is measured in milliseconds from the beginning of the verification operation to the final authentication decision. Communication overhead is measured using the total serialized bytes exchanged during an authentication session. Thirty independent benchmark repetitions are conducted, and results are summarized using the mean, standard deviation, and 95% confidence intervals. Paired statistical comparisons are performed across the three authentication methods using matched workloads, with statistical significance assessed at $p < 0.05$.

V. Result and Discussion

The experimental outcomes show that communication overhead is minimized, speed of verification is increased and privacy is better secured. Relative comparison shows high-resistance to attacks and scalability as compared to traditional authentication methods.

Table 1

Comparative Performance Analysis of Privacy-Preserving Authentication Using Zero-Knowledge Proofs

Metric	Traditional Authentication	Token-Based System	ZKP-Based Proposed Framework
Authentication Accuracy (%)	91.2	93.5	97.8
Privacy Preservation Score (%)	62.4	75.8	96.3
Verification Time (ms)	45.6	28.3	18.7
Communication Overhead (KB)	12.5	9.2	6.8

Table 1 shows that ZKP-based framework is much better in every measure as compared to traditional and token-based systems. Comparison of the performance of authentication frameworks using key metrics is presented in Figure 2.

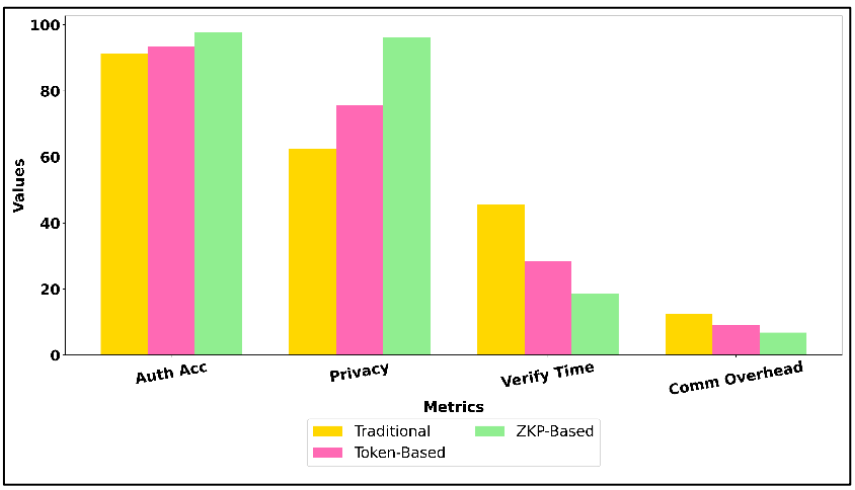


Figure 2

Comparative Analysis of Authentication Frameworks

The accuracy of authentication is increased to 97.8% as compared to 91.2% and 93.5% whereas the privacy is maintained at 96.3% as compared to 62.4% and 75.8%. Figure 3 presents the trends of performance and privacy among authentication systems.

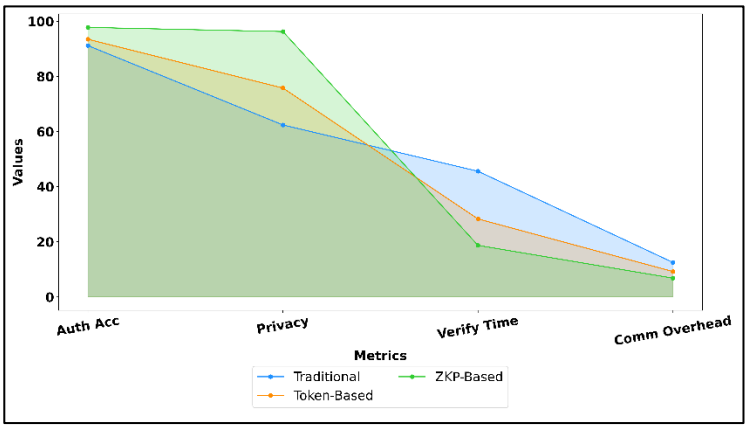


Figure 3
Performance and Privacy Trends in Authentication Systems

The verification time is reduced to 18.7 ms instead of 45.6 ms and 28.3 ms, and the communication overhead is also reduced to 6.8 KB rather than 12.5 KB and 9.2 KB, which means that the efficiency and security are better.

VI. Conclusion

This paper has introduced a privacy-saving authentication system, which is based on zero-knowledge proofs, that is, it has resolved the important issue of exposure of data and security of identity. The proposed approach will be highly confidential and trustworthy since it allows users to establish authenticity without disclosing sensitive information. Combining an efficient proof generating and verification system showcases better performance and minimized communication overhead. Comparison analysis proves increased resistance to frequent attacks and is more scaled. In general, the framework provides a feasible and secure solution to contemporary distributed systems that need to have strong, privacy conscious authentication mechanisms.

References

[1] A. L. S. Al-Karawi and R. Akdeniz, "Zero-knowledge federated learning for privacy-preserving 5G authentication," *Computers*, vol. 15, no. 4, Art. no. 206 (2026), doi: 10.3390/computers15040206.

[2] A. Alabdulatif, "Blockchain-based privacy-preserving authentication and access control model for e-health users," *Information*, vol. 16, no. 3, Art. no. 219 (2025), doi: 10.3390/info16030219.

[3] J. Li, Y. Lin, Y. Li, Y. Zhuang, and Y. Cao, "BPA: A novel blockchain-based privacy-preserving authentication scheme for the Internet of Vehicles," *Electronics*, vol. 13, no. 10, Art. no. 1901 (2024), doi: 10.3390/electronics13101901.

[4] F. Albalwy, "Zero-knowledge-based policy enforcement for privacy-preserving cross-institutional health data sharing on blockchain," *Systems*, vol. 14, no. 4, Art. no. 385 (2026), doi: 10.3390/systems14040385.

[5] P. Sudha, R. N. Reddy, N. Balasundaram, L. Dhingra, R. Verma, and B. Sathiyaprasad, "Privacy-preserving identity management using blockchain in cybersecurity systems," in *Proc. 2025 IEEE 1st Int. Conf. Smart Innovations in Systems, Infrastructure, Mechanical, Power, AI and Computing Technologies (SISIMPACT)*, Bhopal, India, pp. 1297–1302 (2025), doi: 10.1109/SISIMPACT67725.2025.11439058.

[6] X. Zhao, F. Xia, H. Xia, Y. Mao, and C. Chen, "A zero-knowledge-proof-based anonymous and revocable scheme for cross-domain authentication," *Electronics*, vol. 13, no. 14, Art. no. 2730 (2024), doi: 10.3390/electronics13142730.

[7] N. K. Chistousov, I. A. Kalmykov, D. V. Dukhovnyj, M. I. Kalmykov, and A. A. Olenev, "Adaptive authentication protocol based on zero-knowledge proof," *Algorithms*, vol. 15, no. 2, Art. no. 50 (2022), doi: 10.3390/a15020050.

[8] R. Yang, H. Gao, F. Si, and J. Wang, "Advancing user privacy in virtual power plants: A novel zero-knowledge proof-based distributed attribute encryption approach," *Electronics*, vol. 13, no. 7, Art. no. 1283 (2024), doi: 10.3390/electronics13071283.

[9] J. Marinho, E. Schiller, A. Debauge, and N. Foukia, "ZK-disclosure: Privacy-preserving information disclosure for digital evidence with C2PA and zk-SNARKs," in *Proc. 2025 Annual Computer Security Applications Conf. Workshops (ACSAC Workshops)*, Honolulu, HI, USA, pp. 309–315 (2025), doi: 10.1109/ACSACW69556.2025.00040.

[10] F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil, "Authentication based on non-interactive zero-knowledge proofs for the Internet of Things," *Sensors*, vol. 16, no. 1, Art. no. 75 (2016), doi: 10.3390/s16010075.

[11] B. Mbimbi, D. Murray, and M. Wilson, "Preserving whistleblower anonymity through zero-knowledge proofs and private blockchain: A secure digital evidence management framework," *Blockchains*, vol. 3, no. 2, Art. no. 7 (2025), doi: 10.3390/blockchains3020007.

[12] B. Haiba and N. Rafalia, "Blockchain-based solution for privacy-preserving SIM card registration," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, Art. no. 30 (2026), doi: 10.3390/jcp6010030.

[13] R. Nage and S. Dorle, "Design of an iterative method with unified privacy-preserving authentication and intelligent forensic framework for cloud and IoT security analysis," in *Proc. 2025 IEEE 2nd Int. Conf. Women in Computing (InCoWoCo)*, India, pp. 1–8 (2025), doi: 10.1109/InCoWoCo68239.2025.11407252.

[14] T. Segkoulis and K. Limniotis, "Enhancing multi-factor authentication for mobile devices through cryptographic zero-knowledge protocols," *Electronics*, vol. 14, no. 9, Art. no. 1846 (2025), doi: 10.3390/electronics14091846.

Received April, 2026