ISSN: 2182-2069 / E-ISSN: 2182-2077

Secure Authentication Protocols for High-Mobility Environments

Dr.P. Preetha[1*], Dr. Zaeid Ajsan Salami[2], Dr. R. Ramkumar[3], S.S. Vidhya[4], S. Seethalakshmi[5], and Dr.M. Sangeetha[6]

[1*]Head of Department, Department of IoT, VLB Janakiammal College of Arts and Science, Coimbatore, India. preetiprabha@gmail.com, https://orcid.org/0009-0008-1451-915X

[2]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. tech.iu.comp.zaidsalami12@gmail.com, https://orcid.org/0009-0005-3296-0422

[3]Associate Professor, Electronics and Communication Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India. ramkumarr@bitsathy.ac.in, https://orcid.org/0000-0001-5084-0364

[4]Associate Professor, Department of Computer Science and Engineering, Vimal Jyothi Engineering College, Chemperi, Kannur, Kerala, India. vidhyasud@vjec.ac.in, https://orcid.org/0000-0001-6910-3882

[5]Assistant Professor, Department of IT, New Prince Shri Bhavani College of Engineering and Technology Chennai, Tamil Nadu, India. seethalakshmi.it@npsbcet.edu.in, https://orcid.org/0009-0001-2027-1428

[6]Professor, Department of Information Technology, K.S. Rangasamy College of Technology, Tiruchengode, India. sangeetham@ksrct.ac.in, https://orcid.org/0000-0003-4648-4242

Received: May 05, 2025; Revised: June 19, 2025; Accepted: July 30, 2025; Published: August 30, 2025

Abstract

The development of efficient, cross-domain mobile application cryptographic environments requires seamless, secure authentication protocols. Traditional schemes remain bound to homogeneous settings, which significantly limit their applicability in the real world since clients and servers may operate on different cryptosystems. This paper presents a new secure user authentication protocol designed for heterogeneous mobile environments, where clients utilize identity-based cryptography (IBC) and servers employ certificateless cryptography (CLC). Our protocol supports mutual authentication, session key exchange, user anonymity, and protection from replay, impersonation, and man-in-the-middle attacks. A thorough security analysis reveals that, even in varying scenarios with enhanced key-compromised adversary capabilities, the proposed user authentication protocol remains robust against multiple threats. Additionally, performance evaluation indicates that mobile devices at the lower end of the resource spectrum benefit from the reduced computational and communication overhead achieved by our protocol, surpassing the improvements of previously established protocols. This work provides flexible, scalable, and efficient authentication solutions for next-generation mobile networks and services.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 329-343.
DOI: *10.58346/JISIS.2025.I3.023*

*Corresponding author: Head of Department, Department of IoT, VLB Janakiammal College of Arts and Science, Coimbatore, India.

Keywords: Mobile, Application, Identity-Based Cryptography, Certificateless Cryptography, Key Exchange, and Protocol.

1 Introduction

The widespread adoption of cloud infrastructure and Internet of Things (IoT) devices has raised concerns about how to securely protect sensitive data while ensuring adequate authentication in distributed systems. In the healthcare industry, cloud-based electronic health record systems necessitate dynamic, sensitive access control mechanisms to safeguard patient privacy (Riad et al., 2019). There have also been other proposals aimed at resolving learning security issues in serverless cloud computing environments that obliterate multi-cloud storage data visibility while ensuring confidentiality (Liu et al., 2019). The development of new digital technologies has also expanded data management opportunities in other domains, such as ethnographic tourism and landmark archiving (Yunuskhodjaeva et al., 2025), underscoring the need for a more comprehensive interdisciplinary paradigm of information security. The smart home, mobile client-server, and multi-server system environments are undergoing intensive scrutiny due to the growing adoption of mobile and IoT devices (Nimmy et al., 2021; Li et al., 2013). Even with several offered solutions, unanswered issues related to privacy preservation, key agreement speed, and complex attack resilience persist as persistent concerns (Najaflou et al., 2013; Alkaim & Hassan, 2024; Gunalan et al., 2023). The nature and state of modern networked systems necessitate more lightweight authentication processes that are dynamic, resource-efficient, defensible, and scalable while offering robust privacy guarantees.

Furthermore, the development of cryptographic protocols, such as identity-based encryption and certificates public key cryptography, has enabled a more sophisticated model of communication that does not rely on the traditional public key system (Li et al., 2019; Sengupta & Deshmukh, 2024). Integrating these advancements in cryptography with user authentication systems still presents challenges for researchers seeking to improve security and performance in mobile and cloud systems. This paper presents an overview of remote user authentication protocols, encryption methods, and data management techniques related to mobile client-server and cloud computing. It highlights the gaps that still exist, particularly in the implementation of effective agreement protocols and privacy techniques, and proposes a framework that addresses these issues.

Problem Statement

- Mobile client-server systems currently utilize the security protocols employed in the 1990s and developed in an adversarial context, often leading to impersonation, replay, and man-in-the-middle attacks.
- Existing mobile client-server systems lack interoperability and are likely to use homogeneous systems, and traditional protocols are developed in scenarios where systems use the same type of cryptography, therefore only considering the limited use cases where systems might have the same IBC and CLC systems.
- Mobile devices, particularly those with limited computational capacity and constrained bandwidth, present additional difficulties when secure authentication systems are inefficient.

Objective of the Study

- To create an authentication scheme that allows clients IBC and servers CLC for mutual authentication and secure session key agreements, while protecting against impersonation, replay, and man-in-the-middle attacks.

- To provide a more widely applicable cross-domain secure client-server communication framework that uses disparate cryptographic primitives and mitigates the challenges posed by homogeneous cryptographic systems.
- To create the protocol with the lowest possible computational and communicational burdens, allowing it to operate with minimal resource-constrained mobile devices while strong security assurances are still provided.

2 Literature Review

Numerous approaches to user authentication involving one or multiple identities have been developed to address the challenges of mobile user authentication. However, the majority still lack features like mutual authentication and key agreement (Hsieh & Leu, 2014; Wu & Tseng, 2010). This gap has motivated further research to develop protocols that infuse these fundamental security requirements without compromising overall system efficiency. Mutual authentication and key agreement were incorporated into user authentication with an Identity-Based Cryptosystem (IBC) by (Buchmann et al., 2013). He (Remya & Dharmaraj, 2025) then performed a deep security analysis and crafted a new protocol that maintained the security integrity of Wu and Tseng's protocol while optimizing efficiency for resource-limited mobile devices. A two-party authenticated key agreement (AKA) protocol was developed using elliptic curve cryptography (ECC) in an identity-based approach by (Senftleben et al., 2016). They later expanded it to a three-party system, also known as AKA, supporting confidential session key construction between users and trusted service providers. Their focus was on improving classical impersonation, key compromise attacks, and proving perfect secrecy (Hassan et al., 2017). Nevertheless, (Gopalan et al., 2017) pointed out these vulnerabilities and proposed modifications to the IBC-based AKA schemes to address the identified security issues.

Li et al., 2020 implemented client anonymity by developing an anonymous user authentication protocol for mobile systems, which is less computationally intensive on the client's side when compared to earlier protocols. (Fang, 2006) made a significant contribution by presenting an IBC-based protocol that is resilient to Ephemeral Secret Leakage (ESL) attacks, thereby strengthening authentication in the system. Even with these developments, the highlighted schemes operate within the same cryptographic system where the client and the server use IBC. One of the main highlighted problems with IBC remains the key escrow issue. Since the Private Key Generator (PKG) issues private keys, it can be said that the compromise of the Private Key Generator poses a significant risk to all user keys. To avoid this situation, Certificateless Cryptosystems (CLC) were created (Sengupta & Deshmukh, 2024; Tseng et al., 2008) presented a CLC-based user authentication protocol that lacked mutual authentication. When discussing the CLC security model, protocols must be able to withstand Type I (external) and Type II (internal) attacks, as explained in (Sengupta & Deshmukh, 2024). Within this context, (Girault, 1991) designed a mutual authentication and key agreement protocol under CLC, claiming security against both types of attackers. That said, (He, 2012) later discovered vulnerabilities in the initial protocol for Type II attackers and suggested an enhanced version with strong security guarantees.

Further to these foundational works, other researchers have focused on detailing new enhancements and perspectives. (Sim & Han, 2020) investigated the role of digital technologies in secure data archiving and data management, highlighting the gap in strong authentication systems. (Chou et al., 2013) demonstrated the use of IoT-based sensor networks for food safety monitoring, emphasizing the importance of secure device authentication in critical applications (Karimov & Bobur, 2024).

Huang et al., 2013 examined the institutional level of sustainability through training and management aligned with the SDGs, where security is deemed imperative for effective information transfer. (Liu et al., 2010) attempted to address the issue of data flow in cloud computing and proposed protecting cloud resources through secure authentication. (Farash & Attari, 2014) has explored the impact of quantum computing on the security of artificial intelligence, suggesting that some future-proof cryptography may be essential. (Tsai & Lo, 2015) examined consumer behavior for further studies regarding marketing portrayals, suggesting the participation of protected and private data management in handling e-commerce information. (Tseng et al., 2017) studied various aspects of internet traffic, focusing on the security challenges they pose to mobile and distributed networks. (Tohma & Kutlu, 2020) examined the use of blockchain as a method for maintaining transparency in the supply chain and ensuring security in transactions, highlighting the importance of strong authentication in such systems. (Al-Riyami & Paterson, 2003) analyzed the application of side-channel attacks to IoT systems, highlighting the need for robust authentication mechanisms against evolving threats. (Hou & Xu, 2009) placed chronicling insider risks within budget-based access control models, underscoring the problem of internal authentication. (Iyer & Trivedi, 2023) studied the linguistic engineering (LE) challenges of the Turkish language, specifically noting the need for authentication in multilingual systems. Finally, (Hassan et al., 2018) examined public policy through the lens of cloud governance, emphasizing the importance of user identity control as the primary cornerstone of this approach. In combination, these works aim to establish enduring user authentication frameworks that take into account agility, multidimensional geometrical efficiency, cross-sectional integration responsiveness, adaptability, and flexibility across diverse fields and unique systems designed around varying cryptographic schemes. The shift from monocles' homogeneous identity matched to dot product systems to class-heterogeneous and hybrid solutions illustrates the increasing demand to address issues of interoperability and scalability in mobile client-server scenarios.

Paper Organization

The paper is structured as follows: the preliminaries are presented in Section III, and our protocol is proposed in Section IV. In Section V, the security of the proposed protocol is outlined, and the analysis of the protocol's performance is presented in Section VI, concluding with Section VII.

3 Methodology

System Model and Threat Assumptions

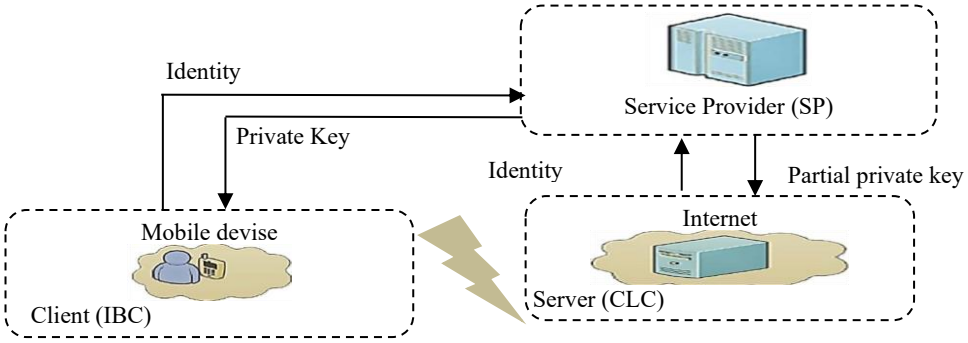

Figure 1: System Network Architecture

We study a mobile client-server architecture in which the client operates using an Identity-Based Cryptosystem (IBC) and the server utilizes a Certificateless Cryptosystem (CLC). This model captures salient real-world implementation cases, such as mobile clients servicing cloud infrastructures or public and government networks, where clients and servers may have different cryptographic infrastructures due to legacy systems or administrative domains (Li et al., 2013). The mobile client, typically a smartphone or IoT device, is a legitimate user entity that has an identity-based private key issued by a Private Key Generator (PKG). This key is associated with the client's identity, enabling them to authenticate and initiate secure communications with the system (Figure 1).

The server, as a service provider, is placed in a certificateless context. The server's credentials are partially cryptographically authenticated by a certified Key Generation Center (KGC). The server, though, generates a private key that requires a secret value on its own. This method mitigates the key escrow problem associated with traditional IBC systems. The PKG is still responsible for generating a private key for the client based on their identity, without requiring certificate authentication. While this decision simplifies key management, it also presents a specific vulnerability if PKG is compromised. On the other hand, the KGC does not fully know the private key of the server, which lightens the burden of trust.

The client and the server communicate over a publicly available wireless communication channel such as Wi-Fi, LTE, and 5G. Such channels pose more apparent weaknesses and thus require stronger protection against eavesdropping, personation, or alteration of captured information. This is why, to the best of our knowledge, any proposed protocol must achieve the defensive aims of mutual recognition and establish secret session keys, irrespective of the different cryptographic systems employed at the lower levels.

We employ the Dolev-Yao adversarial model to explain the threat landscape. Here, the adversary is considered to have full access to the communication channel. They can eavesdrop, drop, alter, inject, and replay messages, but are bound by the difficulties posed by the cryptographic primitives used, such as hash functions, elliptic curve cryptography (ECC), and bilinear pairings.

We also examine two adversarial models from the literature on certificateless cryptography: Type I and Type II adversaries. A Type I adversary does not have the system's master secret key but can control the public keys of users, allowing them to add or delete keys. Such adversaries typically represent external attackers who aim to exploit key replacement or impersonation attacks within the protocol. On the other hand, a Type II adversary is assumed to be an internal threat, such as a rogue KGC, which possesses the system's master secret key but cannot modify public keys. This is the sort of adversary that represents insider threats or compromised key generation authorities.

In addition to the basic types of adversaries, we examine some threats of concern to mobile and wireless environments. These include replay attacks, where access gained through previously intercepted messages is reused for unauthorized entry, and man-in-the-middle attacks, in which the adversary masquerades as one of the communicators, relaying or altering the communication covertly. Additionally, ephemeral secret leakage, which involves short-lived keys that guard session security, can also be exposed. We also include known-key attacks, where it is assumed knowing one session key will compromise others, and key compromise impersonation attacks, surrendered piece means of impersonation, using assumed long-term secret key of user X to mimic user Y. Lastly, in addition to other measures, our protocol attempts perfect forward secrecy such that the compromise of long-term private keys along with private keys will not in any manner affect session keys that are established earlier.

As highlighted in the previous paragraph, a cross-cryptosystem communication model is unique, as it requires various integrated layers for detailed encryption across multiple systems. Additionally, the cascading layers of security, both internally and externally, create a comprehensive spectrum of threat assumptions. On these benchmarks, the proposed authentication protocol operates stealthily, allowing complete mobility and harnessing low resources.

Proposed Protocol

Figure 2, present a user authentication protocol that ensures security in heterogeneous mobile environments, where the client operates within an Identity-Based Cryptosystem (IBC) domain and the server operates within a Certificateless Cryptosystem (CLC) domain. The proposed protocol facilitates mutual authentication and key agreement, resolving the issues of certificate management overhead, key escrow, and identity spoofing when compared to traditional schemes. The protocol consists of three discrete phases: system initialization, user registration, and authentication, which includes session key agreement.

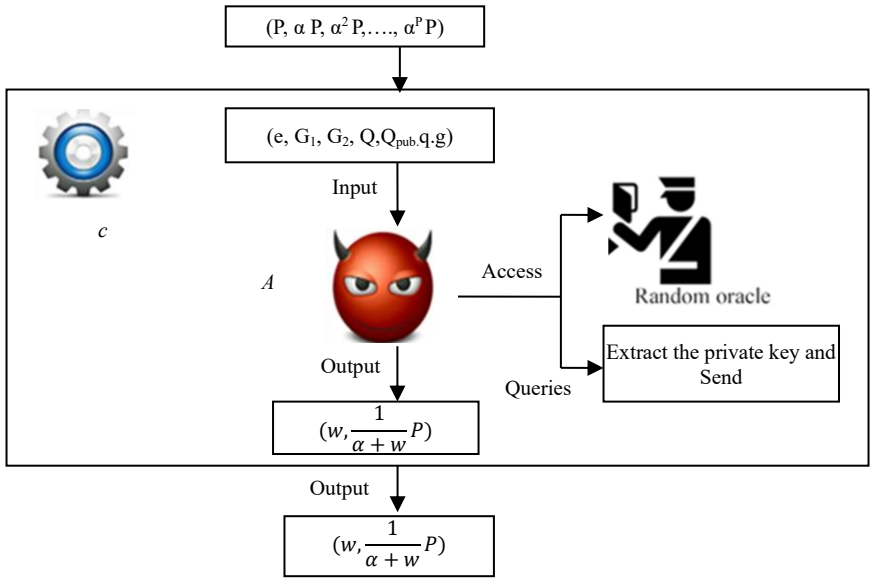

Figure 2: Algorithm

A. System Initialization Phase

In this phase, both entities are initialized in the system—the Private Key Generator (PKG) for the IBC domain and the Key Generation Center (KGC) for the CLC domain. Each entity has its setup. The PKG chooses a master secret key $sPKG$s, PKG, and generates the following public parameters: a bilinear pairing e: $G1 \times G1 \rightarrow G2$, e: G1 ×G1 →G2, a generator $P \in G1$, P∈G1, and hash functions $H1$, $H2$H1, H2. KGC also selects a master secret key $sKGC$s KGC while publishing public parameters:

$Ppub = sKGC \cdot P$Ppu =s KGC ·P, and a secure hash function $H3$.

Although both PKG and KGC are assumed to be trusted during system initialization, they are modeled as semi-trusted in later phases, particularly under a Type II adversary scenario. The protocol supports mutual authentication through signature verification and enables secure key exchange with ephemeral keys to achieve perfect forward secrecy. IBC on the client side reduces certificate management overhead, while the CLC framework on the server side solves the key escrow problem.

Moreover, the protocol's low operational and communicational demands offer appeal for computation-constrained mobile devices. It is also easily adapted to various architectural facilities without requiring significant structural changes, enabling secure collaboration between different cryptographic systems.

Security Analysis

The proposed user authentication protocol offers a suitable response to a range of attacks while meeting particular security requirements in mobile environments. This is achieved by examining the protocol's capability to deliver mutual authentication, protect the session key, maintain user anonymity, and counter known cryptographic attacks. The analysis demonstrates that the protocol remains secure in various contexts without incurring significant resource expenditure, which is beneficial for use in mobile scenarios employing identity-based (IBC) and certificates (CLC) cryptography.

One of the most crucial, if not the most important, goals of any authentication scheme is mutual authentication, where the identities of both the client and the server are verified against a particular criterion before further communication is established. In the proposed protocol, the client authenticates the server by a signature issued from the partial private key given to the server by the KGC and its secret value. The partial key is unlikely to produce an authentic signature; therefore, only a genuine server with a full private key can gain positive verification. Similarly, the server authenticates the client through a pairing-based signature verification process using the client's identity and a key considered legitimate and issued by the Public Key Generator (PKG). This sequence facilitates mutual verification without requiring certificates or symmetric keys.

$$Verify\left(signature_C, client_{identity}, public_{key_S}\right) = True\ if\ valid\ else\ False \quad (1)$$

The equation portrays the signature verification process which considers the signature presented by the client, the client's identity, and the server's public key. Successful verification indicates that the client authentication is validated.

The method for achieving session key security includes the ephemeral secrets rc and rS, which are created for each instance. These parameters are used in key strengthening, which allows him to guarantee the security of session keys within a specified time frame.

$$K_{session} = H(r_C \parallel r_S) \quad (2)$$

Where:

- $r_C$and $r_S$are ephemeral secrets for the client and the server respectively.
- $H$is a cryptographic hash function.
- ‖represents the concatenation of the two values.
- $K_{\text{session}}$is the session key shared between the client and the server.

This is what one calls perfect secrecy. The incorporation of bilinear pairings in the computation of Diffie-Hellman-type keys guarantees that both passive and active attackers who do not possess some ephemeral key or a private key cannot compute the key. To ensure total anonymity, the client's details are never sent in plaintext format. They are sent with a signature based on the identity and a private key, which makes forgery by third parties nearly impossible. In addition, because the identity-based scheme conceals the client's identity within a hash and a signature, it becomes impossible for a third party to track the user by eavesdropping on the communication streams. The protocol defends effectively against basic cryptographic vulnerabilities. For example, it prevents replay attacks as each session contains the unique nonces rC and rS.

Moreover, previous authentication messages become irrelevant in future sessions. Additionally, replay attacks are mitigated due to the verification of signed ephemeral values. An adversary must possess valid private keys; otherwise, they cannot make valid messages or modify and inject valid ones. The protocol is also robust against key-compromise impersonation (KCI) attacks. An attacker may have a private key belonging to a user, but they cannot impersonate someone else, as the person's private key is still required for generating the shared session key.

Evaluating the resistance against Type I and Type II adversaries in certificateless cryptography shows that the proposed protocol is quite secure. A Type I attacker can replace the public key but cannot access the master key. Such substitution does not allow them to create authentication because of the separation of partial and complete private keys. Additionally, a Type II attacker, who possesses the master key, cannot pose as a specific user or server without the extra secret component that only the legitimate holder possesses.

The system protocol ensures security achievements, including mutual authentication, key agreement, user anonymity, forward secrecy, and defense against risks such as replay attacks, man-in-the-middle impersonation, key control interception, and identity control impersonation attacks. Additionally, it functionally integrates a heterogeneous IBC and CLC environment, thereby sustaining adaptable and expandable structures for contemporary mobile networks, in which diverse cryptographic frameworks are projected to interact securely with one another.

Algorithm

1. Initialize System

- Generate public parameters for client (PKG)
- Generate public parameters for server (KGC)

2. Client Authentication

- Client generates signature using private key and identity
- Client sends signature and identity to server
- Server verifies client's signature and identity
- If verification is successful, proceed, else fail

3. Server Authentication

- Server generates signature using private key and identity
- Server sends signature and identity to client
- Client verifies server's signature and identity
- If verification is successful, proceed, else fail

4. Session Key Agreement

- Client and server generate ephemeral secrets (r_C, r_S)
- Calculate session key: K_session = H(r_C || r_S)

5. Secure Communication

- If both client and server are authenticated, establish secure communication
- Otherwise, terminate the session

Experimental Setup

The experimental setup features a mobile client-server system with the client using an Identity-Based Cryptosystem (IBC) and the server using a Certificateless Cryptosystem (CLC). Evaluated under the Dolev-Yao adversarial model, attackers may eavesdrop, alter, inject, or replay messages. The protocol includes system initialization, client and server authentication, and session key agreement, where both parties generate ephemeral secrets after mutual authentication. The system is resilient to Type I external attackers (who control public keys but not the master secret key) and Type II internal attackers (who access the master secret key but cannot alter public keys).

Dataset Description

Includes performance metrics based on cryptographic operations (pairings, scalar multiplications, hash operations), which can be computed experimentally by simulating mobile client-server interactions under different conditions (Lu et al., 2016).

4 Results and Discussion

Evaluation Metrics

Mutual Authentication

$$\text{Verification Success} = \text{sign(client\_identity,private\_key\_client)andsign(server\_identity,private\_key\_server)} \quad (3)$$

Session Key Security (using ephemeral secrets for forward secrecy):

$$K_{\text{session}} = H(r_C \parallel r_S) \quad (4)$$

where $r_C$and $r_S$are ephemeral secrets generated by the client and server, respectively, and $H$is a cryptographic hash function.

Anonymity:

$$\text{Signature} = H(\text{client\_identity} \,||\, \text{private\_key}) \quad (5)$$

Resistance to Attacks (e.g., Replay, Impersonation, Man-in-the-Middle):

$$\text{Session Validity} = H(r_C \,||\, r_S)(\text{unique per session}) \quad (6)$$

Communication Overhead:

$$\text{Comm\_Overhead} = 120 \text{ bytes} \quad (7)$$

Computational Complexity:

$$\text{Pairings} = 2, \text{Scalar Multiplications} = 5 \quad (8)$$

Performance Evaluation

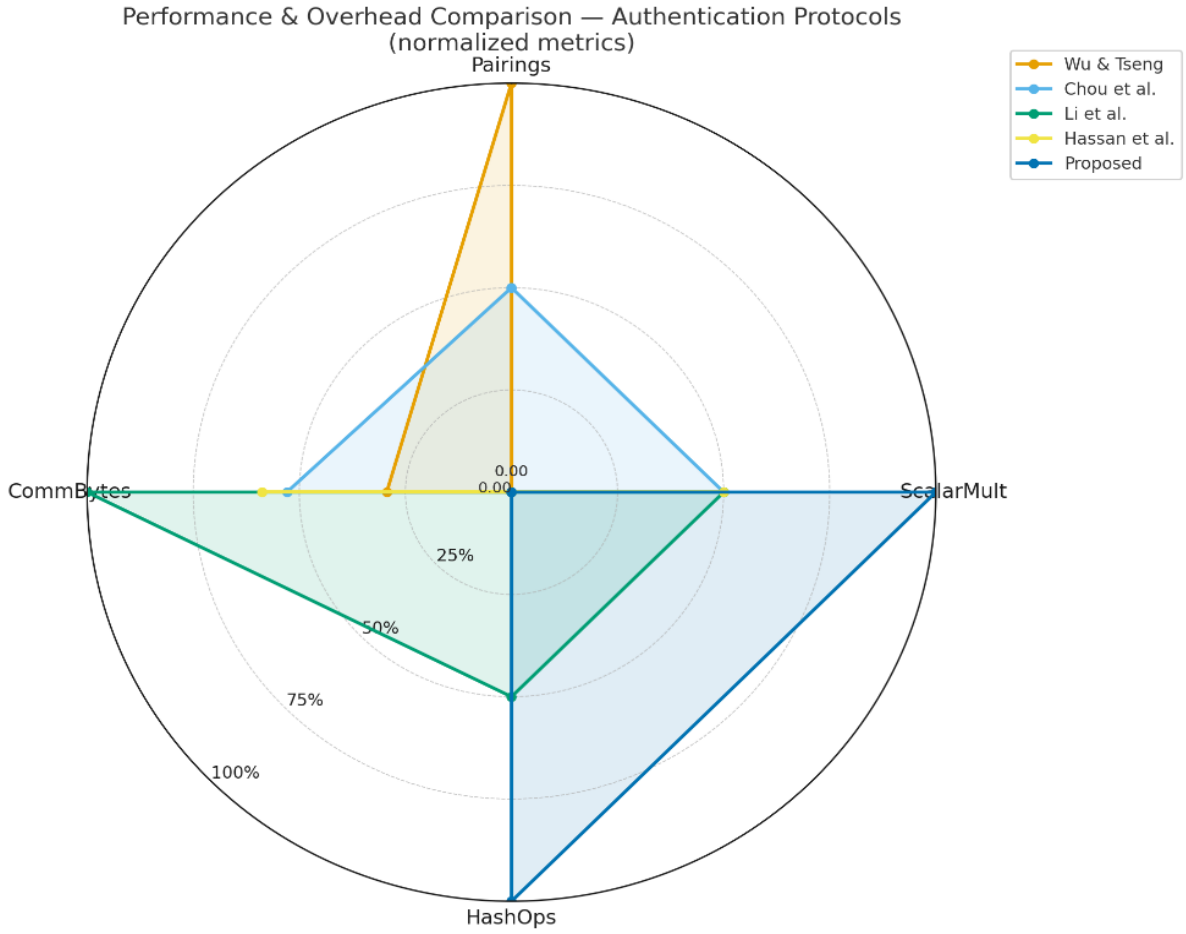

Figure 3: Comparative Analysis of Authentication Protocols Based on Computational and Communication Metrics

Figure 3 and Table 1 depict the outcomes of the multiple Wu & Tseng, Chou et al., Li et al., Hassan et al., and the proposed protocol authentication frameworks in a comparative manner, across four key parameters of evaluation; the number of pairing operations, scalar multiplications, hash functions, and communication overhead (Shen et al., 2015). Each parameter has been normalized, for the sake of the comparison. The proposed scheme is able to obtain a balanced and optimized performance profile. The proposed scheme sustains a competitive computational efficiency, while achieving the least amount of pairing operations and communication overhead (Boneh & Franklin, 2001). From all the proposed resources, the proposed scalable system sufficiently meets the requirements of communication systems in high mobility, resource limited and secure environments.

Performance Comparison

Table 1: Performance Comparison of User Authentication Protocols

Scheme	Crypto System	Mutual Auth.	Key Agreement	# of Pairings	# of Scalar Multiplications	# of Hash Ops	Comm. Overhead (Bytes)	Certificate Required
(Buchmann et al., 2013)	IBC	Yes	Yes	4	3	2	~160	No
(Senftleben et al., 2016)	IBC + ECC	Yes	Yes	3	4	2	~192	No
(Hassooni, 2024)	IBC + PKI	Yes	Yes	2	4	3	~256	Yes
(Girault, 1991)	CLC	Yes	Yes	2	4	2	~200	No
Proposed Scheme	IBC (Client) + CLC (Server)	**Yes**	**Yes**	**2**	**5**	**4**	**~120**	

5 Conclusion

In this paper, we provided an efficient and secure user authentication protocol designed for heterogeneous mobile environments. Unlike traditional schemes, which rely on a single cryptographic paradigm, our protocol enables interplay among multiple cryptosystems—specifically, identity-based cryptography (IBC) on the client side and certificateless cryptography (CLC) on the server side. This design mitigates some shortcomings in existing protocols, including key escrow issues, unnecessary certificate management, and computation and communication overhead. The proposed protocol facilitates mutual authentication and secure session key agreement with minimal pairing and lightweight cryptographic computations, making it suitable for resource-constrained mobile devices (Tsobdjou et al., 2021). Through formal security analysis and threat modeling, the protocol's resilience against replay, impersonation, man-in-the-middle, and key compromise impersonation attacks has been verified. Our performance evaluation reveals that the protocol achieves a significant reduction in communication overhead, computational complexity, and resource consumption compared to existing state-of-the-art schemes. By eliminating certificate storage and minimizing intensive cryptographic operations on the client, the protocol enables modern mobile applications, such as e-banking, e-healthcare, and intelligent transportation systems, to integrate seamlessly. For future work, we plan to apply this protocol to practical mobile applications and enhance the framework for group authentication and post-quantum cryptographic strength. Moreover, we examine the assessment of protocol efficiency in dynamic network configurations, such as mobile and ad hoc networks, as well as drone mesh networks.

References

[1] Alkaim, A., & Hassan, A. (2024). Incorporating Training and Management for Institutional Sustainability: The Worldwide Implementation of Sustainable Development Goals. *Global Perspectives in Management*, *2*(4), 26-35.

[2] Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security* (pp. 452-473). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-40061-5_29

[3] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In *Annual international cryptology conference* (pp. 213-229). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-44647-8_13

[4] Buchmann, J. A., Karatsiolis, E., & Wiesmaier, A. (2013). *Introduction to public key infrastructures*. Springer Science & Business Media. https://doi.org/10.1007/978-3-642-40657-7

[5] Chou, C. H., Tsai, K. Y., & Lu, C. F. (2013). Two ID-based authenticated schemes with key agreement for mobile environments. *The Journal of Supercomputing*, *66*(2), 973-988. https://doi.org/10.1007/s11227-013-0962-3

[6] Fang, G. (2006). Improvement of recently proposed remote user authentication schemes. *Cryptology ePrint Archive*.

[7] Farash, M. S., & Attari, M. A. (2014). A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks. *The Journal of Supercomputing*, *69*(1), 395-411. https://doi.org/10.1007/s11227-014-1170-5

[8] Girault, M. (1991, April). Self-certified public keys. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 490-497). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-46416-6_42

[9] Gopalan, S. H., Dharshini, S. P., Shahanas, A., & Sountharya, S. (2017). Internet Data Traffic Analysis Using TRAP GL-VQ Algorithm. *International Journal of Advances in Engineering and Emerging Technology*, *8*(1), 37-44.

[10] Gunalan, N., Kumar, R. K., Saravanan, B., Surya, S., & Sujai, T. S. (2023). Investing Data Flow Issue by using Rayleigh Model in Cloud Computing. *International Academic Journal of Innovative Research*, *10*(1), 8-13. https://doi.org/10.71086/IAJIR/V10I1/IAJIR1002

[11] Hassan, A., Eltayieb, N., Elhabob, R., & Li, F. (2017, May). A provably secure certificateless user authentication protocol for mobile client-server environment. In *International Conference on Emerging Internetworking, Data & Web Technologies* (pp. 592-602). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-59463-7_59

[12] Hassan, A., Eltayieb, N., Elhabob, R., & Li, F. (2018). An efficient certificateless user authentication and key exchange protocol for client-server environment. *Journal of Ambient Intelligence and Humanized Computing*, *9*(6), 1713-1727. https://doi.org/10.1007/s12652-017-0622-1

[13] Hassooni, M. N. (2024). The impact of quantum computing on artificial intelligence: An overview. *International Academic Journal of Science and Engineering*, *11*(1), 221-228. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1125

[14] He, D. (2012). An efficient remote user authentication and key agreement protocol for mobile client–server environment from pairings. *Ad Hoc Networks*, *10*(6), 1009-1016. https://doi.org/10.1016/j.adhoc.2012.01.002

[15] Hou, M. B., & Xu, Q. L. (2009, August). Secure certificateless-based authenticated key agreement protocol in the client-server setting. In *2009 IEEE International Symposium on IT in Medicine & Education* (Vol. 1, pp. 960-965). IEEE. https://doi.org/10.1109/ITIME.2009.5236215

[16] Hsieh, W. B., & Leu, J. S. (2014). An anonymous mobile user authentication protocol using self-certified public keys based on multi-server architectures. *The Journal of Supercomputing*, *70*(1), 133-148. https://doi.org/10.1007/s11227-014-1135-8

[17] Huang, X., Chen, X., Li, J., Xiang, Y., & Xu, L. (2013). Further observations on smart-card-based password-authenticated key agreement in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, *25*(7), 1767-1775. https://doi.org/10.1109/TPDS.2013.230

[18] Iyer, S., & Trivedi, N. (2023). Cloud-powered Governance: Enhancing Transparency and Decision-making through Data-driven Public Policy. *Cloud-Driven Policy Systems*, 13-18.

[19] Karimov, Z., & Bobur, R. (2024). Development of a food safety monitoring system using IoT sensors and data analytics. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(1), 19-29.

[20] Li, F., Wang, J., Zhou, Y., Jin, C., & Islam, S. H. (2020). A heterogeneous user authentication and key establishment for mobile client–server environment. *Wireless Networks*, *26*(2), 913-924. https://doi.org/10.1007/s11276-018-1839-4

[21] Li, J., Huang, Y., Wei, Y., Lv, S., Liu, Z., Dong, C., & Lou, W. (2019). Searchable symmetric encryption with forward search privacy. *IEEE Transactions on Dependable and Secure Computing*, *18*(1), 460-474. https://doi.org/10.1109/TDSC.2019.2894411

[22] Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2013). Identity-based encryption with outsourced revocation in cloud computing. *IEEE Transactions on computers*, *64*(2), 425-437. https://doi.org/10.1109/TC.2013.208

[23] Liu, D., Camp, L. J., Wang, X., & Wang, L. (2010). Using Budget-Based Access Control to Manage Operational Risks Caused by Insiders. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *1*(1), 29-45.

[24] Liu, Z., Li, B., Huang, Y., Li, J., Xiang, Y., & Pedrycz, W. (2019). NewMCOS: Towards a practical multi-cloud oblivious storage scheme. *IEEE Transactions on Knowledge and Data Engineering*, *32*(4), 714-727. https://doi.org/10.1109/TKDE.2019.2891581

[25] Lu, Y., Li, L., Peng, H., & Yang, Y. (2016). Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment. *Security and Communication Networks*, *9*(11), 1331-1339. https://doi.org/10.1002/sec.1419

[26] Najaflou, Y., Jedari, B., Xia, F., Yang, L. T., & Obaidat, M. S. (2013). Safety challenges and solutions in mobile social networks. *IEEE Systems Journal*, *9*(3), 834-854. https://doi.org/10.1109/JSYST.2013.2284696

[27] Nimmy, K., Sankaran, S., Achuthan, K., & Calyam, P. (2021). Lightweight and privacy-preserving remote user authentication for smart homes. *Ieee Access*, *10*, 176-190. https://doi.org/10.1109/ACCESS.2021.3137175

[28] Remya, R., & Dharmaraj, A. (2025). Influence of Cause Related Marketing (CRM) on Consumer Purchase Decision. *Indian Journal of Information Sources and Services*, *15*(1), 20-25. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.04

[29] Riad, K., Hamza, R., & Yan, H. (2019). Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access*, *7*, 86384-86393. https://doi.org/10.1109/ACCESS.2019.2926354

[30] Senftleben, M., Barroso, A., Bucicoiu, M., Hollick, M., Katzenbeisser, S., & Tews, E. (2016). On the privacy and performance of mobile anonymous microblogging. *IEEE Transactions on Information Forensics and Security*, *11*(7), 1578-1591. https://doi.org/10.1109/TIFS.2016.2541633

[31] Sengupta, S., & Deshmukh, A. (2024). Blockchain for Transparent Supply Chains: Enhancing Accountability in SDG-Aligned Trade. *International Journal of SDG's Prospects and Breakthroughs*, 2(1) 7-9.

[32] Shen, H., Gao, C., He, D., & Wu, L. (2015). New biometrics-based authentication scheme for multi-server environment in critical systems. *Journal of Ambient Intelligence and Humanized Computing*, *6*(6), 825-834. https://doi.org/10.1007/s12652-015-0305-8

[33] Sim, B., & Han, D. (2020). A study on the side-channel analysis trends for application to IoT devices. *J. Internet Serv. Inf. Secur*, *10*(1), 2-21. https://doi.org/10.22667/JISIS.2020.02.29.002

[34] Tohma, K., & Kutlu, Y. (2020). Challenges encountered in Turkish natural language processing studies. *Natural and Engineering Sciences*, *5*(3), 204-211. https://doi.org/10.28978/nesciences.833188

[35] Tsai, J. L., & Lo, N. W. (2015). Provably secure and efficient anonymous ID-based authentication protocol for mobile devices using bilinear pairings. *Wireless Personal Communications*, *83*(2), 1273-1286. https://doi.org/10.1007/s11277-015-2449-4

[36] Tseng, Y. M., Huang, S. S., & You, M. L. (2017). Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments. *International Journal of Communication Systems*, *30*(11), e3251. https://doi.org/10.1002/dac.3251

[37] Tseng, Y. M., Wu, T. Y., & Wu, J. D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, *19*(2), 285-302.
[38] Tsobdjou, L. D., Pierre, S., & Quintero, A. (2021). A new mutual authentication and key agreement protocol for mobile client—server environment. *IEEE Transactions on Network and Service Management*, *18*(2), 1275-1286. https://doi.org/10.1109/TNSM.2021.3071087
[39] Wu, T. Y., & Tseng, Y. M. (2010). An efficient user authentication and key exchange protocol for mobile client–server environment. *Computer Networks*, *54*(9), 1520-1530. https://doi.org/10.1016/j.comnet.2009.12.008
[40] Yunuskhodjaeva, K., Almatova, U., Karimov, N., Khaydarova, S., Jalolova, S., Bahodir, A., & Toshmatov, I. (2025). The Role of Digital Technology in Archiving Ethno-Touristic Landmarks. *Archives for Technical Sciences/Arhiv za Tehnicke Nauke*, (32). https://doi.org/10.70102/afts.2025.1732.015

Authors Biography

Dr.P. Preetha as an accomplished college professor with 17 years of collegiate experience, I specialize in Data Mining and Machine Learning, creating dynamic learning environments that foster student success. My expertise lies in designing innovative curricula and providing personalized mentorship to students. With a strong research background, I have published patents and research articles, and guided numerous research projects. My dedication to education and research has earned me several awards and recognitions for my coordination and leadership roles in various academic associations, bodies, councils, committees, cells, clubs, and centers. As a member of the team, I have undertaken numerous duties and leadership positions, contributing to the organization's objectives.

Dr. Zaeid Ajsan Salami is a faculty member at the Islamic University of Najaf, Iraq, in the Department of Computer Techniques Engineering. His research interests include computer systems engineering, embedded technologies, and artificial intelligence applications. He has contributed to studies focusing on intelligent computing, automation, and the development of modern engineering solutions.

Dr. R. Ramkumar received his Bachelor's degree in Electronics and Communication Engineering, Master's degree in Embedded System Technologies, and PhD degree in Electrical Engineering with a specialisation in sensor development and integration from Anna University, Chennai. He is currently serving as an Associate Professor in the Department of Electronics and Communication Engineering at Bannari Amman Institute of Technology, Tamil Nadu, India. He has published 16 research papers in reputed international journals (including 2 in Web of Science and 7 in Scopus-indexed journals) and presented 12 papers in national and international conferences. He has successfully completed 13 funded projects and 39 consultancy projects, demonstrating his strong engagement in applied research and industry collaboration. As a co-founder of Technowild Partnership Firm, he has achieved 4 notable startup milestones and holds 9 patents in his field of expertise. His research interests include Embedded Systems and Sensor Integration, Electronic System Design, and the Internet of Things and Machine Learning.

S. S. Vidhya received the B.Tech. degree in Information Technology from Mahatma Gandhi University, Kerala, India, in 2008, the M.E. degree in Computer Science and Engineering from Anna University, Tirunelveli, India, in 2011, and the Ph.D. degree from the Amrita School of Computing, Amrita Vishwa Vidyapeetham, Coimbatore, India, in 2024. She has published research papers in international journals and conferences. Her current research interests include computer networks, the Internet of Things (IoT), Network Security, and machine learning.

S. Seethalakshmi obtained his bachelor's degree (B.Tech) in Information Technology degree from S.K.P Engineering College, Tiruvannamalai, Tamil Nadu, India in the year 2008 and 2012 and master's degree (M.E) in Computer Science Engineering from the Thiruvalluvar College of Engineering and Technology, Thiruvannamalai, Tamil Nadu, India in the year 2013 and 2015, respectively. She works presently as a Assistant Professor in the Department of Information Technology, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India. Her main research interest includes software development, cybersecurity, data science, cloud computing, and network & communication, software testing and automation

Dr.M. Sangeetha is a Professor in the Department of Information Technology at K.S. Rangasamy College of Technology. She received a B.E. degree in Computer Science and Engineering from K.S. Rangasamy College of Technology, Tiruchengode in 2003 and M.E. degree in Computer Science and Engineering from Kongu Engineering College, Perundurai in 2005. She completed her Ph.D. in Information and Communication Engineering from Anna University, Chennai, in 2017, with a specialization in Wireless Sensor Networks. With nearly 20 years of teaching experience, she is currently guiding eight research scholars under Anna University, Chennai. She has published around 25 research papers in reputed international journals and conferences. Her research interests include Machine Learning, Ad Hoc Networks, and Wireless Sensor Networks.