Research Article

An Identity-Based Anonymous Three-Party Authenticated Protocol for IoT Infrastructure

Akasha Shafiq,1 Muhammad Faizan Ayub,1 Khalid Mahmood1,1 Mazhar Sadiq,1 Saru Kumari,2 and Chien-Ming Chen3

1Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus 57000, Pakistan
2Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India
3College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

Correspondence should be addressed to Chien-Ming Chen; chienming.taiwan@gmail.com

Received 24 April 2020; Revised 18 July 2020; Accepted 29 August 2020; Published 22 September 2020

Abstract

The rapid advancement in the field of wireless sensor and cellular networks have established a rigid foundation for the Internet of Things (IoT). IoT has become a novel standard that incorporates various physical objects by allowing them to collaborate with each other. A large number of services and applications emerging in the field of IoT include healthcare, surveillance, industries, transportation, and security. A service provider (SP) offers several services that are accessible through smart applications from any time, anywhere, and any place via the Internet. Due to the open nature of mobile communication and the Internet, these services are extremely susceptible to various malicious attacks, e.g., unauthorized access from malicious intruders. Therefore, to overcome these susceptibilities, a robust authentication scheme is the finest solution. In this article, we introduce a lightweight identity-based remote user authentication and key agreement scheme for IoT environment that enables secure access to IoT services. Our introduced scheme utilizes lightweight elliptic curve cryptography (ECC), hash operations, and XOR operations. The theoretical analysis and formal proof are presented to demonstrate that our scheme provides resistance against several security attacks. Performance evaluation and comparison of our scheme with several related schemes for IoT environment are carried out using the PyCrypto library in Ubuntu and mobile devices. The performance analysis shows that our scheme has trivial storage and communication cost. Hence, the devised scheme is more efficient not only in terms of storage, communication, and computation overheads but also in terms of providing sufficient security against various malicious attacks.

1. Introduction

In the last few years, wireless networks have experienced tremendous growth. Nowadays, there are enormous networks associating from the cellular systems to noninfrastructure wireless systems such as sensor networks, mobile ad hoc networks, and the Internet of Things (IoT). The communication security is the key element for the success of wireless sensor applications [1, 2], especially for sensitive applications that work in mission-critical and hostile areas. Therefore, the provision of reliable and efficient security in wireless networks has always been a challenging task due to various malignant attacks and resource-constrained environment. The hasty development of wireless communication and information technologies leads to a dramatic evolution of the Internet of Things (IoT) which is the combination of smart services and technologies that renders mutual communication among devices and users through the Internet. Since all data is shared between sensing devices and remote users via a network, therefore, it is necessary to design an efficient, secure, and lightweight remote-user authentication-based solution for an IoT environment. As far as the privacy and security of the network are concerned, mutual authentication is considered as a key element for safely accessing various IoT services. Hence, remote-user authentication becomes a vital component of various valuable services in mobile networks.

Besides confidentiality and authenticity, the exclusive features of the online valuable services raise various security questions for the remote authentication. In the environment of mobile networks where several invisible devices gather the
client’s identity information, the anonymity of the client is necessarily required to make sure that the identity information of the requesting client is only known to the requested service provider (SP) and the client [3–5]. Simultaneously, when the anonymity of the client is provided, SP always wants the client’s nonrepudiation for preventing the clients from the denial of charges of their desired services. The efficiency in terms of both computation and communication is crucial for such kinds of remote-user authentication schemes, especially for IoT infrastructure.

The earliest schemes employed conventional public key cryptography (PKC) [6–10]. In these schemes, clients authenticate themselves to service providers using their signature. For hiding the real identity of the clients from eavesdropping, the clients’ signature and clients’ identifier are encrypted using mutual secret keys between the SP and clients. The certificate of clients’ public key needs to be delivered to the SP that enables the signature’s verification. On the other hand, a considerable disadvantage of this approach is on-demand verification and transmission of public key certificates that cause authentication latency [11] as well as a waste of unfavorable bandwidth. In addition, to attain the clients’ anonymity, encryption is required that adds to the scheme’s complexity. In order to remove the drawbacks that are due to public key certificates, the modern remote-user authentication schemes employ an identity-based cryptosystem (IBC) [12–16].

IBC is another form of PKC. The IBC concept was introduced by Shamir [17] in 1984 which is swiftly evolved after Franklin and Boneh’s first identity-based security-provable encryption using pairings [18]. In the IBC concept, the identity (ID) of the client serves as a client’s public key, and the private key generator (PKG) generates the private key. In IBC, a pair of predefined private or public keys are generated on the basis of the user’s credentials such as phone, name, or email. By using the user’s unique credential or identity, the public key can be determined easily, whereas the private key generator is responsible for the generation of private keys. For communicant entities, PKG generates identity-based certificates and forwards it to the other communicants. The users involved in communication can perform encryption, generate a signature, and communicate with other users when they receive their identity-based key certificates. IBC ensures the effortless production of public and private keys. IBC removes the verification and transmission of the public key certificates; therefore, it has become a compelling substitute to conventional PKC [19]. Thus, IBC is efficient in terms of storage and transfer of certificates/public keys in comparison with the classical public key infrastructure. That is why, for a resource-constraint environment, IBC is proved to be appealing. The main advantage of IBC is there is no need of certificates. There is no need of preenrollment. In the traditional public key cryptography system, if the key is compromised, then the keys need to be revoked. Also, for the decryption of messages for the future, it allows postdating.

In identity-based remote-user authentication schemes, the client produces an authenticator by using his identity-based private key. The client is authorized by the SP only if verification of the client’s authenticator produces an absolute result. However, still, there are many issues that need to be resolved satisfactorily such as (i) some identity-based remote user authentication schemes consider the demand of the client’s anonymity; (ii) many of those schemes introduce identity-based signature (IBS) solution and further using it as an authenticator of the client, but it remains unclear why the introduced IBS is employed rather than employing other existing IBS schemes; and (iii) no thorough quantitative argument has been given about the performance merits of such identity-based schemes over the former PKC-based schemes. Aiming to resolve the abovementioned problems, in this article, we propose an identity-based remote-user authentication scheme that targets to deliver valuable services in mobile networks. The novelty of the proposed scheme yields in its way of realizing the client’s privacy without encryption operation.

1.1. Motivation. IoT serves the society with various opportunities in major fields of life, i.e., agriculture, warehousing, healthcare, and industry, that are accessible to everyone with flexibility and ease. However, this hasty development leads to the evolution of several challenges. Therefore, the fundamental motivational factors of our scheme are listed below:

(i) IoT-based sensing devices serve with limited resources like memory, power, and battery. Therefore, an authentication scheme should have low communication and computation overheads.

(ii) Malicious attacks such as impersonation, replay, denial of services, and man-in-the-middle attacks have become enormous. Therefore, in order to resist against such attacks, the design of secure remote-user authentication scheme is the key necessity.

(iii) Furthermore, due to some components of IoT devices like actuators and sensors that deal with the crucial data of users, IoT-based applications must provide more safety and security.

1.2. Our Contribution. In this article, we have proposed an identity-based anonymous three-party authenticated protocol for IoT infrastructure. The main contributions of this article are as follows:

(1) We have presented a three-party identity-based authentication for the secure communications among users in an IoT infrastructure. The proposed identity-based scheme is designed using simple operations such as XOR, hash, and point multiplication.

(2) The proposed protocol enables mutual authentication between users and gateway for establishing and sharing the session key.

(3) User’s personal credentials such as email and phone are used to generate a public key.

(4) The proposed scheme ensures the secrecy of identity such that the identity is only revealed to gateway for
authentication purpose. No adversary can get the identity.

1.3. Paper Organization. The rest of the paper is organized as follows. The related work is discussed in Section 2. The preliminaries related to our paper are presented in Section 3. The generic security issues in IoT architecture are delineated in Section 4. Our introduced scheme and detailed description are given in Section 6. Section 7 presents the respective security analysis formally and informally. Thereafter, a performance comparison is highlighted in Section 8. In the end, concluding remarks are given in Section 9.

2. Related Work

The password-based authentication key exchange (PAKE) scheme [20–26] is one of the most generally known authentication key exchange (AKE) schemes, which can also be divided into three-party [27–30], two-party, and so on. In the AKE schemes, the three-party authentication key exchange (3PAKE) scheme based on password has the features of easy system maintenance, simple password, and strong expansibility. The 3PAKE scheme is extensively used in the network of modern communication. However, it is determined that the password has low entropy secret value and also prone to password guessing attack, due to the built-in issues related to the password. Therefore, due to the various problems faced by PAKE schemes, this paper reviews the identity-based schemes and introduces a three-party identity-based authentication key exchange scheme for enhancing the security.

The identity-based cryptography (IBC) [17] was developed in order to mitigate various issues associated with the conventional public key cryptography and PAKE schemes. The IBC applies the attributes of the user such as phone numbers or email addresses as public keys in order to diminish the difficulty of digital certificates, while the private key generator (PKG) creates the private keys. Therefore, the identification of user keys is critical and does not require to be revoked. Since then, the utilization of IBC remains popular for designing remote user authentication schemes. So, we review various identity-based schemes in order to find the research gap and security issues in the different infrastructures of the Internet of Things (IoT) such as edge and fog computing.

Roman et al. [31] presented the comparative summary of various security issues, challenges, and appropriate solutions for mobile edge computing (MEC) and fog computing. The readers who are interested in the details of privacy and security problems in the environment of fog computing for IoT, MEC, and mobile cloud computing (MCC) can consult [32–35], respectively. The literature emphasized the requirement of a secure mechanism for authentication. Yang and Chang [36] proposed an identity-based authentication key agreement (AKA) scheme using elliptic curve cryptosystem (ECC) for mobile devices. However, Yoon and Yoo [37] analyzed that the scheme [36] cannot resist masquerading attack and does not offer perfect forward secrecy. A pairing-free AKA scheme based on identity is introduced by Cao et al. [38] with a minimum exchange of messages. However, Cao et al. [38] fail to offer the user untraceability and anonymity like Yang and Chang’s scheme.

Tsai and Lo [39] introduced another authentication scheme based on identity for the distributed services of MCC. Their scheme uses bilinear pairing which causes high computation, but bilinear computation is performed by the server, which has usually more computing power. However, Jiang et al. [40] analyzed that a server impersonation attack cannot be resisted by their scheme [39], and also, it does not offer an appropriate mechanism of mutual authentication. Jiang et al. did not propose any improved solution, although various solutions were proposed in [41, 42].

Yang et al. [43] introduced an ECC-based scheme having the features of user untraceability and anonymity for the environment of MCC. In their scheme, a number of pseudo-IDs are assigned to a user, as well as each pseudo-ID is assigned a family of secret keys. The Access Service Network Gateway (ASN-GW) executes the predistribution process of keys. However, for each registered user, the ASN-GW requires to engender a large number of pseudo-IDs. So, the corresponding secret keys and many pseudo-IDs need to be stored by the mobile user which is impractical due to the constrained resources of mobile devices and also includes scalability issues.

Ibrahim [44] introduced an authentication scheme for the environment of fog computing, in which fog node and fog user authenticate each other. In their scheme [44], the public key infrastructure (PKI) is used to establish the secure communication channel between mobile users and registration authority, while symmetric encryption is utilized to protect the communication between fog nodes and mobile users. In their scheme, all the fog users’ regenerated secret keys are required to be stored by fog node which is also infeasible. Moreover, untraceability and anonymity are not guaranteed by their scheme. A mobile user authentication scheme is introduced by He et al. [45] for multiserver infrastructure. Their scheme uses self-certified public key cryptography which is basically identity-based cryptography. In 2017, a privacy-aware authentication scheme is introduced by Xiong et al. [46] for MCC services.

In 2019, Zhu and Geng [47] presented a three-party dynamic identity-based key exchange scheme. In 2019, Renuka et al. [48] crypt analyzed and found some attacks such as node capture, user phishing, and denial of service attacks in a three-factor authentication scheme devised by Das et al. [49] and presented an enhanced three-factor authentication scheme. Many other three-party schemes for the IoT environment have been presented [50, 51] but still lack major security features and not suitable for resource constraint environment. In 2020, Ramadan et al. [52] presented an identity-based authentication scheme for 5G systems. Kumar et al. [53] proposed an identity-based authentication scheme for cloud computing in 2020. Recently, Farjana et al. [54] presented identity-based schemes; moreover, many other schemes [55–60] are presented recently. In general, the design of efficient and secure identity-based authentication schemes is still a challenging task. In this article, we propose the identity-based lightweight
remote user authentication scheme for the IoT infrastructure in order to offer the secure and efficient communication, so that all the flaws in the discussed literature can be minimized.

3. Preliminaries

This section includes the basics of elliptic curve cryptography such as one-way hash function, collision resistance, and threat model. The common notations used throughout the research work in Table 1 are also given in this section.

3.1. Elliptic Curve Cryptography (ECC). There is a lot of public key cryptography techniques like Rivest Shamir Adleman (RSA), Diffie Hellman, and Digital Signature Algorithm (DSA). The majority of these techniques are heavy in computation. The ECC system’s robustness can be anticipated based on the complexity of ECDLP (Elliptic Curve Discrete Logarithm Problem). Suppose \( E_p(e, f): h^2 + eg + f \mod p \), ECC is based on random points chosen on an elliptic curve, whereas \( e, f \in Z_p \) and \( 4e^3 + 27f^2 \mod p \neq 0 \) for \( p \) (large prime number). The curve is defined by both the points \( e, f \). The former equation must be verified by the points \( (g, h) \) over \( E_p(e, f) \). Through repetitive addition, scalar multiplication is achieved such as \( qS = S + S + S + \cdots + S \) (\( q \) times), where \( S \) is a point over \( E_p(e, f) \) and \( q \in F_p \). The field parameters \( (p, e, f, S, q) \) belongs to the field \( (F_p) \).

Definition 1. Discrete logarithm problem aimed at ECDLP.

Two specified random points \( S, R \in E_p(e, f) \), calculate a scalar \( (q) \) such that \( S = qR \). During the polynomial time \( (t) \), the benefits of \( \mathcal{U}_{Adv} \) is given as: \( \text{Adv}_{\mathcal{U}_{Adv}}^{ECDLP}(t) = \text{Prb}[(\mathcal{U}_{Adv})((S, R)) = x : x \in Z_p] \). The supposition of ECDLP states that \( \text{Adv}_{\mathcal{U}_{Adv}}^{ECDLP}(t) \leq \epsilon \).

3.2. One-Way Hash Function. Hash functions are used to get an output \( f(\cdot) \) of fixed size. Hash functions can be applied to any random argument or string \( y \) of any size such as \( f = h(y) \). A small change in \( y \) can make a huge difference in resultant \( f \). Subsequent parameters should be found for a secure function of hash.

(1) If \( y \) is defined, then it is not difficult to calculate \( f = h(y) \)
(2) If \( f \) = \( h(y) \) is defined, then it is impossible to find out \( y \)
(3) If \( h(y_1) = h(y_2) \) is defined, then it is a tiresome task to know the specific input \( y_1, y_2 \). The defined property is also referred to as collision resistance

Definition 2. Collision resistance characteristics aimed at hash function.

Hash function \( h(\cdot) \) is secured by predefined collision resistance. The chances that an adversary \( (\mathcal{U}_{Adv}) \) can find out a couple \( (y_1 \neq y_2) \) as \( h(y_1) = h(y_2) \) is defined as Ad \( \text{Prb}_{\mathcal{U}_{Adv}}(t) = \text{Prb}[(y_1, y_2) \in \mathcal{U}_{Adv} : (y_1 \neq y_2) \) and \( h(y_1) = h(y_2) ] \), whereas \( \mathcal{U}_{Adv} \) is allowed to select a couple \( y_1, y_2 \) randomly. \( \mathcal{U}_{Adv} \)'s advantage is determined over a random selection in polynomial time \( (t) \). Collision resistance is stated as \( \text{Adv}_{\mathcal{U}_{Adv}}^{\lesssim} \leq \epsilon \), whereas \( \epsilon>0 \) is an adequately small value.

3.3. Identity-Based Cryptography (IBC). IBC was introduced by Shamir in 1984 [17]. It is one of the types of public key cryptography. IBC has the following properties:

(1) Identity-based cryptosystems use user’s personal credentials such as email, name, or phone number for deriving public/private keys
(2) The public key is generated by predefined user’s identity or personal credentials
(3) Third parties or trusted authorities as PKG are responsible for the generation of private keys
(4) PKG generates identity-based certificates, and using these certificates, encryption, generation digital signatures, and mutual authentication are performed
(5) IBC is cost-efficient in terms of transfer and storage of keys as compared to other traditional PKI systems

3.4. Threat Model. In order to understand the capabilities of an adversary, we have used Doele-Yao’s [61] threat model. The capabilities of \( \mathcal{U}_{Adv} \) are as follows:

(1) \( \mathcal{U}_{Adv} \) has full control over the public channel

| Table 1: Common notations. |
|-----------------------------------------------|
| Notation | Description |
|-----------------|-------------|
| \( \mathcal{U}_i \) | \( \mathcal{U}_i \)'th remote user of the system |
| ID \( _j \) | \( \mathcal{U}_j \)'s identity |
| \( \mathcal{F}\mathcal{P}\mathcal{M}_i \) | \( \mathcal{U}_i \)'s tamper proof on-board memory/storage |
| \( \mathcal{GW}\mathcal{N} \) | Gateway node |
| ID \( _{\mathcal{GW}N} \) | \( \mathcal{GW}\mathcal{N} \)'s identity |
| \( x \) | \( \mathcal{GW}\mathcal{N} \)'s secret key |
| Pub = \( xG \) | \( \mathcal{GW}\mathcal{N} \)'s public key |
| \( Ep(e, f) \) | An elliptic curve |
| \( h(\cdot) \) | One-way function |
| \( \oplus \) | XOR operator |
| \( || \) | Concatenation operator |
| \( \Rightarrow \) | Secure channel |
| \( \rightarrow \) | Public channel |
| \( \mathcal{U}_{Adv} \) | Adversary |
4. Security Issues in IoT

In the design of IoT applications, IoT’s security is the most important thing. Therefore, the major challenge which requires serious consideration is to provide strong security for IoT. In the Internet world, IoT has a very bright future. Thus, for the realization of services of modern technologies and their benefits, security requirements such as authentication and privacy are much important.

Therefore, subsequent issues must be handled with consideration.

4.1. Common Vulnerabilities in IoT Architecture. The devices of IoT existing in an abandoned environment require active inspection of every feasible condition in which the attacker can attack on devices of IoT. As per detailed scrutiny, we can wrap up the vulnerabilities of IoT as follows:

(i) **Impersonation Attack.** A malignant hacker can masquerade as a service provider or a user by responding to an authentic request from old transmission between any two legal entities. Therefore, a malignant hacker can enjoy the same services as a legitimate user or service provider.

(ii) **Denial of Service Attack.** The attacker by flooding the network with previous login requests or information exchanged between two entities can reduce the network’s performance and can make the services unavailable.

(iii) **Eavesdropping Attack.** The attacker can listen to private communication on a public channel and can misuse it later to attack a user or server.

(iv) **Man-in-Middle Attack (MITM).** The adversary can forge the message exchanged between the gateway and user, later using this information can impersonate as a legal gateway/server and user using different techniques.

(v) **Parallel Session Attack.** An attacker can eavesdrop the messages between the system of IoT and then attempts to generate a session to get the old data.

(vi) **Gateway Node Bypassing Attack.** To obtain IoT sensitive information and services without authentication of a gateway, an attacker can try to access the system by bypassing the gateway.

(vii) **Stolen Smart Device Attack.** An attacker can derive the user’s personal data from smart devices and utilize it later to impersonate as a legitimate user of the network.

(viii) **Offline Guessing Attack.** Using an offline dictionary attack, the adversary can attempt to get access to the system of IoT by guessing all possible passwords.

4.2. Security Feature Requirements in IoT. Many security features must be incorporated while designing the authentication schemes. The following is a list of important security features that can be exploited to design an efficient and secure scheme.

(i) **User Anonymity.** The participant’s identity must be secured such that if an attacker tries to eavesdrop the message and intercept message during the login and authentication stage. If the identity is revealed, then the attacker can misuse it and the user’s privacy is breached.

(ii) **Mutual Authentication.** Two participating entities must mutually authenticate each other to avoid security threats.

(iii) **Availability.** Whenever a user requires to access the system, all IoT resources should be available.

(iv) **Confidentiality.** The user’s personal and sensitive information must be protected and should be visible only to legitimate users.

(v) **Scalability.** The system of authentication must be responsive to the modification occurring in the network, and the system should be allowed to grow dynamically according to the modifications that are being happened.

(vi) **Forward Secrecy.** The access to entities in any authentication scheme is granted by sharing the session key. That is why the old session keys cannot be used to initiate a new session.

(vii) **Resistance to Attacks.** A secure authentication scheme must resist the major security threats such as the Distributed Denial of Services (DDoS), MITM, impersonation, and stolen verifier attack.

5. System Setup

In an IoT infrastructure, gateway plays an important role to ensure the security in the network. Our presented model consists of two participants as shown in Figure 1, such as IoT nodes and gateway. In general, IoT nodes have limited resources in terms of computation, communication, and power. The IoT nodes aimed to communicate with each other by authenticating via a trusted gateway. As in Figure 1, IoT node (1) and IoT node (a) initiate a session...
by sending a login request to the gateway. The gateway is responsible for establishing a secure communication between IoT nodes. Once the IoT nodes are authenticated by the gateway, the IoT nodes can then securely communicate with each other. Due to the public nature and limited resources, the IoT nodes face several security and privacy challenges. The generic three-party IoT infrastructure for remote-user authentication is demonstrated in Figure 1. Suppose a remote user wants to communicate with another remote user, then they both have to pass the authentication process. For this purpose of authentication, each entity will be verified through gateway node \( GWN \). If both entities have been authenticated, then the \( GWN \) sends a challenge message to both entities. Upon receiving the challenge message, each entity authenticates the \( GWN \) and computes a session key. In the end, both users agreed on this common shared session key.

6. The Proposed Scheme

In this section, we elaborated on our proposed identity-based scheme which upholds user anonymity, user untraceability, perfect forward secrecy, key agreement, and mutual authentication. The introduced scheme comprises of these phases: Section 6.1 the registration phase and Section 6.2 the login and authentication phase. These two phases are described below in detail.

6.1. Registration Phase. If a user \( U_a \) wants to communicate with another user \( U_b \), then they both have to pass the authentication process. For authentication, each entity will be verified by \( GWN \). If both entities are authenticated, then they can share the session key. The complete registration process of the user \( U_i \) of the proposed scheme is described in detail in this subsection. Figure 2 shows the registration phase of the proposed scheme. The registration process consists of the following steps:

**RG-Step 1.** The user \( U_i \) chooses his/her ID, and the arbitrary number \( l_i \).

**RG-Step 2.** Upon receiving the registration requests \( (ID_i, h(ID_i \oplus l_i)) \) from \( U_i \), then calculates the following values:

\[
\begin{align*}
  MID_i & = h(ID_i), \\
  V_i & = h(ID_i \oplus l_i), \\
  Y_i & = V_i \oplus h(ID_i \oplus l_i)
\end{align*}
\]

**RG-Step 3.** Upon receiving \( Y_i \) from \( GWN \), \( U_i \) calculates the following values:

\[
\begin{align*}
  V_i & = Y_i \oplus h(ID_i \oplus l_i), \\
  Z_i & = l_i \oplus ID_i, \\
  A_i & = h(V_i \parallel ID_i \parallel l_i)
\end{align*}
\]

After calculating these values, stores \( \{A_i, Y_i, Z_i\} \) in TPM of the mobile device. The registration process of the user \( U_i \) of the proposed scheme is described in detail in this subsection. Figure 2 shows the registration phase of the proposed scheme. The registration process consists of the following steps:

**RG-Step 1.** The user \( U_i \) chooses his/her ID, and the arbitrary number \( l_i \).

**RG-Step 2.** Upon receiving the registration requests \( (ID_i, h(ID_i \oplus l_i)) \) from \( U_i \), then calculates the following values:

\[
\begin{align*}
  MID_i & = h(ID_i), \\
  V_i & = h(ID_i \oplus l_i), \\
  Y_i & = V_i \oplus h(ID_i \oplus l_i)
\end{align*}
\]

**RG-Step 3.** Upon receiving \( Y_i \) from \( GWN \), \( U_i \) calculates the following values:

\[
\begin{align*}
  V_i & = Y_i \oplus h(ID_i \oplus l_i), \\
  Z_i & = l_i \oplus ID_i, \\
  A_i & = h(V_i \parallel ID_i \parallel l_i)
\end{align*}
\]

6.2. Login and Authentication Phase. The complete process of login and authentication of the introduced scheme as presented in Figure 3 is elaborated in this subsection which consists of the following steps:

**AT-Step 1.** Both \( U_a \) and \( U_b \) input their identity \( (ID_a, ID_b) \), respectively. Then, \( U_a \) calculates the following values on the basis of the credentials stored in tamper proof on-board memory TPM of the mobile device:

\[
\begin{align*}
  l_{a1} & = Z_a \oplus ID_a, \\
  V_a & = Y_a \oplus h(ID_a, ID_b) \\
  A_a & = h(V_a \parallel ID_a \parallel l_{a1})
\end{align*}
\]
Further computation generates a random number $l_{a2}$ and calculates the following values:

$$Q_a = l_{a2}G,$$

$$\text{PID}_a = (\text{ID}_a \| \text{MID}_a) \oplus l_{a2}\text{Pub},$$

$$\text{auth}_a = h(\text{ID}_a \| \text{MID}_a \| \text{ID}_{GWN} \| V_a),$$

whereas $U_b$ calculates the following values on the basis of the credentials entered during the registration process.

$$l_{b1} = Z_b \oplus \text{ID}_b,$$

$$V_b = Y_b \oplus h(\text{ID}_b \oplus l_{b1}),$$

$$A_b = h(V_b \| \text{ID}_b)$$

Further, $U_b$ generates a random number $l_{b2}$ and computes the following values:

$$Q_b = l_{b2}G,$$

$$\text{PID}_b = (\text{ID}_b \| \text{MID}_a) \oplus l_{b2}\text{Pub},$$

$$\text{auth}_b = h(\text{ID}_b \| \text{MID}_a \| \text{ID}_{GWN} \| Y_b \oplus h(\text{ID}_b \| l_{b1})).$$

After calculating these values, $U_a$ and $U_b$ send login request $\{\text{auth}_a, Q_a, \text{PID}_a\}$ and $\{\text{auth}_b, Q_b, \text{PID}_b\}$, respectively, towards the gateway.

AT-Step 2. After receiving login requests from $U_a$, the GWN calculates the following values for $U_a$:

$$xQ_a = l_{a2}xG = l_{a2}\text{Pub},$$

$$(\text{ID}_a \| \text{MID}_b) = \text{PID}_a \oplus l_{a2}\text{Pub},$$

$$\text{MID}_a = h(\text{ID}_a),$$

$$\text{auth}_a = h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{GWN} \| h(x \| \text{MID}_a))$$

Also, calculate the following values for $U_b$ upon receiving the login request $\{\text{auth}_b, Q_b, \text{PID}_b\}$

$$xQ_b = l_{b2}xG = l_{b2}\text{Pub},$$

$$(\text{ID}_b \| \text{MID}_a) = \text{PID}_b \oplus l_{b2}\text{Pub},$$

$$\text{MID}_b = h(\text{ID}_b),$$

$$\text{auth}_b = h(\text{ID}_b \| \text{MID}_a \| \text{ID}_{GWN} \| h(x \| \text{MID}_b))$$

Further, the $\mathcal{N}$ generates $l_{GWN}$ and calculate the following values as:
Login and authentication phase:

U_a inputs ID_a
l_a1 = Z_a ⊕ ID_a
V_a = Y_a ⊙ h(ID_a ⊙ l_a1)
A_a = \frac{1}{2} h(V_a||ID_a||l_a2)
Generate a random number l_a2
Q = l_a2G
PID_a = (ID_a||MID_b) ⊕ l_a2pub
auth_a = h(ID_a||MID_b||ID_GWN||V_a)

U_b inputs ID_b
l_b1 = Z_b ⊕ ID_b
V_b = Y_b ⊙ h(ID_b ⊙ l_b1)
A_b = \frac{1}{2} h(V_b||ID_b||l_b2)
Generate a random number l_b2
Q = l_b2G
PID_b = (ID_b||MID_a) ⊕ l_b2pub
auth_b = h(ID_b||MID_a||ID_GWN||V_b)

Calculation for U_a
\text{xQ} = l_a2xG = l_a2Pub
(ID_a||MID_a) = PID_a ⊙ l_a2Pub
MID_a = h(ID_a)
auth_a = \frac{1}{2} h(ID_a||MID_a||ID_GWN||h(x||MID_a))

Calculation for U_b
\text{xQ} = l_b2xG = l_b2Pub
(ID_b||MID_b) = PID_b ⊙ l_b2Pub
MID_b = h(ID_b)
auth_b = \frac{1}{2} h(ID_b||MID_b||ID_GWN||h(x||MID_b))

Generates l_GWN
M_{GWN} = (ID_GWN||x||V_GWN)

N_{GWN1} = M_{GWN} ⊕ V_a
N_{GWN2} = M_{GWN} ⊕ V_b
auth_{GWN1} = h(ID_a||ID_GWN||V_a||M_{GWN})
auth_{GWN2} = h(ID_b||ID_GWN||V_b||M_{GWN})

M_{GWN} = N_{GWN1} ⊕ V_a
auth_{GWN1} = \frac{1}{2} h(ID_a||ID_GWN||V_a||M_{GWN})
k = l_a2Q_b
SK_{ab} = h(MID_a||MID_b||ID_GWN||k)

M_{GWN} = N_{GWN2} ⊕ V_b
auth_{GWN2} = \frac{1}{2} h(ID_b||ID_GWN||V_b||M_{GWN})
k = l_b2Q_a
SK_{ab} = h(MID_a||MID_b||ID_GWN||k)

SK = h(MID_a||MID_b||ID_GWN||k)

Figure 3: Login and authentication process of U_i.
Subsequent communication.

WN sends values along with the session key:  

\[ \text{auth}_\text{GWN1} = h(\text{ID}_a \oplus \text{ID}_\text{GWN} \oplus V_a \Vert M_{\text{GWN}}), \]

\[ \text{auth}_\text{GWN2} = h(\text{ID}_b \oplus \text{ID}_\text{GWN} \oplus V_b \Vert M_{\text{GWN}}) \]

7. Security Analysis

This section presents the formal and informal security analysis of the proposed scheme. We have used Real-Or-Random (ROR) [64] in order to prove the security of the proposed scheme. Furthermore, informal security analysis shows that the proposed scheme provides resilience against all known attacks.

7.1. Informal Security Analysis. The security of the proposed scheme is analyzed informally in this section. The informal security analysis represents the proposed scheme’s correctness and ensures that it resists various attacks.

7.1.1. Identity Security. The abundance of resource-constrained devices among the advanced communication infrastructures has made the existing protocol incompatible for diverse real-time applications like IoT and smart grid. Therefore, the demand for lightweight solutions is on the peak, IBC is one of them. It is a new way to solve these problems without any complex computation. That is why it has grabbed the attention of the researchers. For achieving confidentiality, the personal information for identification should be sent via a secure channel. The respective users have the private key corresponding to his/her own ID. Also, identity security includes the availability of identity. If a user’s identity is revoked by GWN, even then, the U has control over his ID and the relevant claims, which states that the user still can use his/her ID in other applications.

7.1.2. Key Agreement. After completing the successful process of mutual authentication, a common session key SK is shared between the users. This shared session key is established through \( SK_{ab} = h(\text{MID}_a \Vert \text{MID}_b \Vert k \Vert ID_{\text{GWN}} \Vert k) \). Hence, the scheme offers a successful key agreement.

7.1.3. Mutual Authentication. In our introduced scheme, the \( \mathcal{W}N \) can authenticate \( \mathcal{U}_a \) by verifying \( \text{auth}_\text{GWN} = h(\text{ID}_a \Vert \text{ID}_\text{GWN} \Vert V_a \Vert M_{\text{GWN}}) \). The values ID, MID, ID, V, are only known to valid \( \mathcal{U}_a \), as an adversary cannot calculate all these values. So, only legitimate user \( \mathcal{U}_a \) can be authenticated by \( \mathcal{W}N \). Likewise, \( \mathcal{W}N \) authenticates the other user. Similarly, user \( \mathcal{U}_a \) can also authenticate \( \mathcal{W}N \) by verifying \( h(\text{ID}_a \Vert M_{\text{GWN}}) \). The values ID, ID, MID, MID, V, are only known to valid \( \mathcal{U}_a \). As adversary cannot calculate these values, only the legitimate \( \mathcal{W}N \) can be authenticated by \( \mathcal{U}_a \). Likewise, other users can authenticate \( \mathcal{W}N \). Thus, it is proved that our introduced scheme offers mutual authentication between users and \( \mathcal{W}N \).

7.1.4. User Untraceability. During the login and authentication stage, the identity of \( \mathcal{F} \mathcal{D}_a \) of user \( \mathcal{U}_a \) is not transmitted in plain text; instead, the pseudoidentity PID is sent over the public channel. Furthermore, the identity of \( \mathcal{U}_a \) is not stored in temper proof onboard memory/storage. That is why adversary cannot retrieve the identity of \( \mathcal{U}_a \) without having the private key. So, our proposed scheme provides user untraceability.

7.1.5. User Untraceability. During the design of the authentication scheme, untraceability is considered as an important factor. The proposed scheme provides user’s untraceability because in each login session \( \mathcal{U}_a \) computes unique PID, it is clear that \( \mathcal{U}_a \) does not transmit the same dynamic identity instead every time session-specific random number is used to calculate PID. So, it cannot be guessed by any adversary that two different sessions are established by the same or different users.

7.1.6. Perfect Forward Secrecy. In our introduced scheme, if \( \mathcal{U}_{A_{ab}} \) is able to know the secret parameters such as the secret key of \( \mathcal{W}N \), even then, he cannot determine the former session keys. In the proposed scheme, arbitrary numbers \( l_{a1}, l_{a2} \) are used to compute the valid value of k that is further used in the computation of SK. Due to the usage of random numbers, different session keys are generated in each session. So, even after getting the secret parameter, the adversary cannot guess the previous session keys.
7.1.7. Backward Secrecy. In the introduced scheme, if \( \mathcal{U}_{A_{uwb}} \) is able to find the secret parameters of \( \mathcal{F}_W \mathcal{N} \), even then, he cannot find the future sessions. In the proposed scheme, the calculation of valid \( S_{k_{ab}} \) requires arbitrary number \( \{l_{u_1}, l_{u_2}\} \). Due to these random numbers, the session key is specific for every session; thus, \( \mathcal{U}_{A_{uwb}} \) cannot find future session keys.

7.1.8. Privileged Insider and Stolen Verifier Attack. During the registration phase, \( \mathcal{U}_{u} \) transmit ID\(_{1}\) and \( l_{u} \) through the private channel to \( \mathcal{F}_W \mathcal{N} \), where arbitrary number \( l_{u} \) is generated by \( \mathcal{U}_{u} \). Furthermore, for \( \mathcal{U}_{u} \)'s identity, no table is preserved, for authentication \( \mathcal{F}_W \mathcal{N} \) uses \( x \) his secret key. Thus, no insider \( \mathcal{U}_{A_{uwb}} \) can get access to the user’s identity and credentials. Hence, the introduced scheme resists stolen verifiers and privileged insider attacks.

7.1.9. User Masquerading Attack. Suppose \( \mathcal{U}_{A_{uwb}} \) tries to masquerade a legal \( \mathcal{U}_{u} \) by means of sending a legal login request message on behalf of \( \mathcal{U}_{u} \) to the \( \mathcal{F}_W \mathcal{N} \). In order to produce an original login message \( \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\} \), the adversary needs to calculate valid \( \text{auth}_{\mathcal{F}_W \mathcal{N}} = h(\text{ID}_{a}||\text{MID}_{\mathcal{F}_W \mathcal{N}}||V_{a}) \). It is not possible for the adversary to calculate \( \text{auth}_{\mathcal{F}_W \mathcal{N}} \) because \( \mathcal{U}_{A_{uwb}} \) does not know \( \text{ID}_{a} \) of \( \mathcal{U}_{u} \). Likewise, the other user is also secured from impersonating by an adversary. So, the proposed scheme has the ability to withstand the user masquerading attack.

7.1.10. \( \mathcal{F}_W \mathcal{N} \) Masquerading Attack. Suppose an attacker \( \mathcal{U}_{A_{uwb}} \) tries to impersonate a legal server \( \mathcal{F}_W \mathcal{N} \) by means of sending a legal challenge message on the behalf of \( \mathcal{F}_W \mathcal{N} \) to the user. In order to produce an original challenge message \( \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\} \), the adversary needs to calculate the valid \( \text{auth}_{\mathcal{F}_W \mathcal{N}} = h(\text{ID}_{a}||\text{MID}_{\mathcal{F}_W \mathcal{N}}||V_{a}) \). However, this operation is computationally expensive because for determining \( V_{a} = h(x||\text{MID}_{a}) \), it needs a private key of \( \mathcal{F}_W \mathcal{N} \). So, the proposed scheme has the ability to withstand the user masquerading attack.

7.1.11. Man-in-the-Middle Attack (MITM). Suppose \( \mathcal{U}_{A_{uwb}} \) forges the login message \( \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\} \) sent by \( \mathcal{U}_{u} \) to \( \mathcal{F}_W \mathcal{N} \), still, any tampering in the login request message will easily be identified while determining \( \text{auth}_{\mathcal{F}_W \mathcal{N}} = h(\text{ID}_{a}||\text{MID}_{\mathcal{F}_W \mathcal{N}}||\text{ID}_{\mathcal{F}_W \mathcal{N}}(V_{a})) \). \( \mathcal{U}_{A_{uwb}} \) requires the user’s identity which is unknown to adversary. Likewise, the other user is also secure against this attack. So, the proposed scheme is secured against MITM.

7.1.12. Replay Attack. If \( \mathcal{U}_{A_{uwb}} \) intercepts the request message \( \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\} \) of \( \mathcal{U}_{u} \) and later replays the intercept message, the calculation of \( Q_{a} \) and \( \text{PID}_{\mathcal{F}_W \mathcal{N}} \) includes a random number \( l_{a} \) which is session specific. Because of the random number, the values of the entities will always be different for every session. Hence, a replay attack is not possible on the proposed scheme.

7.1.13. Parallel Session Attack. Suppose the scheme’s parallel session is tried to be constructed by \( \mathcal{U}_{A_{uwb}} \), but this scenario is not possible in the proposed scheme as a unique identity is utilized. Therefore, even one valid session cannot be run by \( \mathcal{U}_{A_{uwb}} \) to masquerade a legitimate user. Thus, a parallel session attack can be efficiently resisted by the proposed scheme.

7.1.14. No Clock Synchronization. In the proposed scheme, session-specific random numbers are used in every session instead of a time stamp. So, no clock synchronization is required.

7.2. Formal Security Analysis. In this subsection, we prove that our scheme is AKA-Secure if the ECDHP is a hard problem. We present this proof under the (BRP) [64, 65] and Abdalla et al.’s [66] security model.

**Theorem 2.** Let the proposed scheme be denoted as \( \mathcal{P}_{p} \). If \( \mathcal{U}_{A_{uwb}} \) is an attacker who builds at most \( q_{\text{send}} \) Send queries, \( q_{\text{rel}} \) Reveal queries, \( q_{\text{exe}} \) Execute queries, \( q_{\text{hash}} \) Hash queries and succeed the game having benefit \( \text{Adv}_{\mathcal{P}_{p}}^{\text{AKA}}(\mathcal{U}_{A_{uwb}}) \), then an algorithm that should be existed, which can efficiently resolve ECDHP hard problem on group \( G \) having benefit \( \text{Adv}_{G}^{\text{ECDHP}} \), where

\[
\text{Adv}_{\mathcal{P}_{p}}^{\text{AKA}} \leq \frac{q_{\text{send}}}{2^{13}} + \frac{q_{\text{rel}} + q_{\text{exe}}}{2^{13}} + \frac{q_{\text{hash}}}{2^{13}} + \frac{2q_{\text{exe}}}{2^{13}} + 2q_{\text{hash}}\text{Adv}_{G}^{\text{ECDHP}}
\]

\[(13)\]

**Proof.** Suppose, for the base point \( G \) and elliptic group \( E_{p} \) there exists an ECDHP instance \( (P, aP, bP) \), we make a challenge \( \mathcal{C}_{r} \), who wishes to calculate \( abP \) using \( \mathcal{U}_{A_{uwb}} \) as a function. The function that is taken as an arbitrary oracle in the proposed scheme is referred to as hash \( h(\cdot) \). In order to record the hash queries and their answer, \( \mathcal{C}_{r} \) maintains a hash list and is referred to as \( L_{\text{hash}} \). To make it simple, we use three transcripts between entities, which are as follows:

\[
\begin{align*}
\mathcal{M}_{1} & = \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\}, \\
\mathcal{M}_{2} & = \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{b}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\}, \\
\mathcal{M}_{3} & = \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, Q_{b}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\}
\end{align*}
\]

\[(14)\]

After simulating the scheme, \( \mathcal{C}_{r} \) answers the queries questioned by \( \mathcal{U}_{A_{uwb}} \) as follows:

1. **Hash Query.** after getting the hash query with input \( m \) from \( \mathcal{U}_{A_{uwb}} \), \( \mathcal{C}_{r} \) scans the \( L_{\text{hash}} \) and returns \( r \) to \( \mathcal{U}_{A_{uwb}} \) if entry \( (m, r) \in L_{\text{hash}} \); otherwise, \( \mathcal{C}_{r} \) selects \( r \) randomly and gives \( r \) back to \( \mathcal{U}_{A_{uwb}} \) and adds \( (m, r) \) in to \( L_{\text{hash}} \)

2. **Send Query.**

   (i) \( \mathcal{C}_{r} \) simulates \( \mathcal{U}_{A_{uwb}} \)'s response in the following way after getting Send(\( \mathcal{U}_{A_{uwb}}, \text{Start} \)): selects a random numbers \( l_{u_1}, l_{u_2} \) and computes \( Q_{a} = l_{u_1} G \), \text{PID}_{\mathcal{F}_W \mathcal{N}} = (\text{ID}_{a}||\text{MID}_{\mathcal{F}_W \mathcal{N}}) \oplus l_{u_2} \), \text{auth}_{\mathcal{F}_W \mathcal{N}} = h(\text{ID}_{a}||\text{MID}_{\mathcal{F}_W \mathcal{N}}||V_{a}) \) and returns back \( \{\text{auth}_{\mathcal{F}_W \mathcal{N}}, Q_{a}, \text{PID}_{\mathcal{F}_W \mathcal{N}}\} \) as response

Theorem 2 states that the proposed scheme is AKA-Secure under the ECDHP assumption.
Upon the reception of query $\text{Send}(\mathcal{U}_b, (\text{auth}_a, Q_a, \text{PID}_a))$, assume that $\mathcal{U}_b$ is in accurate state. $\mathcal{U}_b$'s response is simulated by $\mathcal{C}_r$ as follows: selects random numbers $l_{g1, g2}$ and computes $Q_a = l_{g1}G$, $\text{PID}_a = (\text{ID}_a || \text{MID}_a) || l_{g2}2^p$, $\text{auth}_a = h(\text{ID}_a || \text{MID}_a || g_a || \text{MID}_b || V_b)$ and returns back $\{\text{auth}_a, Q_a, \text{PID}_a\}$ as response.

(3) Upon getting $\text{Send}(\text{GWN}((\text{auth}_a, Q_a, \text{PID}_a)))$, suppose that $\mathcal{GWN}$ is in true state, then the response of Send query is simulated by $\mathcal{C}_r$ as follows: computes $xQ_a = l_{g1}xG = l_{g1}2^p$, $(\text{ID}_a || \text{MID}_b) = \text{PID}_a \oplus l_{g2}2^p$, $\text{MID}_a = h(\text{ID}_a)$, and $\text{auth}_a = h(\text{ID}_a || \text{MID}_a || \text{GWN} || h(x || \text{MID}_a))$. Furthermore, GWN generates $l_{\text{GWN}}$ and computes $N_{\text{GWN}} = M_{\text{GWN}} \oplus V_{\text{GWN}}$, $\text{auth}_{\text{GWN}} = h(\text{ID}_a || \text{GWN} || V_a || M_{\text{GWN}})$ and response back with $\{\text{auth}_{\text{GWN}}, Q_a, N_{\text{GWN}}\}$.

(4) After receiving query $\text{Send}(\text{GWN}, (\text{auth}_b, Q_b, \text{PID}_b))$ and assuming $\mathcal{GWN}$ as a correct state, $\mathcal{C}_r$ simulates $\mathcal{GWN}$'s response as follows: computes $xQ_b = l_{g1}xG = l_{g1}2^p$, $(\text{ID}_b || \text{MID}_a) = \text{PID}_b \oplus l_{g2}2^p$, $\text{MID}_b = h(\text{ID}_b)$ and verifies $\text{auth}_b = h(\text{ID}_b || \text{MID}_a || \text{GWN} || h(x || \text{MID}_a))$. Furthermore, generate $l_{\text{GWN}}$ and compute $N_{\text{GWN}} = M_{\text{GWN}} \oplus V_{\text{GWN}}$, $\text{auth}_{\text{GWN}} = h(\text{ID}_a || \text{GWN} || V_a || M_{\text{GWN}})$, and return $\{\text{auth}_{\text{GWN}}, Q_a, N_{\text{GWN}}\}$ as response.

(5) In the end, the session key is shared among the participants if checks $\text{auth}_{\text{GWN}} = h(\text{ID}_a || \text{GWN} || V_a || M_{\text{GWN}})$ and $\text{auth}_{\text{GWN}} = h(\text{ID}_b || \text{GWN} || V_a || M_{\text{GWN}})$ are hold true. Otherwise, the session will be terminated.

(iii) Execute Query. While getting execute query $(U_a, \text{GWN}, U_b)$, $\mathcal{C}_r$ simulates the send query as follows:

$$m_{U_a, g} = \text{Send}(\mathcal{U}_a, \text{Start}),$$

$$m_{U_b, g} = \text{Send}(\mathcal{U}_b, m_{U_a, g}),$$

$$m_{\mathcal{GWN}, U_b} = \text{Send}(\mathcal{GWN}, m_{U_a, g}, m_{U_b, g})$$

$\mathcal{C}_r$ returns $m_{U_a, g}$, $m_{U_b, g}$ and $m_{\mathcal{GWN}, U_b}$ as an answer.

(iv) Corrupt Query.

1. On getting a query $\text{Corrupt}(\mathcal{U}_b, \{\text{ID}_b\})$, $\mathcal{C}_r$ responds $V_i = h(x || \text{MID}_b)$

2. On receiving query $\text{Corrupt}(\text{GWN}, \{V_i\})$, $\mathcal{C}_r$ responds all information stored in temper proof onboard storage/memory

(v) Reveal Query: after getting a query $\text{Reveal}(U_i)$, $\mathcal{C}_r$ responds SK$_{ab}$ if the instance is accepted; otherwise, ⊥ will be responded.

Table 2: Desktop device specifications.

| Item        | Specification |
|-------------|---------------|
| Processor   | i7 3.60 GHz   |
| RAM         | 8 GB          |
| Operating system | Ubuntu       |

Table 3: Mobile device specifications.

| Item        | Specification |
|-------------|---------------|
| Mobile device | Vivo S1      |
| Processor   | Octa-Core     |
| ROM         | 128 GB        |
| RAM         | 6 GB          |

(vi) Test query: upon the reception of query $\text{Test}(U_i)$, toss up a coin $b \in \{0, 1\}$. The right session key SK$_{ab}$ will be returned if $b = 1$. Otherwise, an arbitrary value of the same size will be returned.

A game sequence $G_{a0}, G_{a1}, ..., G_{a5}$ is defined next. For every game $G_{a0}$, assume $S_i$ is an event that $U_{\text{Adv}}$ wins the game, which means $U_{\text{Adv}}$ predicted $b$ successfully. The following is the description:

Game $G_{a0}$: This game is the original attack game constructed by (BRP) [64, 65] and Abdalla et al.'s [66] security model, where the hash functions are modeled as a random oracle. According to the definition, we got:

$$\text{Adv}_{U_{\text{Adv}}} = 2P_r[S_b] - 1$$

Game $G_{a1}$: $G_{a1}$ is similar to $G_{a0}$, but the difference is that hash queries are entertained by scanning the $l_{\text{hash}}$ by $\mathcal{C}_r$. $G_{a1}$ remains indistinguishable from $G_{a0}$ until the queries are answered similarly in $G_{a0}$. Hence, we got

$$P_r[S_1] = P_r[S_0]$$

Game $G_{a2}$: $G_{a2}$ is similar to $G_{a1}$. But, the difference is that $G_{a2}$'s simulation terminates if subsequent events occur:

1. Event 1. Collision of hash queries during simulation.
2. Event 2. Collision on the simulation of transcripts $m_{U_a, g}, m_{U_b, g}, m_{\mathcal{GWN}, U_b}$. As per the concept of birthday paradox, we got $P_r[\text{Event}_2] \leq q^{1/2}$.

For transcript $m_{U_b, g}$, the collision probability of Event 2 is $(q_{\text{end}} + q_{\text{exe}})^3/2r^2$, while the probability
We got:

| Schemes                | No. of operations at Ui | No. of operation at GWN | Total no. of operations | Total time (ms) |
|------------------------|-------------------------|-------------------------|-------------------------|-----------------|
| Ours                   | 5 h(.) + 3 PM           | 4 h(.) + 2 PM           | 9 h(.) + 5 PM           | 44.0094         |
| He et al. [67]         | 6 h(.) + 4 PM           | 8 h(.) + 8 PM           | 14 h(.) + 12 PM         | 56.0296         |
| Challa et al. [68]     | 8 h(.) + 5 PM           | 4 h(.) + 4 PM           | 12 h(.) + 9 PM          | 72.0148         |
| Ma et al. [69]         | 4 h(.) + 3 PM           | 9 h(.) + 6 PM           | 13 h(.) + 9 PM          | 40.0253         |
| Taher et al. [70]      | 9 h(.)                  | 6 h(.)                  | 15 h(.)                 | 36.0062         |
| Chandrakar and Om [71] | 11 h(.) + 4 PM          | 6 h(.) + 4 PM           | 17 h(.) + 8 PM          | 76.0169         |
| Lu et al. [72]         | 8 h(.) + 4 PM           | 6 h(.) + 1 PM           | 14 h(.) + 5 PM          | 64.0088         |
| Mo and Chen [73]       | 13 h(.) + 1 PM          | 10 h(.)                 | 23 h(.) + 1 PM          | 60.0103         |

Table 4: Computation Cost of Proposed and Related Schemes.

| Schemes                | Communication structure |
|------------------------|-------------------------|
| Ours                   | $U_i \rightarrow GW \rightarrow U_i$ |
| He et al. [67]         | $U_i \rightarrow S_j \rightarrow GW \rightarrow S_j \rightarrow U_i$ |
| Challa et al. [68]     | $U_i \rightarrow TA \rightarrow S_j$ |
| Ma et al. [69]         | $U_i \rightarrow S_j \rightarrow CS \rightarrow S_j \rightarrow U_i$ |
| Taher et al. [70]      | $U_i \rightarrow GW \rightarrow U_i$, $S_j$ |
| Chandrakar and Om [71] | $U_i \rightarrow GW \rightarrow S_j \rightarrow GW \rightarrow U_i$ |
| Lu et al. [72]         | $U_i \rightarrow GW \rightarrow S_j \rightarrow U_i$ |
| Mo and Chen [73]       | $U_i \rightarrow GW \rightarrow S_j \rightarrow GW \rightarrow U_i$ |

Table 5: Communication structure.

of collision on the transcript $m_{u_a}, m_{u_b}$ is $(q_{send} + q_{exe})^2/2p$.

We got:

$$|P_r[S_2] - P_r[S_1]| \leq \frac{q_{Hash}}{2^{2l+1}} + \frac{(q_{send} + q_{exe})^2}{2p^2} + \frac{(q_{send} + q_{exe})^2}{2p}$$

(18)

Game $G_{a5}$: In $G_{a4}$, $G_{a5}$ is modified as follows:

(i) $U_a$ scans $L_{Hash}$ for ID$_a$. If the entries exist, then calculate \{auth$_a$, Q$_a$, PID$_a$\}.

(ii) GWN verifies the legitimacy of $U_a$. If it holds, then GWN scans for \{auth$_a$, Q$_a$, PID$_a$\} in the Send list. Otherwise, the session aborts. $G_{a5}$ will succeed if $U_{A_{ab}}$ guess the authentication parameters without a hash oracle. So

$$|P_r[S_2] - P_r[S_1]| \leq \frac{q_{send}}{2^l}$$

(20)

GAME $G_{a5}$: In $G_{a5}$, the $G_{a4}$ is modified as follows:

(i) $U_a$ randomly chooses $l_{a2}$ and computes $Q_a = l_{a2}G$, $PID_a = (ID_a \parallel MID_a) \oplus l_{a2}Pub$, and auth$_a = h(ID_a \parallel MID_a \parallel ID_{GWN} \parallel Y_a \parallel h(ID_a \parallel l_{a1}))$ and stores \{auth$_a$, Q$_a$, PID$_a$\} in $L_{Hash}$.

$h_a$, auth$_{GWN_1}$ and auth$_{GWN_2}$ without knowing the hash oracle. Thus, we got

$$|P_r[S_2] - P_r[S_1]| \leq \frac{q_{send}}{2^l}$$

(19)
Ub randomly selects lb and computes $Q_b = lbG$, $\text{PID}_b = (\text{ID}_b || \text{MID}_a) \oplus \text{lb}\text{pub}$, and $\text{auth}_b = h(\text{ID}_b || \text{MID}_a || \text{IDGWN} || \text{Y}_b \oplus h(\text{ID}_b || \text{lb}_{1}))$ and stores $\{\text{auth}_b, Q_b, \text{PID}_b\}$ in $H_{\text{hash}}$.

Now, the updated $G_{a5}$ is indistinguishable from $G_{a4}$ until $U_{A_{a5}}$ asks a hash oracle on $abP$, whose probability is $1/q_{\text{hash}}$. So

\[ |P_r[S_b] - P_r[S_b]| \leq q_{\text{hash}} \text{Adv}_{G}^{\text{ECDHP}} \quad (21) \]

GAME $G_{a6}$: In this game, if $U_{A_{a6}}$ asks a hash query for $abP$ then test query will be terminated.

The probability of obtaining the session key here is $q_{\text{hash}}/2^{l+1}$. So $U_{A_{a6}}$ has no advantage in $G_{a6}$. The resultant of all equations that we got is:

\[ \text{Adv}_{U_{A_{a6}}}^{\text{ECDHP}} \leq \frac{q_{\text{hash}}^2}{2^{2l+1}} + \frac{q_{\text{send}}^2}{2^{2l+2}} + \frac{(q_{\text{send}} + q_{\text{exe}})^2}{p} + q_{\text{exe}} \text{Adv}_{G}^{\text{ECDHP}} \quad (22) \]

### 8. Functionality Comparison and Performance Analysis

In this section, we compared our proposed scheme with related schemes [67–73] in terms of resource utilization (storage, communication, and computation cost) and security functionality. The detailed description is as follows.

#### 8.1. Computational Overhead Comparison

We have evaluated our scheme and related schemes to determine the computational efficiency. For this purpose, we have considered hash function $h(.)$ and point multiplication PM. Cryptographic operations have been implemented at the server end on a desktop device, whereas operations at $U_i$ end are...
implemented using a mobile device. The specifications of both devices are listed in Tables 2 and 3.

The time taken by hash and point multiplication on the system is 0.001032 and 0.002672 milliseconds (ms), respectively, whereas the time taken by hash and point multiplication on the system is 4 and 8 milliseconds (ms), respectively. The computation cost of the related and proposed schemes [67–73] is presented in Table 4. Table 4 shows that the proposed scheme requires 44.0094 ms for computation. The time required by [67–73] is also mentioned in Table 4.

If we present the Table 4 results graphically we can observe the proposed scheme is efficient in terms of computation as compared to [67, 68, 71–73] and slightly greater than [69, 70].

In Figure 4, the vertical axis (Y-axis) shows the time required in millisecond (ms), whereas schemes are presented on horizontal axis (X-axis). Figure 4 visually demonstrates the total time taken for the computation of the operations.

8.2. Communicational Overhead Comparison. We compared our proposed scheme with the related schemes [67–73] in terms of communicational expenses in this subsection. The communication structure of the proposed and related schemes [67–73] is demonstrated in Table 5 on the basis of scheme architecture. The communication structure in Table 5 shows the way in which communicating entities interact with each other and how they exchange messages. In Table 5, the symbol represents $U_i$: users, $S_j$: sensor node, $TA$: trusted authority, $CS$: server.

Considering the communication structure demonstrated the Table 5, we computed the communication cost as presented in Table 6. For conventional comparison, we assumed identities (ID, ID$_{GWN}$), random numbers, and point multiplication require 160 bits respectively, whereas we assumed 256 bits for hash, secrete, and public keys ($\text{x}, \text{Pub}$). The total bits required for communication by the proposed scheme is 2016 bits, whereas Table 6 shows the proposed scheme requires the least number of bits as compared to the related schemes [67–73].

The time taken for communication stated in Table 6 is graphically presented in Figure 5. The bits required for communication are displayed on the vertical axis (y-axis) and the schemes on the horizontal axis (x-axis). The proposed scheme requires less number of bits than [67–73] for communication.

8.3. Storage Overhead Comparison. The number of bits required to store parameters in smart devices (i.e., temper proof onboard memory/storage) is referred to as storage cost. In this subsection, we have compared our scheme with related schemes [67–73] for evaluating the storage efficiency. Table 7 depicts the storage cost comparison of proposed and related schemes. It is evident from the table that the proposed scheme’s storage cost is equal to [67] and less than [68–73].

The storage cost mentioned in Table 7 is graphically presented in Figure 6. In Figure 6, the vertical axis (y-axis) presents the number of bits, whereas the horizontal axis (x-axis) presents the schemes. Figure 6 clearly shows that the proposed scheme’s storage cost is less from [68–73] and equals to [67].

8.4. Security Functionality. In this subsection, we have discussed the proposed and related schemes in terms of security functionality. It is clear from Table 8 that the proposed scheme provides aided security as compared to related schemes.

Upon evaluating Tables 4, 6–8 we can state that the proposed scheme is efficient in terms of resource utilization; also, the proposed scheme provides aided and reliable security features. Thus, minimum resource utilization and enhanced
security features make the proposed authentication scheme efficient and suitable for the underlying infrastructure.

9. Conclusion

We have proposed an identity-based three-party lightweight remote user authentication scheme, for an IoT environment. We have demonstrated with the help of informal security analysis that the proposed scheme does not let any attacker to penetrate the system. We have shown that the proposed scheme has a vigorous capability to resist various attacks. In addition, formal security proof of the proposed scheme is given using Real-Or-Random (ROR); it shows that there exists secure mutual authentication between the remote users through a gateway in IoT infrastructure. Furthermore, the storage, computation, and communication cost of our scheme is far less than various related schemes. Hence, our proposed scheme is more efficient and reliable for IoT infrastructure as compared to various existing schemes.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Qu, L. Zhao, and Z. Xiong, "Cross-layer congestion control of wireless sensor networks based on fuzzy sliding mode control," *Neural Computing and Applications*, vol. 32, no. 17, pp. 13505–13520, 2020.

[2] H. Chen, Y. Chen, and L. Yang, "Intelligent early structural health prognosis with nonlinear system identification for RFID signal analysis," *Computer Communications*, vol. 157, pp. 150–161, 2020.

[3] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy-preserving authentication and access control scheme for pervasive computing environments," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 4, pp. 1373–1384, 2006.

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: anonymous on-demand routing in mobile ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2376–2385, 2006.

[5] Z. Cheng, L. Chen, R. Comley, and Q. Tang, "Identity-based key agreement with unilateral identity privacy using pairings," in *International Conference on Information Security Practice and Experience*, pp. 202–213, Springer, Berlin, Heidelberg, 2006.

[6] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC press, 1996.

[7] J. Zhou and K.-Y. Lam, "Undeniable billing in mobile communication," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom ’98*, Dallas, TX, USA, 1998.

[8] Y. Liu and J. Cao, "An improved anonymous remote authentication protocol," in 2009 Second International Symposium on Information Science and Engineering, pp. 181–184, Shanghai, China, 2009.

[9] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in *European Symposium on Research in Computer Security*, pp. 277–293, Springer, 1998.

[10] S.-J. Wang, "Anonymous wireless authentication on a portable cellular mobile system," *IEEE Transactions on Computers*, vol. 53, no. 10, pp. 1317–1329, 2004.

[11] G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication protocols for mobile network environment value-added services," *IEEE Transactions on Vehicular Technology*, vol. 51, no. 2, pp. 383–392, 2002.

[12] Z. Jia, Y. Zhang, H. Shao, Y. Lin, and J. Wang, "A remote user authentication scheme using bilinear pairings and ecc," in *Sixth International Conference on Intelligent Systems Design and Applications*, Jinan, China, 2006.

[13] G. Shailaja, K. P. Kumar, and A. Saxena, "Pairing based mutual authentication scheme using smart cards," *IACR Cryptology ePrint Archive*, vol. 2006, p. 152, 2006.

[14] Y.-P. Liao and S.-S. Wang, "A secure and efficient scheme of remote user authentication based on bilinear pairings," in *TENCON 2007 - 2007 IEEE Region 10 Conference*, Taipei, Taiwan, 2007.

[15] C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," in *Lecture Notes in Computer Science*, pp. 306–312, Springer, Berlin, Heidelberg, 2007.

Table 8: Security features comparison of the proposed and related schemes.

| Security features                                      | Ours | [67] | [68] | [69] | [70] | [71] | [72] | [73] |
|--------------------------------------------------------|------|------|------|------|------|------|------|------|
| Mutual authentication                                  | •    | •    | •    | •    | •    | •    | •    | •    |
| Key agreement                                          | •    | •    | •    | •    | •    | •    | •    | •    |
| User Untraceability                                   | •    | •    | •    | •    | •    | •    | •    | •    |
| User masquerading attack                               | •    | •    | •    | •    | •    | •    | •    | •    |
| GWF. N masquerading attack                             | •    | •    | •    | •    | •    | •    | •    | •    |
| Man-in-middle attack                                   | •    | •    | •    | •    | •    | •    | •    | •    |
| Parallel session attack                                | •    | •    | •    | •    | •    | •    | •    | •    |
| Privileged insider and stolen verifier attack           | •    | •    | •    | •    | •    | •    | •    | •    |
| Perfect forward secrecy                                 | •    | •    | •    | •    | •    | •    | •    | •    |
| No clock synchronization                               | •    | •    | •    | •    | •    | •    | •    | •    |

* • resists, ‘ not resists, ≈ not applicable.*
A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Z. W. Tan, D. Boneh and M. Franklin, “C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, 16 Journal of Sensors A. Shamir, M. Abdalla, D. Catalano, C. Chevalier, and D. Pointcheval, C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, T.-Y. Chang, M.-S. Hwang, and W.-P. Yang, A. Irshad, M. Usman, S. Ashraf Chaudhry, H. Naqvi, and M. Shafiq, “A provably secure and efficient authenticated key agreement scheme for Energy Internet based Vehicle-to-Grid technology framework,” IEEE Transactions on Industry Applications, vol. 56, no. 4, p. 1, 2020. K. Mansoor, A. Ghanis, C. Chaudhry, S. Shamshirband, S. Ghayyur, and A. Mosavi, “Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography,” Sensors, vol. 19, no. 21, p. 4752, 2019. T.-Y. Chang, M.-S. Hwang, and W.-P. Yang, “A communication-efficient three-party password authenticated key exchange protocol,” Information Sciences, vol. 181, no. 1, pp. 217–226, 2011. H. Cheng and Y. Liu, “An improved RSU-based authentication scheme for VANET,” Journal of Internet of Technology, vol. 21, no. 4, pp. 1137–1150, 2020. C.-M. Chen, K.-H. Wang, K.-H. Veh, B. Xiang, and T.-Y. Wu, “Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications,” Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 8, pp. 3133–3142, 2019. C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, “An novel three-party authenticated key exchange protocol using one-time key,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 498–503, 2013. A. Ghani, K. Mansoor, S. Mehmod, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, “Security and key management in iot-based wireless sensor networks: an authentication protocol using symmetric key,” International Journal of Communication Systems, vol. 32, no. 16, 2019. Z. W. Tan, “A Note on an Enhanced Three-Party Authentication Key Exchange Protocol,” Key Engineering Materials, vol. 439-440, pp. 1367–1372, 2010. H. Wang, H. Zhang, J. Li, and C. Xu, “A (3, 3) visual cryptography scheme for authentication,” Journal of Shenyang Normal University, vol. 31, no. 101, 2013. R. Roman, J. Lopez, and M. Mambo, “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges,” Future Generation Computer Systems, vol. 78, pp. 680–698, 2018. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, “Fog computing for the internet of things: security and privacy issues,” IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017. S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: a review of current applications and security solutions,” Journal of Cloud Computing, vol. 6, no. 1, p. 19, 2017. T. X. Tran, M.-P. Hosseini, and D. Pomplii, “Mobile edge computing: recent efforts and five key research directions,” IEEE COMSOC MMTC Commun.-Frontiers, vol. 12, pp. 29–34, 2017. E. Ahmed and M. H. Rehmani, Mobile Edge Computing: Opportunities, Solutions, and Challenges, Elsevier, 2017. J.-H. Yang and C.-C. Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Computers & Security, vol. 28, no. 3-4, pp. 138–143, 2009. E.-J. Yoon and K.-Y. Yoo, “Robust ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC,” in 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 2009. X. Cao, W. Kou, and X. Du, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges,” Information Sciences, vol. 180, no. 15, pp. 2895–2903, 2010. J.-L. Tsai and N.-W. Lo, “A privacy-aware authentication scheme for distributed mobile cloud computing services,” IEEE Systems Journal, vol. 9, no. 3, pp. 805–815, 2015. Q. Jiang, J. Ma, and F. Wei, “On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services,” IEEE Systems Journal, vol. 12, no. 2, pp. 2039–2042, 2018. A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, “An improved multi-server authentication scheme for distributed mobile cloud computing services,” TIIIS, vol. 10, no. 12, pp. 5529–5552, 2016. R. Amin, S. H. Islam, G. Biswas, D. Giri, M. K. Khan, and N. Kumar, “A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments,” Security and Communication Networks, vol. 9, no. 17, pp. 4650–4666, 2016. X. Yang, X. Huang, and J. K. Liu, “Efficient handover authentication with user anonymity and untraceability for mobile cloud computing,” Future Generation Computer Systems, vol. 62, pp. 190–195, 2016. M. H. Ibrahim, “Octopus: an edge-fog mutual authentication scheme,” IJ Network Security, vol. 18, no. 6, pp. 1089–1101, 2016. D. He, S. Zeadally, N. Kumar, and W. Wu, “Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2052–2064, 2016. L. Xiong, D. Peng, T. Peng, and H. Liang, “An Enhanced Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services,” KSII Transactions on Internet and Information Systems, vol. 11, no. 12, 2017. H. Zhu and S. Geng, “A three-party dynamic identity-based authenticated key exchange protocol with forward
