Hindawi
Journal of Sensors
Volume 2020, Article ID 8829319, 17 pages
https://doi.org/10.1155/2020/8829319

Research Article

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

Akasha Shafiq,[1] Muhammad Faizan Ayub,[1] Khalid Mahmood,[1] Mazhar Sadiq,[1] Saru Kumari,[2] and Chien-Ming Chen[3]

[1]*Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus 57000, Pakistan*
[2]*Department of Mathematics, Chaudhary Charan Singh University, Meerut, Uttar Pradesh 250004, India*
[3]*College 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

Academic Editor: Fei Yu

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 that 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' pregenerated 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 $E_p(e,f)$: $h^2 + eg + f \bmod p$, ECC is based on random points chosen on an elliptic curve, whereas $e, f \in Z_p$ and $4e^3 + 27f^2 \bmod p \neq 0$ 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 $qS = S + S + S + S + S + \cdots\cdots + S$ (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 $\mathcal{U}_{A_{\text{adv}}}$ is given as: $\text{Adv}^{\text{ECDLP}}_{\mathcal{U}_{A_{\text{adv}}}}(t) = Prb[(\mathcal{U}_{A_{\text{adv}}})(S, R) = x : x \in Z_p]$. The supposition of ECDLP states that $\text{Ad}\,\text{v}^{\text{ECDLP}}_{\mathcal{U}_{A_{\text{adv}}}}(t) \leq \epsilon$.

3.2. One-Way Hash Function. Hash functions are used to get an output (f) 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 $h(.)$ is secured by predefined collision resistance. The chances that an adversary $(\mathcal{U}_{A_{\text{adv}}})$ can find out a couple $(y_1 \neq y_2)$ as $h(y_1) = h(y_2)$ is defined as $\text{Ad}\,\text{v}^{\text{hash}}_{\mathcal{U}_{A_{\text{adv}}}}(t) = \text{Prb}[(y_1, y_2) \Leftarrow_r \mathcal{U}_{A_{\text{adv}}} : (y_1 \neq y_2) \text{ and } h(y_1) = h(y_2)]$, whereas $\mathcal{U}_{A_{\text{adv}}}$ is allowed to select a couple y_1, y_2 randomly. $\mathcal{U}_{A_{\text{adv}}}$'s advantage is determined over a random selection in polynomial time (t). Collision resistance is stated as $\text{Ad}\,\text{v}^{\text{hash}}_{\mathcal{U}_{A_{\text{adv}}}}(t) \leq \epsilon$, whereas $\epsilon > 0$ is an adequately small value.

Table 1: Common notations.

Notation	Description
$\mathcal{U}_i$	$\mathcal{U}_i$th remote user of the system
ID_i	$\mathcal{U}_i$'s identity
$\mathcal{TPM}_i$	$\mathcal{U}_i$'s tamper proof on-board memory/storage
$\mathcal{GWN}$	Gateway node
ID_{GWN}	$\mathcal{GWN}$'s identity
x	$\mathcal{GWN}$'s secret key
$\text{Pub} = xG$	$\mathcal{GWN}$'s public key
$E_p(e,f)$	An elliptic curve
G	Base-point of elliptic curve $Ep(e,f)$
$h(.)$	One-way function
$\oplus$	XoR operator
$\|$	Concatenation operator
$\Rightarrow$	Secure channel
$\rightarrow$	Public channel
$\mathcal{U}_{A_{\text{adv}}}$	Adversary

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 Dolev-Yao's [61] threat model. The capabilities of $U_{A\text{adv}}$ are as follows:

(1) $U_{A\text{adv}}$ has full control over the public channel

(2) U_{Aadv} can easily intercept the messages of all the participants during communication over the public channel

(3) U_{Aadv} can be trusted or deceitful user of the system

(4) U_{Aadv} can be an insider of the system

(5) The identities are publicly known

(6) U_{Aadv} cannot find or extract x (GWN's private key)

(7) U_{Aadv} cannot access the messages that are being transmitted over a secure channel

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

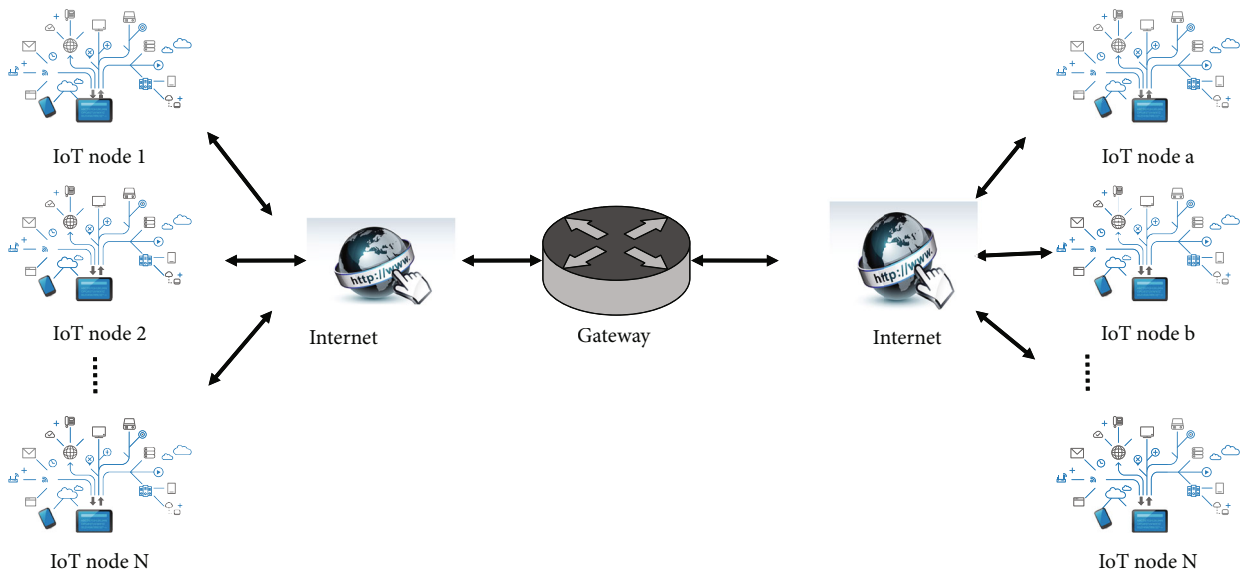

Figure 1: System setup for the proposed scheme.

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 $\mathcal{U}_a$ wants to communicate with another user $\mathcal{U}_b$, then they both have to pass the authentication process. For authentication, each entity will be verified by $\mathcal{GWN}$. If both entities are authenticated, then they can share the session key. The complete registration process of the user $\mathcal{U}_i$ 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. $\mathcal{U}_i$ chooses his/her ID_i and the arbitrary number l_{i1}.

RG-Step 2. $\mathcal{GWN}$ upon receiving the registration requests $(ID_i, h(ID_i \oplus l_{i1}))$ from U_i, then calculates the following values:

$$\begin{aligned} \mathrm{MID}_i &= h(\mathrm{ID}_i), \\ V_i &= h(x \| \mathrm{MID}_i), \\ Y_i &= V_i \oplus h(\mathrm{ID} \oplus l_{i1}) \end{aligned} \tag{1}$$

RG-Step 3. On receiving Y_i from GWN, U_i calculates the following values:

$$\begin{aligned} V_i &= Y_i \oplus h(\mathrm{ID}_i \oplus l_{i1}), \\ Z_i &= l_{i1} \oplus \mathrm{ID}_i, \\ A_i &= h(V_i \| \mathrm{ID}_i \| l_{i1}) \end{aligned} \tag{2}$$

After calculating these values, stores $\{A_i, Y_i, Z_i\}$ in $\mathcal{TPM}_i$s.

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 $\mathcal{TPM}_i$ of the mobile device [62, 63]:

$$\begin{aligned} l_{a1} &= Z_a \oplus \mathrm{ID}_a, \\ V_a &= Y_a \oplus h(\mathrm{ID}_a \oplus l_{a1}), \\ A_a &\stackrel{?}{=} h(V_a \| \mathrm{ID}_a \| l_{a1}) \end{aligned} \tag{3}$$

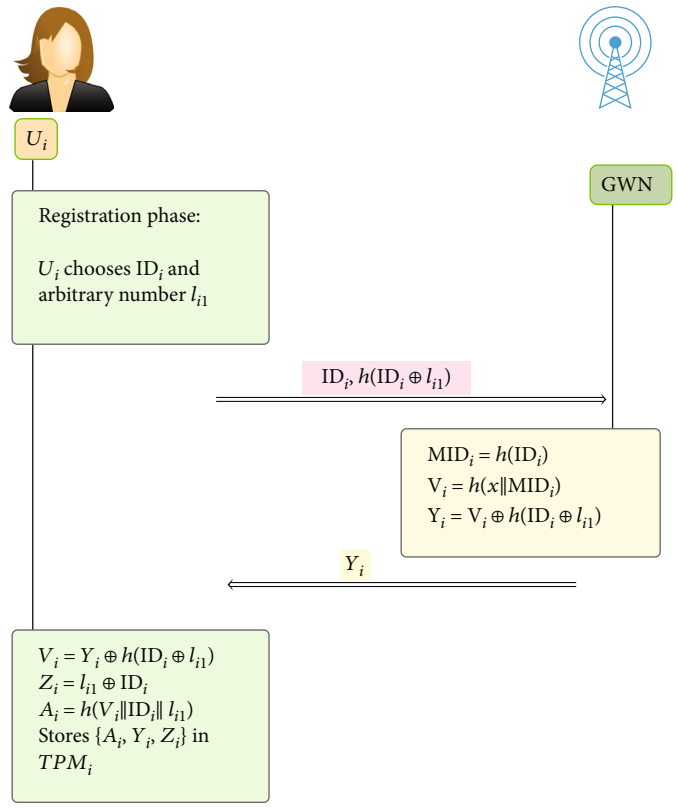

FIGURE 2: Registration process of U_i.

Further computation generates a random number l_{a2} and calculates the following values:

$$\begin{aligned} Q_a &= l_{a2}G, \\ \text{PID}_a &= (\text{ID}_a \| \text{MID}_b) \oplus l_{a2}\text{Pub}, \\ \text{auth}_a &= h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{\text{GWN}} \| V_a) \end{aligned} \tag{4}$$

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

$$\begin{aligned} l_{b1} &= Z_b \oplus \text{ID}_b, \\ V_b &= Y_b \oplus h(\text{ID}_b \oplus l_{b1}), \\ A_b &\stackrel{?}{=} h(V_b \| \text{ID}_b \| l_b) \end{aligned} \tag{5}$$

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

$$\begin{aligned} Q_b &= l_{b2}G, \\ \text{PID}_b &= (\text{ID}_b \| \text{MID}_a) \oplus l_{b2}\text{Pub}, \\ \text{auth}_b &= h(\text{ID}_b \| \text{MID}_a \| \text{ID}_{\text{GWN}} \| Y_b \oplus h(\text{ID}_b \| l_{b1})) \end{aligned} \tag{6}$$

After calculating these values, $\mathcal{U}_a$ and $\mathcal{U}_b$ 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:

$$\begin{aligned} xQ_a &= l_{a2}xG = l_{a2}\text{Pub}, \\ (\text{ID}_a \| \text{MID}_b) &= \text{PID}_a \oplus l_{a2}\text{Pub}, \\ \text{MID}_a &= h(\text{ID}_a), \\ \text{auth}_a &\stackrel{?}{=} h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{\text{GWN}} \| h(x \| \text{MID}_a)) \end{aligned} \tag{7}$$

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

$$\begin{aligned} xQ_b &= l_{b2}xG = l_{b2}\text{Pub}, \\ (\text{ID}_b \| \text{MID}_a) &= \text{PID}_b \oplus l_{b2}\text{Pub}, \\ \text{MID}_b &= h(\text{ID}_b), \\ \text{auth}_b &\stackrel{?}{=} h(\text{ID}_b \| \text{MID}_a \| \text{ID}_{\text{GWN}} \| h(x \| \text{MID}_b)) \end{aligned} \tag{8}$$

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

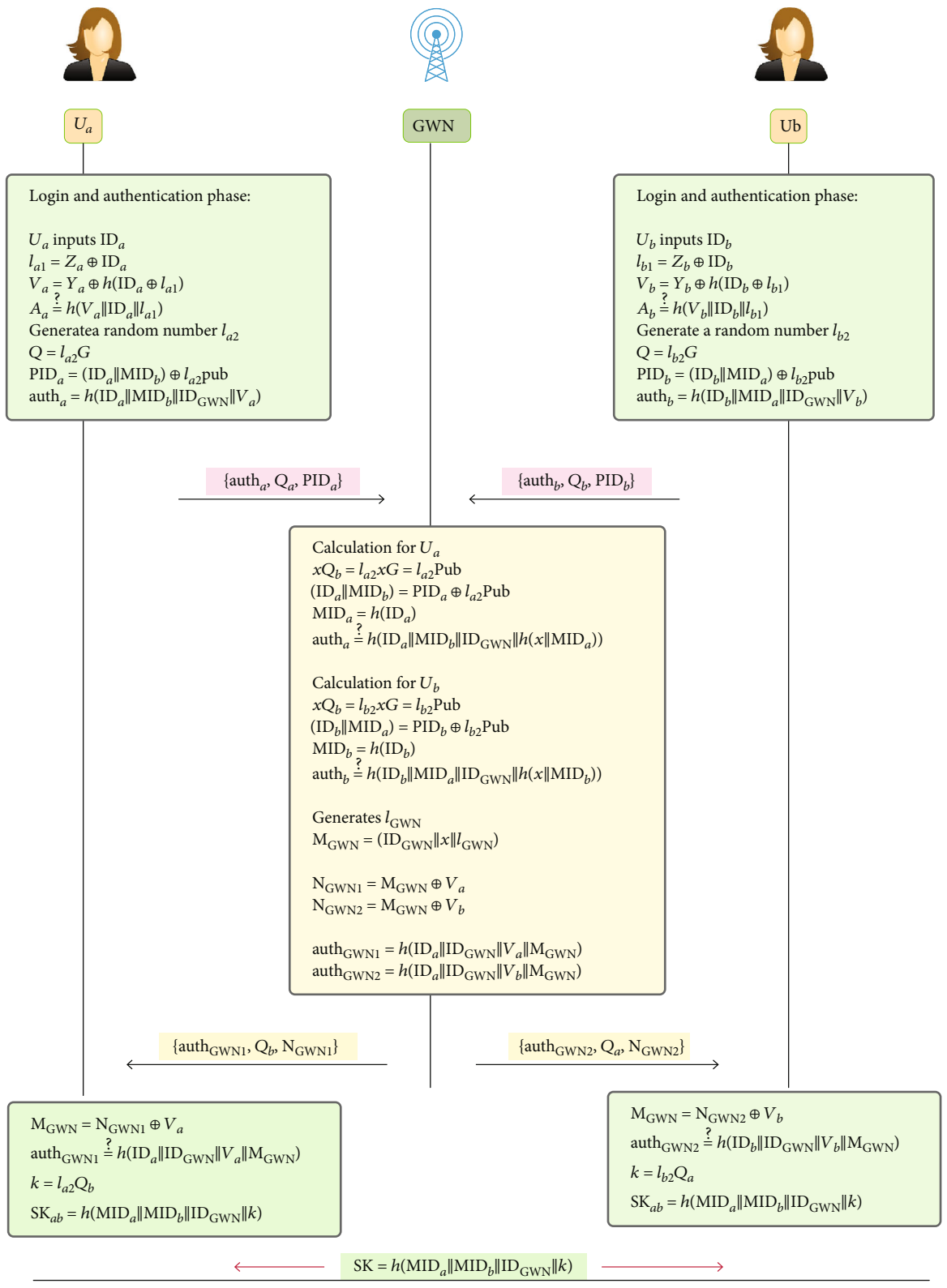

Figure 3: Login and authentication process of U_i.

$$\begin{aligned} M_{\mathrm{GWN}} &= (\mathrm{ID}_{\mathrm{GWN}} \| x \| l_{\mathrm{GWN}}), \\ N_{\mathrm{GWN1}} &= M_{\mathrm{GWN}} \oplus V_a, \\ N_{\mathrm{GWN2}} &= M_{\mathrm{GWN}} \oplus V_b, \\ \mathrm{auth}_{\mathrm{GWN1}} &= h(\mathrm{ID_a} \| \mathrm{ID}_{\mathrm{GWN}} \| V_a \| M_{\mathrm{GWN}}), \\ \mathrm{auth}_{\mathrm{GWN2}} &= h(\mathrm{ID_b} \| \mathrm{ID}_{\mathrm{GWN}} \| V_b \| M_{\mathrm{GWN}}) \end{aligned} \tag{9}$$

AT-Step 3. After the calculation of the above values, $\mathcal{GWN}$ sends $\{\mathrm{auth}_{\mathrm{GWN1}}, Q_b, N_{\mathrm{GWN1}}\}$ and $\{\mathrm{auth}_{\mathrm{GWN2}}, Q_a, N_{\mathrm{GWN2}}\}$ to $\mathcal{U}_a$ and $\mathcal{U}_b$, respectively. $\mathcal{U}_a$ then calculates the following values along with the session key:

$$\begin{aligned} M_{\mathrm{GWN}} &= N_{\mathrm{GWN2}} \oplus V_a, \\ \mathrm{auth}_{\mathrm{GWN1}} &\stackrel{?}{=} h(\mathrm{ID}_a \| \mathrm{ID}_{\mathrm{GWN}} \| V_a \| M_{\mathrm{GWN}}), \\ k &= l_{a2} Q_b, \\ \mathrm{SK}_{ab} &= h(\mathrm{MID}_a \| \mathrm{MID}_b \| \mathrm{ID}_{\mathrm{GWN}} \| k) \end{aligned} \tag{10}$$

Also, $\mathcal{U}_b$ on the basis of the received parameters $\{\mathrm{auth}_{\mathrm{GWN2}}, Q_a, N_{\mathrm{GWN2}}\}$ calculates the following values along with the session key:

$$\begin{aligned} M_{\mathrm{GWN}} &= N_{\mathrm{GWN2}} \oplus V_b, \\ \mathrm{auth}_{\mathrm{GWN2}} &\stackrel{?}{=} h(\mathrm{ID}_b \| \mathrm{ID}_{\mathrm{GWN}} \| V_b \| M_{\mathrm{GWN}}), \\ k &= l_{b2} Q_a, \\ \mathrm{SK}_{ab} &= h(\mathrm{MID}_a \| \mathrm{MID}_b \| \mathrm{ID}_{\mathrm{GWN}} \| k), \end{aligned} \tag{11}$$

Finally, $\mathcal{GWN}$ computes a shared session key as:

$$SK_{ab} = h(\mathrm{MID}_a \| \mathrm{MID}_b \| \mathrm{ID}_{\mathrm{GWN}} \| k) \tag{12}$$

Hence, both the entities $\mathcal{U}_a$ and $\mathcal{U}_a$ authenticate themselves via $\mathcal{GWN}$ and consequently shared a session key for subsequent communication.

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 U_i has the private key corresponding to his/her own ID_i. Also, identity security includes the availability of identity. If a U_i's identity is revoked by GWN, even then, the U_i has control over his I D_i and the relevant claims, which states that the U_i still can use his/her ID_i 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 $\mathrm{SK}_{ab} = h(\mathrm{MID}_a k \mathrm{MID}_b k \mathrm{ID}_{\mathrm{GWN}} k k)$. Hence, our scheme offers a successful key agreement.

7.1.3. Mutual Authentication. In our introduced scheme, the $\mathcal{GWN}$ can authenticate $\mathcal{U}_a$ by verifying $\mathrm{auth}_a \stackrel{?}{=} h(\mathrm{ID}_a \| \mathrm{MI}$ $\mathrm{D}_b \| \mathrm{ID}_{\mathrm{GWN}} \| V_a)$. The values $\mathrm{ID}_a, \mathrm{MID}_b, \mathrm{ID}_{\mathrm{GWN}}, V_a$ 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 $\mathcal{GWN}$. Likewise, $\mathcal{GWN}$ authenticates the other user. Similarly, user $\mathcal{U}_a$ can also authenticate $\mathcal{GWN}$ by verifying aut $\mathrm{h}_{\mathrm{GWN}} \stackrel{?}{=} h(\mathrm{ID}_a \| \mathrm{ID}_{\mathrm{GWN}} \| V_a \| M_{\mathrm{GWN}})$. The values $\mathrm{ID}_a, \mathrm{ID}_{\mathrm{GWN}}$, V_a, M_{GWN} are only known to valid $\mathcal{U}_a$. As adversary cannot calculate all these values, so only the legitimate $\mathcal{GWN}$ can be authenticated by $\mathcal{U}_a$. Likewise, other users can authenticate $\mathcal{GWN}$. Thus, it is proved that our introduced scheme offers mutual authentication between users and $\mathcal{GWN}$.

7.1.4. User Anonymity. During the login and authentication stage, the identity of $\mathcal{ID}_a$ of user $\mathcal{U}_a$ is not transmitted in plain text; instead, the pseudoidentity $\mathrm{PID_a}$ 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 provide user anonymity.

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_a, 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_a. 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 $\mathcal{U}_{A_{\mathrm{adv}}}$ is able to know the secret parameters such as the secret key of $\mathcal{GWN}$, 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_{ab}. 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 $\mathcal{U}_{A_{\text{adv}}}$ is able to find the secret parameters of $\mathcal{GWN}$, even then, he cannot find the future sessions. In the proposed scheme, the calculation of valid Sk_{ab} requires arbitrary number $\{l_{a1}, l_{a2}\}$. Due to these random numbers, the session key is specific for every session; thus, $\mathcal{U}_{A_{\text{adv}}}$ cannot find future session keys.

7.1.8. Privileged Insider and Stolen Verifier Attack. During the registration phase, $\mathcal{U}_i$ transmit ID_i and l_{i1} through the private channel to $\mathcal{GWN}$, where arbitrary number l_{i1} is generated by $\mathcal{U}_i$. Furthermore, for $\mathcal{U}_i$'s identity, no table is preserved, for authentication $\mathcal{GWN}$ uses x his secret key. Thus, no insider $\mathcal{U}_{A_{\text{adv}}}$ 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 $\mathcal{U}_{A_{\text{adv}}}$ tries to masquerade a legal $\mathcal{U}_a$ by means of sending a legal login request message on behalf of $\mathcal{U}_a$ to the $\mathcal{GWN}$. In order to produce an original login message $\{\text{auth}_a, Q_a, \text{PID}_a\}$, the adversary needs to calculate valid $\text{auth}_a = h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{\text{GWN}} \| V_a)$. It is not possible for the adversary to calculate auth_a because $\mathcal{U}_{A_{\text{adv}}}$ does not know ID_a of $\mathcal{U}_a$. 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. $\mathcal{GWN}$ Masquerading Attack. Suppose an attacker $\mathcal{U}_{A_{\text{adv}}}$ tries to impersonate a legal server $\mathcal{GWN}$ by means of sending a legal challenge message on the behalf of $\mathcal{GWN}$ to the user. In order to produce an original challenge message $\{\text{auth}_{\text{GWN}}, Q_a, N_{\text{GWN}}\}$, the adversary needs to calculate the valid $\text{auth}_{\text{GWN1}} \stackrel{?}{=} h(\text{ID}_a \| \text{ID}_{\text{GWN}} \| V_a \| M_{\text{GWN}})$. However, this operation is computationally expensive because for determining $V_a = h(x \| \text{MID}_a)$, it needs a private key of $\mathcal{GWN}$. So, the proposed scheme has the ability to withstand the user masquerading attack.

7.1.11. Man-in-the-Middle Attack (MITM). Suppose $\mathcal{U}_{A_{\text{adv}}}$ forges the login message $\{\text{auth}_a, Q_a, \text{PID}_a\}$ sent by $\mathcal{U}_a$ to $\mathcal{GWN}$, still, any tampering in the login request message will easily be identified while determining $\text{auth}_a = h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{\text{GWN}} \| V_a)$. $\mathcal{U}_{A_{adv}}$ 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 $\mathcal{U}_{A_{\text{adv}}}$ intercepts the request message $\{\text{auth}_a, Q_a, \text{PID}_a\}$ of $\mathcal{U}_i$ and later replays the intercept message, the calculation of Q_a and PID_a 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 $\mathcal{U}_{A_{\text{adv}}}$, 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 $\mathcal{U}_{A_{\text{adv}}}$ 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 $\mathcal{U}_{A_{adv}}$ is an attacker who builds at most q_{send}Send queries, q_{rvl}Reveal queries, q_{exe}Execute queries, q_{hash}Hash queries and succeed the game having benefit $Adv_{P_p}^{AKA}(\mathcal{U}_{A_{adv}})$, then an algorithm that should be existed, which can efficiently resolve ECDHP hard problem on group G having benefit Adv_G^{ECDHP}, where*

$$Adv_{P_p}^{AKA} \leq \frac{q_{hash}^2}{2^l - 1} + \frac{q_{send}}{2^{l-2}} + \frac{(q_{send} + q_{exe})^2}{P} + \frac{(q_{send} + q_{exe})^2}{P} + 2q_{hash} Adv_{G_p}^{ECDHP} \tag{13}$$

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 $\mathcal{U}_{A_{\text{adv}}}$ as a function. The function that is taken as an arbitrary oracle in the proposed scheme is referred to as hash $h(.)$. In order to record the hash queries and their answer, $\mathcal{C}_r$ maintains a hash list and is referred to as a L_{hash}. To make it simple, we use three transcripts between entities, which are as follows:

$$\begin{aligned} m\mathcal{U}_a &= \{\text{auth}_a, Q_a, \text{PID}_a\}, \\ m\mathcal{U}_b &= \{\text{auth}_b, Q_b, \text{PID}_b\}, \\ m\mathcal{GWN} &= \{\text{auth}_{\text{GWN}_1}, Q_b, N_{\text{GWN}_1}, \text{auth}_{\text{GWN}_2}, Q_a, N_{\text{GWN}_2}\} \end{aligned} \tag{14}$$

After simulating the scheme, C_{rs} answers the queries questioned by $U_{A_{\text{advs}}}$ as follows:

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

(ii) *Send Query*.

(1) $\mathcal{C}_r$ simulates $\mathcal{U}_{A_{\text{adv}}}$'s response in the following way after getting $\text{Send}(\mathcal{U}_{A_{\text{adv}}}, \text{Start})$: selects a random numbers l_{a1}, l_{a2} and computes $Q_a = l_{a2} G$, $\text{PID}_a = (\text{ID}_a \| \text{MID}_b) \oplus l_{a2.\text{pub}}$, $\text{auth}_a = h(\text{ID}_a \| \text{MID}_b \| \text{ID}_{\text{GWN}} \| V_a)$ and returns back $\{\text{auth}_a, Q_a, \text{PID}_a\}$ as response

(2) Upon the reception of query Send($\mathcal{U}_b$, (auth$_a$, Q_a, 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_{b1}, l_{b2} and computes $Q_b = l_{b2}G$, PID$_b$ = (ID$_b$‖MID$_a$) ⊕ l_{b2}pub, auth$_b$ = h(ID$_b$‖MID$_b$‖ID$_{GWN}$‖V_b) and returns back { auth$_b$, Q_b, PID$_b$} as response

(3) Upon getting Send(GWN(auth$_a$, Q_a, 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 $xQ_a = l_{a2}xG = l_{a2}$pub, (ID$_a$‖MID$_b$) = PID$_a$ ⊕ l_{a2}pub, MID$_a$ = h(ID$_a$), and auth$_a$ = h(ID$_a$‖MID$_b$‖ID$_{GWN}$‖h(x‖MID$_a$)). Furthermore, GWN generates l_{GWN} and computes $N_{GWN_1=M_{GWN}\oplus V_a}$, auth$_{GWN_1}$ = h(ID$_a$‖ID$_{GWN}$‖V_a‖M_{GWN}) and response back with {auth$_{GWN_1}$, Q_b, N_{GWN_1}}.

(4) After receiving query Send(GWN, (auth$_b$, Q_b, PID$_b$)) and assuming $\mathcal{GWN}$ as a correct state, $\mathcal{C}_r$ simulates $\mathcal{GW}$N's response as follows: computes $xQ_b = l_{b2}xG = l_{b2}$pub, (ID$_b$‖MID$_a$) = PID$_b$ ⊕ l_{b2}pub, MID$_b$ = h(ID$_b$) and verifies auth$_b$ = h(ID$_b$‖MID$_a$‖ID$_{GWN}$‖h(x‖MID$_b$)). Furthermore, generate l_{GWN} and compute $N_{GWN_2} = M_{GWN} \oplus V_b$, auth$_{GWN_2}$ = h(ID$_b$‖ID$_{GWN}$‖V_b‖M_{GWN}), and return {auth$_{GWN_a}$, Q_a, N_{GWN_2}} as response

(5) In the end, the session key is shared among the participants if checks auth$_{GWN_1}$ $\stackrel{?}{=}$ h(ID$_a$‖ID$_{GWN}$‖V_a‖M_{GWN}) and auth$_{GWN_2}$ $\stackrel{?}{=}$ h(ID$_b$‖ID$_{GWN}$‖V_b‖M_{GWN}) are hold true. Otherwise, the session will be terminated

(iii) *Execute Query*. While getting execute query (U_a, GWN, U_b), C_r simulates the send query as follows:

$$\begin{aligned} m_{\mathcal{U}_a g} &= \text{Send}(\mathcal{U}_a, \text{Start}), \\ m_{\mathcal{U}_b g} &= \text{Send}\left(\mathcal{U}_b, m_{\mathcal{U}_a}\right), \\ m_g \mathcal{U}_a \mathcal{U}_b &= \text{Send}\left(\mathcal{GWN}, m_{\mathcal{U}_a g}, m_{\mathcal{U}_b g}\right) \end{aligned} \tag{15}$$

C_r returns $m_{\mathcal{U}_a g}$, $m_{\mathcal{U}_b g}$ and $m_g \mathcal{U}_a \mathcal{U}_b$ as an answer.

(iv) *Corrupt Query*.

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

(2) On receiving query Corrupt(GWN, {V_i}), C_r responds all information stored in temper proof onboard storage/memory

(v) *Reveal query*: after getting a query Reveal(U_i), 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 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 $G_{a0}, G_{a1} \cdots G_{a5}$ is defined next. For every game G_{ai}, assume S_i is an event that $U_{A\text{adv}}$ wins the game, which means $U_{A\text{adv}}$ 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:

$$\text{Adv}_{\mathcal{U}_{A_{\text{adv}}}} = |2P_r[S_0] - 1| \tag{16}$$

Game G_{a1}. G_{a1} is similar to G_{a0}, but the difference is that hash queries are entertained by scanning the L_{hash} by C_r. G_{a1} remains indistinguishable from G_{a0} until the queries are answered similarly in G_{a0}. Hence, we got

$$P_r[S_1] = P_r[S_0] \tag{17}$$

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

(i) *Event_1*. Collision of hash queries during simulation.

(ii) *Event_2*. Collision on the simulation of transcripts $m_{\mathcal{U}_a g}, m_{\mathcal{U}_b g}, m_g \mathcal{U}_a \mathcal{U}_b$.

As per the concept of birthday paradox, we got P_r[Even t$_1$] ≤ $q_{\text{hash}}^2/2^{l+1}$. For transcript $m_g \mathcal{U}_a \mathcal{U}_b$, the collision probability of Event$_2$ is $(q_{\text{send}} + q_{\text{exe}})^2/2_{P^2}$, while the probability

Table 4: Computation Cost of Proposed and Related Schemes.

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

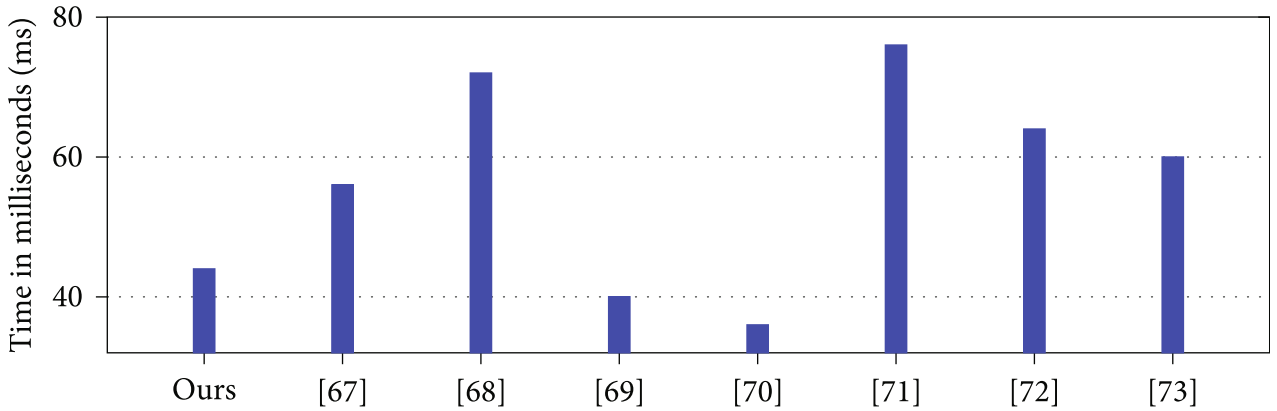

Figure 4: Comparison of the proposed and related scheme computation overhead.

Table 5: Communication structure.

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

of collision on the transcript $m_{\mathcal{U}_a}, m_{\mathcal{U}_b}$ is $(q_{\mathrm{Send}} + q_{\mathrm{exe}})^2/2_p$. We got:

$$|P_r[S_2] - P_r[S_1]| \leq \frac{q_{\mathrm{hash}}^2}{2^{l+1}} + \frac{(q_{\mathrm{send}} + q_{\mathrm{exe}})^2}{2p^2} + \frac{(q_{\mathrm{send}} + q_{\mathrm{exe}})^2}{2p} \tag{18}$$

Game G_{a3}. G_{a3} is almost similar to G_{a2}, but the difference is that, $\mathcal{U}_{A_{\mathrm{adv}}}$ may know the authentication value auth_a, aut h_b, $\mathrm{auth}_{\mathrm{GWN}_1}$ and $\mathrm{auth}_{\mathrm{GWN}_2}$ without knowing the hash oracle. Thus, we got

$$|P_r[S_3] - P_r[S_2]| \leq \frac{q_{\mathrm{Send}}}{2^l} \tag{19}$$

Game G_{a4}. In G_{a4}, G_{a3} is modified as follows:

(i) $\mathcal{U}_a$ scans L_{Hash} for ID_a. If the entries exist, then calculate $\{\mathrm{auth}_a, Q_a, \mathrm{PID}_a\}$

(ii) GWN verifies the legitimacy of $\mathcal{U}_a$. If it holds, then GWN scans for $\{\mathrm{auth}_a, Q_a, \mathrm{PID}_a\}$ in the Send list. Otherwise, the session aborts. G_{a4} will succeed if $\mathcal{U}_{A_{\mathrm{adv}}}$ guess the authentication parameters without a hash oracle. So

$$|P_r[S_4] - P_r[S_3]| \leq \frac{q_{\mathrm{send}}}{2^l} \tag{20}$$

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

(i) $\mathcal{U}_a$ randomly chooses l_{a2} and computes $Q_a = l_{a2}G$, $\mathrm{PID}_a = (\mathrm{ID}_a \| \mathrm{MID}_a) \oplus l_{a2}\mathrm{pub}$, and $\mathrm{auth}_a = h(\mathrm{ID}_a \| \mathrm{MI}\ \mathrm{D}_a \| \mathrm{ID}_{\mathrm{GWN}} \| Y_a \oplus h(\mathrm{ID}_a \| l_{a1}))$ and stores $\{\mathrm{auth}_a, Q_a, \mathrm{PID}_a\}$ in L_{Hash}

Table 6: Communication cost of the proposed and related schemes.

Schemes	No. of messages exchanged	Cost of registration phase	Cost of login authentication	Total cost
Ours	3	672	1344	2016
He et al. [67]	6	928	3776	4704
Challa et al. [68]	5	512	2976	3488
Ma et al. [69]	8	832	4704	5536
Taher et al. [70]	8	3392	5440	8832
Chandrakar and Om [71]	8	2368	3360	5728
Lu et al. [72]	5	672	2944	3616
Mo and Chen [73]	6	2112	4504	6616

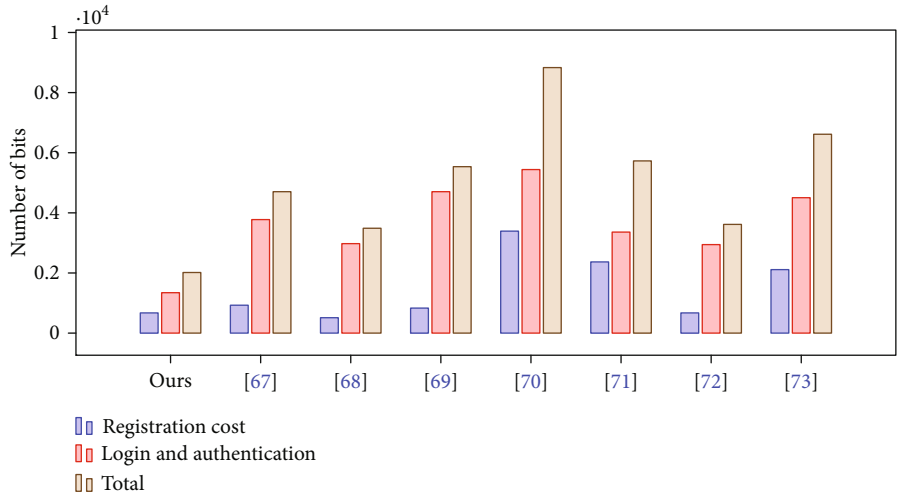

Figure 5: Comparison of proposed and related scheme communication overhead.

Table 7: Storage cost of the proposed and related schemes.

Schemes	No. of bits required for storage
Ours	672
He et al. [67]	672
Challa et al. [68]	1024
Ma et al. [69]	672
Taher et al. [70]	1536
Chandrakar and Om [71]	1856
Lu et al. [72]	768
Mo and Chen [73]	2464

(ii) $\mathcal{U}_b$ randomly selects l_{b2} and computes $Q_{b2} = l_{b2}G$, $\text{PID}_b = (\text{ID}_b \| \text{MID}_a) \oplus l_{b2}\text{pub}$, and $\text{auth}_b = h(\text{ID}_b \| \text{MID}_a \| \text{ID}_{\text{GWN}} \| Y_b \oplus h(\text{ID}_b \| l_{b1})$ and stores $\{\text{auth}_b, Q_b, \text{PID}_b\}$ in L_{Hash}

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

$$|P_r[S_5] - P_r[S_4]| \leq q_{\text{hash}} \text{Adv}_G^{\text{ECDHP}} \quad (21)$$

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

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

$$\text{Advt}_{P_p}^{\text{AKA}} \leq \frac{q_{\text{hash}}^2}{2^{l-1}} + \frac{q_{\text{send}}}{2^{l-2}} + \frac{(q_{\text{send}} + q_{\text{exe}})^2}{P^2} + \frac{(q_{\text{send}} + q_{\text{exe}})^2}{P} + 2_{q_{\text{hash}}} \text{Adv}_G^{\text{ECDHP}} \quad (22)$$

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

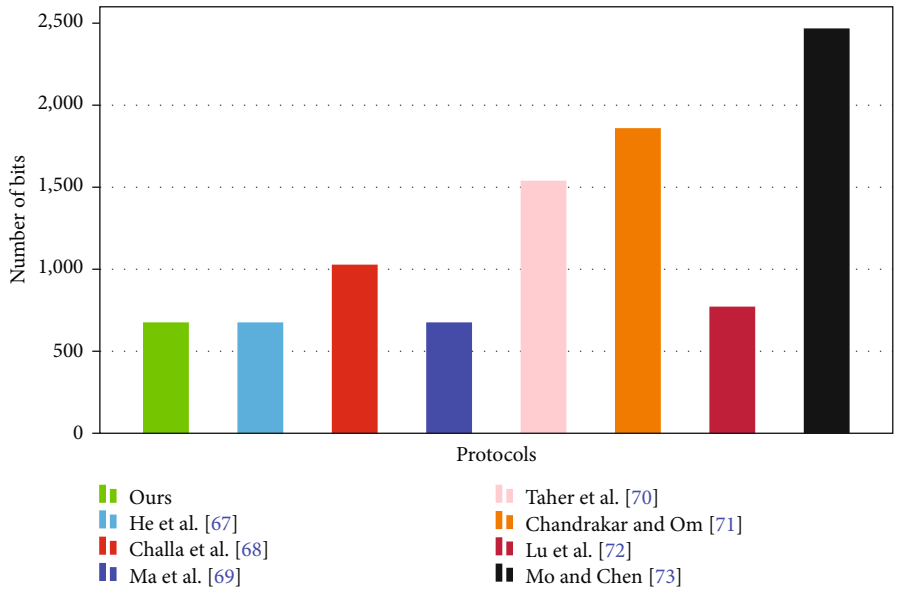

Figure 6: Comparison of the proposed and related scheme storage overhead.

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_i, ID_{GWNs}), random numbers, and point multiplication require 160 bits respectively, whereas we assumed 256 bits for hash, secrete, and public keys (x, 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

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

Security features	Schemes							
	Ours	[67]	[68]	[69]	[70]	[71]	[72]	[73]
Mutual authentication	•	•	•	•	•	•	•	•
Key agreement	•	•	•	•	•	•	•	•
User Untraceability	•	°	•	•	•	•	°	•
User masquerading attack	•	•	•	•	•	•	°	•
$\mathcal{GWN}$ masquerading attack	•	•	•	•	•	•	•	•
Man-in-middle attack (MITM)	•	•	•	•	•	•	•	•
Parallel session attack	•	•	•	≈	•	•	•	•
Privileged insider and stolen verifier attack	•	•	°	•	•	•	°	•
Perfect forward secrecy	•	•	•	•	•	•	°	•
No clock synchronization	•	°	°	°	°	°	°	°

• resists, ° not resists, ≈ not applicable.

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.

[16] Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, "A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices," in *31st Annual International Computer Software and Applications Conference - Vol. 2 - (COMPSAC 2007)*, pp. 700–710, Beijing, China, 2007.

[17] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*, pp. 47–53, Springer, Berlin, Heidelberg, 1984.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, pp. 213–229, Springer, Berlin, Heidelberg, 2001.

[19] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, 2006.

[20] M. Abdalla, D. Catalano, C. Chevalier, and D. Pointcheval, "Efficient two-party password-based key exchange protocols in the uc framework," in *Topics in Cryptology – CT-RSA 2008*, pp. 335–351, Springer, Berlin, Heidelberg, 2008.

[21] C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Information Systems*, pp. 1–16, 2020.

[22] 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.

[23] K. Mansoor, A. Ghani, S. 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.

[24] 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.

[25] 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.

[26] C.-M. Chen, K.-H. Wang, K.-H. Yeh, 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.

[27] 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.

[28] A. Ghani, K. Mansoor, S. Mehmood, 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.

[29] Z. W. Tan, "A Note on an Enhanced Three-Party Authentication Key Exchange Protocol," *Key Engineering Materials*, vol. 439-440, pp. 1367–1372, 2010.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] T. X. Tran, M.-P. Hosseini, and D. Pompili, "Mobile edge computing: recent efforts and five key research directions," *IEEE COMSOC MMTC Commun.-Frontiers*, vol. 12, pp. 29–34, 2017.

[35] E. Ahmed and M. H. Rehmani, *Mobile Edge Computing: Opportunities, Solutions, and Challenges*, Elsevier, 2017.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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," *TIIS*, vol. 10, no. 12, pp. 5529–5552, 2016.

[42] 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.

[43] 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.

[44] M. H. Ibrahim, "Octopus: an edge-fog mutual authentication scheme," *IJ Network Security*, vol. 18, no. 6, pp. 1089–1101, 2016.

[45] 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.

[46] 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.

[47] H. Zhu and S. Geng, "A three-party dynamic identity-based authenticated key exchange protocol with forward

anonymity," *Wireless Personal Communications*, vol. 109, no. 3, pp. 1911–1924, 2019.

[48] K. Renuka, S. Kumar, S. Kumari, and C.-M. Chen, "Cryptanalysis and improvement of a privacy-preserving three-factor authentication protocol for wireless sensor networks," *Sensors*, vol. 19, no. 21, p. 4625, 2019.

[49] A. K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1377–1404, 2015.

[50] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in iot networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.

[51] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Networks*, vol. 25, no. 8, pp. 4737–4750, 2019.

[52] M. Ramadan, Y. Liao, F. Li, and S. Zhou, "Identity-based signature with server-aided verification scheme for 5G mobile systems," *IEEE Access*, vol. 8, pp. 51810–51820, 2020.

[53] S. Kumar, S. Akbar Abbas Jafri, N. A. Nigam, N. Gupta, G. Gupta, and S. K. Singh, "A new user identity based authentication, using security and distributed for cloud computing," *IOP Conference Series: Materials Science and Engineering*, vol. 748, 2020.

[54] N. Farjana, S. Roy, M. J. N. Mahi, and M. Whaiduzzaman, "An identity-based encryption scheme for data security in fog computing," in *Proceedings of International Joint Conference on Computational Intelligence*, pp. 215–226, Dhaka, Bangladesh, 2020.

[55] Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets," *IEEE Systems Journal*, pp. 1–11, 2020.

[56] X. Jia, N. Hu, S. Su et al., "IRBA: an identity-based cross-domain authentication scheme for the internet of things," *Electronics*, vol. 9, no. 4, p. 634, 2020.

[57] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems," *Computer Communications*, vol. 153, pp. 527–537, 2020.

[58] S. Hussain and S. A. Chaudhry, "Comments on biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10936–10940, 2019.

[59] M. Ramadan, Y. Liao, F. Li, S. Zhou, and H. Abdalla, "IBEET-RSA: identity-based encryption with equality test over RSA for wireless body area networks," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 223–233, 2020.

[60] M. Shuai, B. Liu, N. Yu, L. Xiong, and C. Wang, "Efficient and privacy-preserving authentication scheme for wireless body area networks," *Journal of Information Security and Applications*, vol. 52, p. 102499, 2020.

[61] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[62] G. Hammouri, E. Öztürk, and B. Sunar, "A tamper-proof and lightweight authentication scheme," *Pervasive and Mobile Computing*, vol. 4, no. 6, pp. 807–818, 2008.

[63] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.

[64] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pp. 394–403, Miami Beach, FL, USA, 1997.

[65] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *International conference on the theory and applications of cryptographic techniques*, pp. 139–155, Springer, Berlin, Heidelberg, 2000.

[66] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *International Workshop on Public Key Cryptography*, pp. 65–84, Springer, Berlin, Heidelberg, 2005.

[67] J. He, Z. Yang, J. Zhang, W. Liu, and C. Liu, "On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 14, no. 1, 2018.

[68] S. Challa, M. Wazid, A. K. Das et al., "Secure signature-based authenticated key establishment scheme for future iot applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[69] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably-secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8065–8075, 2019.

[70] B. H. Taher, S. Jiang, A. A. Yassin, and H. Lu, "Low-overhead remote user authentication protocol for iot based on a fuzzy extractor and feature extraction," *IEEE Access*, vol. 7, pp. 148950–148966, 2019.

[71] P. Chandrakar and H. Om, "A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC," *Computer Communications*, vol. 110, pp. 26–34, 2017.

[72] Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[73] J. Mo and H. Chen, "A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks," *Security and Communication Networks*, vol. 2019, Article ID 2136506, 17 pages, 2019.