Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 9960264, 11 pages
https://doi.org/10.1155/2021/9960264

Research Article

An Efficient Scheme for Industrial Internet of Things Using Certificateless Signature

Ali Muhammad,[1] Noor Ul Amin,[1] Insaf Ullah,[2] Ahmed Alsanad,[3] Saddam Hussain,[1] Suheer Al-Hadhrami,[4] M. Irfan Uddin,[5] Hizbullah Khattak,[1] and Muhammad Asghar Khan[2]

[1]*Department of Information Technology, Hazara University, Mansehra 21120, Khyber Pakhtunkhwa, Pakistan*
[2]*Hamdard Institute of Engineering & Technology, Hamdard University, Islamabad 44000, Pakistan*
[3]*STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*
[4]*Computer Engineering Department, Engineering College, Hadhramout University, Hadhramout, Yemen*
[5]*Institute of Computing, Kohat University of Science and Technology, Kohat 2600, Pakistan*

Correspondence should be addressed to Insaf Ullah; insafktk@gmail.com and Ahmed Alsanad; aasanad@ksu.edu.sa

Received 24 March 2021; Revised 28 May 2021; Accepted 19 June 2021; Published 20 July 2021

Academic Editor: Dilbag Singh

Currently, hyperelliptic curve cryptography (HECC) got attractions towards low power devices such as Industrial Internet of Things (IIoT). As we all know, it has the capability of utilizing low key size, which can be suitable for IIoT environment. Inspired by the aforementioned property of HECC, we proposed an efficient scheme for IIoT using certificateless signature with the help of HECC. The presented approach is proven to be unforgeable against the challenges of type I and type II attackers. We tested the security of the designed approach through Automated Validation of Internet Security Protocols and Applications (AVISPA). We also performed the computational and communicational cost comparisons with already existed schemes, and it is observed from our analysis that our scheme is computationally efficient and needs low communication cost.

1. Introduction

Internet of Things (IoT) is a network of physical interconnected devices, which incorporate embedded technologies such as RFID, sensors, and other smart devices [1, 2], networked together for communicating with the external environments via the Internet [3, 4]. On the other hand, IoT is growing its scope through linking cities to mature smart systems. These smart systems are designed to combine our routine items with smart devices to create a fully automated intelligent system (AIS) that has the potential to reduce human effort. According to a recent Ericsson report, about 18 billion smart IoT devices will be connected to the Internet by 2022 [5]. This new innovative trend has paved the way for integrating these innovative technologies into various fields such as healthcare, data mining, transportation, and commerce [6–10]. Since its first proposal [11], IoT has attained considerable admiration among the research community in both pedagogy and industries [12].

Recently, IoT has been used in the industry to enhance and modernize the industrial progression by integrating with cyberphysical systems (CPS) termed as Industrial Internet of Things (IIoT). The purpose behind the introduction of IIoT is to maximize the flow of production within the industry and to equip smart machines with sensors and wireless connectivity [13]. Though, the continuous expansion of IIoT with cloud storage that shines through remote access service, low cost, high data availability, and extended and high data storage is becoming more popular among both individuals and enterprises [12]. A general picture of IIoT with a cloud server environment is shown in Figure 1, where the enterprises can monitor the condition of deployed

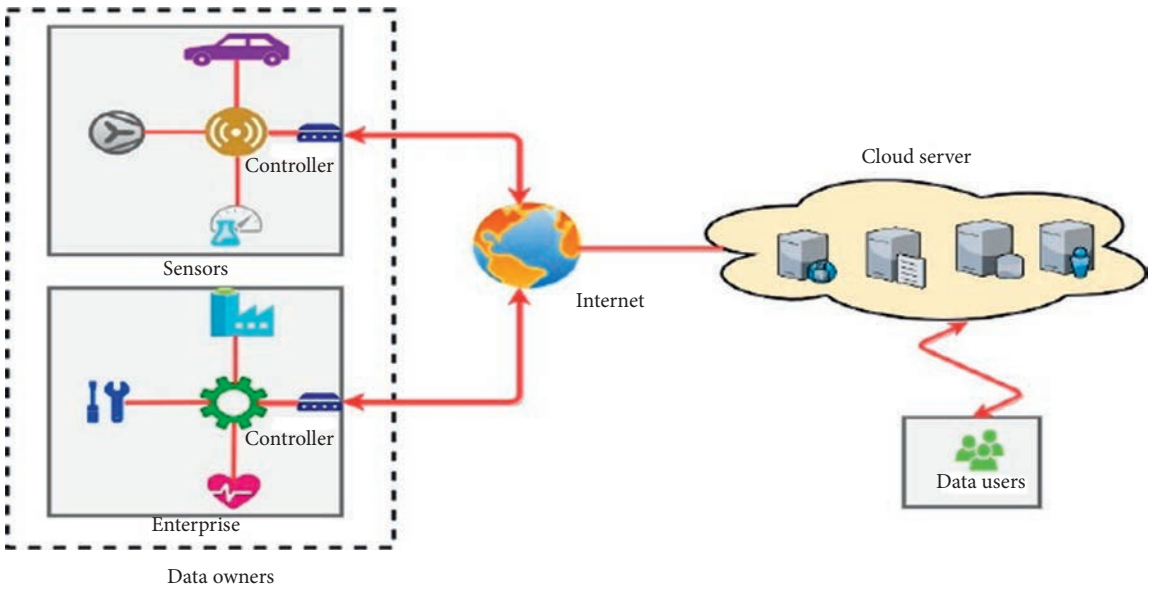

Figure 1: A general picture of IIoT connected to the cloud server.

devices. It can collect the relevant data throughout the industrial production system and send it to the controller. However, additional information can be collected using the services of sensors. The collected data are then forwarded to the cloud server by the controller over the Internet. Cloud servers have the potential to address the serious challenges of data storage, data processing, and data classification through data-based services to improve the reliability of IIoT environment [14]. Besides the positive aspects, the cloud servers can easily be intercepted where frequent sensitive data and information can be easily disclosed and leaked.

Despite the constant development and research in the IIoT technology, security risks still fail its comprehensive applications [15–19]. Consider the generic IIoT scenario in which the application sends collected data through a public channel. In such case, due to the open nature of the channel contact, an attacker can carry out multiple attacks, such as injecting, intercepting, responding, and modifying. By doing so, the attacker could damage the repute and assets of data owners and data consumers [20–24].

To preserve a strategic distance from the above results, a significant number of studies have been conducted to confirm the integrity of the IIoT data for structural information [25–28]. Though, in the IIoT infrastructure [15, 21, 29], digital signature-based cryptography (DSBC) is considered to be efficient and reliable cryptography to achieve data integrity. Using DSBC, sensitive information can be easily authenticated in a nonreversible manner for the entire transmission phase period [30].

A certificateless signature approach is an auspicious contender that reduces the overhead of certificate managing and solves the key escrow that comes with identity-based signing approaches. The certificateless signature cryptography is based on a third party termed as the key generation center (KGC) which has a master secret key. Additionally, KGC also offers users a partial private key (PPK) that can be computed from each user's identity. The receiver user has a selected secret value that combines the secret value and PPK to create its own private key [31]. Next, the user associates the public parameter set with a secret value for generating their public key. Taking advantage of the above discussion, several schemes have been devised to prevent data authentication in IIoT structural information [32–37]. However, the mentioned schemes sustain high communication and computing costs.

Normally, to provide efficient and strong security with minimal computational and communicational overheads, the most common techniques used are RSA, bilinear pairing (BPG), elliptic curve cryptosystem (ECC), and hyperelliptic curve cryptosystem (HECC), respectively [38–44]. Among them, the HECC gives the same security with fewer key and parameter sizes [45, 46]. Therefore, the HECC is considered as an appropriate and efficient cryptographic mechanism that offers an improved performance in contrast to RSA, BPG, and ECC. Furthermore, the HECC uses 80 bits keys with efficient and strong security that can suit the IIoT environments.

1.1. Motivation and Contribution. Inspired from the abovementioned discussion, a new certificateless signature scheme has been proposed for IIoT infrastructure. The proposed scheme is primarily based on HECC categorized by its smaller key length. The main contribution of this work is listed.

(i) A cost-effective certificateless signature scheme is constructed for IIoT environment using HECC

(ii) We provide a proper algorithm for the proposed scheme that avoids key escrow problems and guarantees the security assets of unforgeability, man-in-the-middle attack, and antireplay attack

(iii) We validated the designed approach using a widely accepted validation tool (AVISPA) by using the popular backend protocols, i.e., on-the-fly model checker (OFMC) and constraint logic-based Attack Searcher (AtSe)

(iv) We also give the AVISPA code and simulation results that are available in the simulation study (Appendix) in Section 8

(v) In the end, a comprehensive comparative analysis against relevant schemes have been given which shows how our proposed scheme is better in terms of both communication and computation costs from them

1.2. Road Map of the Article. The article is arranged as follows: Section 2 discusses literature presented for IIoT environment. Section 3 discusses the threat model and the preliminaries of our proposed certificateless signature construction (CLSC) scheme. Similarly, Section 4 describes the proposed network model for certificateless signature. Section 5 includes the proposed algorithm. In Section 6, we described the informal security analysis for CLSC scheme. In Section 7, we compared the CLSC scheme against relative existing certificateless signature schemes. In Section 8, we give the simulation study (Appendix), and in Section 9, we concluded our proposed scheme.

2. Related Work

In order to minimize data management overhead due to the popularity and introduction of IIoT into modern digitization, most organizations are outsourcing their respective data on the cloud server. However, this revolution requires and needs to create some low overhead data authentication schemes.

For this purpose, Karati et al. [32] proposed a novel scheme for IIoT environment in certificateless settings. The authors claim that their scheme is safe against type I and type II adversaries under the standard model. Later, the scheme of Karati et al. [32] was found unsafe by [33, 34], against both type I and type II adversaries. Also, the security of Karati et al. scheme is on BPG. Naturally, BPG has the worst performance in terms of computing and communication resources and therefore does not correspond to the resource-limited setting of IIoT.

Zhang et al. [33] broke the scheme mentioned in [32] by showing that their scheme cannot resist type I and type II adversaries. However, the authors in [33] did not construct a new scheme for the claimed statements. Later in 2019, Zhang et al. [34] also improved the scheme of [32] by constructing a robust technique for IIoT in certificateless settings. The authors in [34] utilized the ECC algorithm to reduce the cost consumption of IIoT. Unfortunately, ECC works on 160 bits key size, which needs to be reduced further to suit the resource-constrained devices of IIoT. In the same year, Yang et al. [35] claim that the scheme of [34] is not secure against the public key replacement attack. According to Yang et al., an invader can effortlessly forge a valid signature utilizing a fake public key. However, the authors in [35] did not construct a new scheme for the claimed statements.

In 2019, Xiong et al. [36] presented a key-insulated signature scheme for IIoT using certificateless signature. The authors utilized the ECC algorithm under the random oracle model (ROM) to reduce the cost consumption of IIoT. As mentioned, ECC works on 160 bits key size that needs to be reduced further for resource-limited devices. Later, Rezaeibagha et al. [37] also improved the scheme of [32] by proposing a more concrete certificateless signature scheme under the standard model. The authors claim that their scheme is safe against type I and type II adversaries. However, Shim [47] proved the invalidity of the designed scheme against the type I adversary. Also, the security of [37] is based on BPG which does not correspond to the resource-limited setting of IIoT due to heavy pairing operations.

2.1. Outcomes of the Literature. The above schemes are constructed on the notion of BPG and ECC and hence withstand high computing and communication costs. Furthermore, the schemes mentioned in [33, 35] are unable to provide proper schemes for the claimed statements. Additionally, none of the previous schemes are validated by proper formal security tools such as AVISPA. For this reason, we suggest a lightweight certificateless signature scheme for IIoT using HECC.

3. Preliminaries

3.1. Hyperelliptic Curve Discrete Logarithm Problem (HDLP). Let $\vartheta \mathscr{E}\{1, 2, 3, 4, 5, \ldots, (q-1)\}$ and $\mathscr{L} = \vartheta \cdot D$; then, finding ϑ from the given equation is called HDLP.

3.2. Threat Model. The most well-known Dolev–Yao threat model was used for this study's certificateless signature scheme [48]. In this model, an adversary can intercept any open channel communications between two parties, which creates the possibility of eavesdropping, exchanging, and modifying messages. Given the use of wireless communications in IIoT environments, adversaries can contribute to sensitive data leakages.

Type I (A_1) and type II (A_{11}) challenges were considered for security clarification of the CLE scheme [49]. A description of these challenges is given as follows:

Type I ($\mathbf{A}_1$): A_1 is a malicious adversary, frequently regarded as an external attacker without master key access

Type II ($\mathbf{A}_{11}$): A_{11} is frequently regarded as an internal attacker (also a malicious KGC) with master key access but without the ability to replace public keys

Concerning the purpose of A_1 and A_{11} adversaries, these produce fake digital signatures for the scheme of core certificateless signature.

4. Network Model

The proposed scheme consists of entities comprised of application provider (AP), data owner (DO), cloud server (CS), and data clients as shown in Figure 2. The detailed descriptions of their role are given.

AP: it plays the role of KGC. The AP is accountable for selecting the master secret key and master public key. Moreover, it is also answerable for issuing mathematical parameters in the entire network. Additionally, it is answerable for producing a partial private key for all the participants.

DO: it is accountable for producing its respective private key and certificateless signature data of IIoT. Later, after signing, the DO sends the signed IIoT data to the CS, while the CS then sends the signed data to the intended clients, respectively.

CS: the CS is a potential service for both short-term and long-term data storage

Data clients: the data client is responsible for verifying the intended received data using his/her own private key.

5. Proposed Certificateless Signature Scheme

5.1. Certificateless Signature Construction (CLSC) Scheme. Consisting of the following four phases, the signature component is extracted from [50]: first, setup; second, key generation; third, signature; and fourth, verification. These phases lead to the practical formulation of a novel certificateless signature for real-world IIoT settings. Prior to beginning the algorithm's process, it is worth consulting the notation presented in Table 1.

5.1.1. Setup. A series of initial tasks are undertaken by an application provider (AP), which carries out the role of KGC. These tasks are as follows:

(i) AP chooses a prime number Q to serve as a master private key, where $Q \leqslant 1 \leqslant n-1$

(ii) AP generates the master public key by computing $R = Q \cdot D$

(iii) Public parameter set param = (R, D, $n = 280$, hEC) is selected

(iv) The chosen master private key Q is kept in AP storage memory, while param and R are issued in the entire network.

5.1.2. Key Generation. This phase consists of the following tasks:

(i) Partial private key generation (PPK): for a user with an identity $(I\ du)$, an AP undertakes the onward process for PPK. This involves the following steps: choosing ru, where $ru \leqslant 1 \leqslant n-1$; computing $Xu = ru \cdot D$; concatenating $Lu = (I\ du \| Xu)$; computing $Vu = (ru + Q \cdot Lu)$; and last, the AP sending (Vu, Xu) to the users. Together, the DC and DO calculate $Vu \cdot D = Xu + Lu \cdot R$, at the receiving end, thereby confirming a receiving PPK pair (Vu, Xu).

$$\begin{aligned} Vu \cdot D &\stackrel{?}{=} Xu + Lu \cdot R \\ &= Vu \cdot D = (\Upsilon u + Q \cdot Lu) \cdot D, \text{ where } Vu \\ &= (\Upsilon u + Q \cdot Lu) \\ &= (\Upsilon u \cdot D + Q \cdot Lu \cdot D) = Xu + Lu \cdot R, \end{aligned}$$

where $Xu = \Upsilon u \cdot D$ and $R = Q \cdot D$. (1)

(ii) Secret value generation: the secret value Qu is chosen randomly by the users (DO and DC), where $Qu \leqslant 1 \leqslant n-1$

(iii) Private key generation: the users (DO and DC) generate the private key by computing $\Omega u = (Vu, Qu)$

(iv) Public key generation: the users (DO and DC) generate the associated public key in the following way: computing $\mathscr{W}u = (Qu \cdot D)$, concatenating $uu = (I\ du \| \mathscr{W}u)$, computing $Pu = (Xu \| uu \cdot \mathscr{W}u)$, and at last, setting the public key by concatenating $\beta u = (Xu \| u)$.

5.1.3. Signature. To generate a signature, the DO undertakes the following:

(i) Choose w, where $w \leqslant 1 \leqslant n-1$, compute $\mathscr{N} = w \cdot D$.

(ii) Calculate $z = (m \| I\ dD\ o \| \tau)$, where Id Do denotes identity DO

(iii) Calculate $\delta = \mathscr{Q}\ Do + (V\ Do + w) \cdot \mathscr{Z}$, $(\mathscr{Q}\ Do, V\ Do)$ is DO's private key pair

(iv) Calculate the DC signature as $\Phi = (\mathscr{N}, \delta)$

5.1.4. Verification. The DC validates the signature through the following computations:

(i) To begin, compute $\mathscr{G} = X\ Do + R \cdot (I\ dD\ o \| X\ Do \| \ Do)$, where (X $Do \| \ Do$) is DO's public key

(ii) Accept ϕ, if $\delta \cdot D = \mathscr{G} + \mathscr{N} \cdot h(m \| I\ dD\ o \| \tau) + h(m \| I\ dD\ o \| \tau)$

5.1.5. Consistency. Here, DC accepts ϕ upon successful computation.

$$\begin{aligned} \delta \cdot D &= \mathscr{G} + \mathscr{N} \cdot (m \| I\ dD\ o \| \tau) + \mathscr{W}u \cdot (m \| I\ dDo \| \tau) \\ &= (\mathscr{Q}\ Do + (V\ Do + w) \cdot \mathscr{Z}) \cdot D \\ &= (\mathscr{Q}\ Do + (V\ Do + w) \cdot (m \| I\ dDo \| \tau)) \cdot D, \quad \text{where} \\ &\quad \mathscr{Z} = (m \| I\ dDo \| \tau) \\ &= (\mathscr{Q}\ Do + (V\ Do\ \cdot (m \| I\ dD\ o \| \tau) + w \cdot (m \| I\ dDo \| \tau)) \cdot D \\ &= (\mathscr{W}\ DO + V\ Do\ \cdot D \cdot (m \| I\ dDo \| \tau) + w \cdot D \\ &\quad \cdot (m \| I\ dDo \| \tau), \quad \text{where } \mathscr{W}\ DO = \mathscr{Q}\ DO\ \cdot D. \end{aligned}$$

(2)

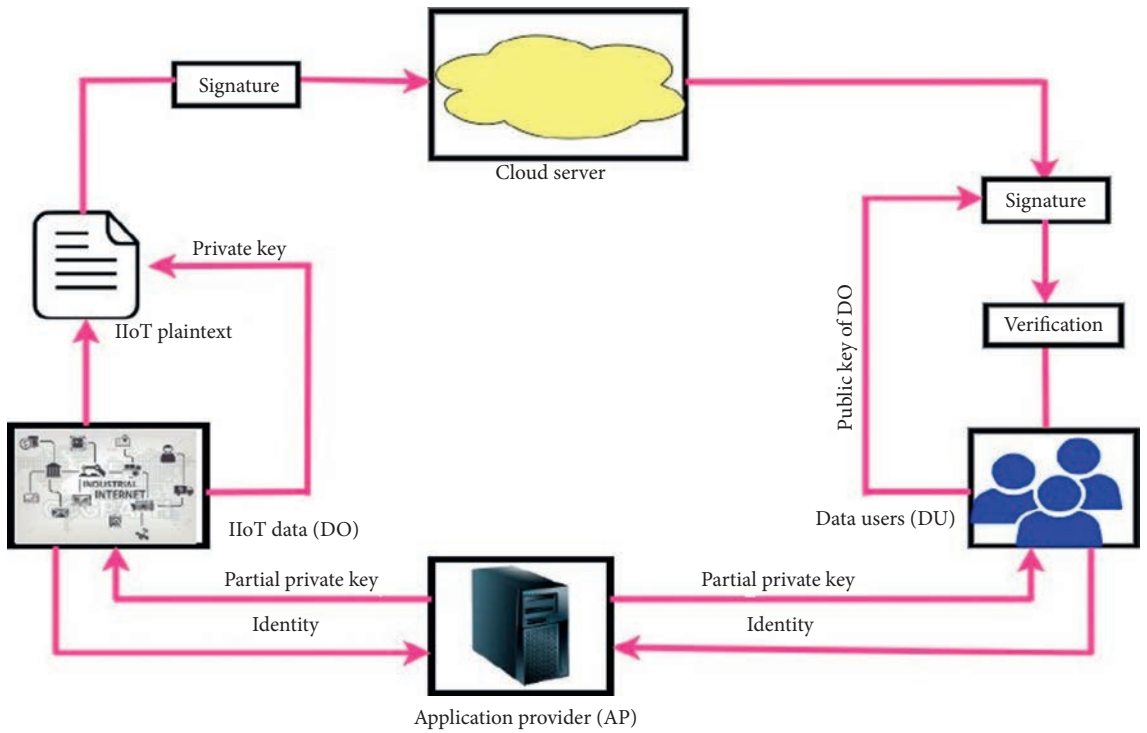

Figure 2: Designed network model for IIoT.

Table 1: Symbols of the proposed algorithm.

Symbol	Description
AP	Application providers
Idu	Identity of any participating user
Q	KGC master private key
D	Hyperelliptic curve divisor
N	Prime no. with size $n = 2^{80}$
R	KGC master public key
PPK	Partial private key
KGC	Key generation center
$Q\ DC$	Secret values of data consumers
$Q\ DO$	Secret values of data owners
$\Omega\ DO$	Data user private key
Ω DC	Data consumer private key
DO	Data owners
DC	Data consumers
$\mathbf{A}_1$	Type I attacker
$\mathbf{A}_{11}$	Type II attacker
$\|$	Concatenation

6. Security Analysis

6.1. Theorem A (Unforgeability). A certificateless signature scheme has the property of unforgeability if it is impossible for adversaries $\mathbf{A}_1$ and $\mathbf{A}_{11}$ to undermine the sender's private key and produce a forged signature on data.

Proof. Initially in the design scheme, a sender generates a signature on plaintext $\delta = \mathcal{Q}\,\mathrm{Do} + (V\,\mathrm{Do} + w) \cdot \mathcal{Z}$. With the public channel, the signature $\Phi = (\mathcal{N}, \delta)$ is forwarded to the receiver.

Case 1 If $\mathbf{A}_1$ tries to create a forge digital signature, then it needs to calculate w from $Q\,\mathrm{Do} + (V\,\mathrm{Do} + w) \cdot \mathcal{Z}$, and to do so, it further requires w from $\mathcal{N} = w \cdot D$, where w is not known and D is a divisor of HECC. Subsequently, it is not feasible for $\mathbf{A}_1$ to solve HCDLP. Hence it is proved from the mentioned discussion that the designed scheme meets the security requirements of unforgeability against an outside attacker.

Case 2 If $\mathbf{A}_1$ tries to forge a signature, it will need to calculate $\mathcal{Q}\ Do$ from $\mathcal{Q}\ Do + (V\ Do + w) \cdot \mathcal{Z}$

that further requires $\mathcal{Q}\ Do$ from $\mathcal{W}\ Do = \mathcal{Q}\ Do\ \cdot D$, where $\mathcal{Q}\ Do$ is a secret value of the DO and D is a divisor of HECC. Consequently, it is not achievable for $\mathbf{A}_1$ to solve HCDLP. Hence it is proved from the mentioned discussion that the designed scheme meets the security requirements of unforgeability against an outside attacker in case two.

Case 3 In the given case, if A_1 tries to create a forge digital signature, it will need to calculate $V\ Do$ from $\mathcal{Q}\ Do + (V\ Do + w) \cdot \mathcal{Z}$ that furthers require $V\ Do$ from $V\ Do = (\Upsilon\ Do + Q \cdot L\ Do)$, where $\gamma\ Do$ is a private number of DO and Q is a master secret key of KGC. Consequently, it is not achievable for $\mathbf{A}_1$ to calculate unknown values from an equation. Hence, demonstrated from the mentioned discussion, the designed scheme meets the security requirements of unforgeability against an outside attacker in case three. □

6.2. Theorem Unforgeability. Here, if the $\mathbf{A}_{11}$ tries to forge a signature, it needs to calculate $V\ Do$, w, and $\mathcal{Q}\ Do$ from $\mathcal{Q}\ Do + (Do + w) \cdot \mathcal{Z}$ as the key generation center only has $V\ Do = (\Upsilon\ Do + Q \cdot L\ Do)$, since $V\ Do$ has been calculated by the key generation center.

Case 1 If $\mathbf{A}_{11}$ tries to create a forge digital signature, then it will need to calculate w from $\mathcal{Q}\ Do + (V\ Do + w) \cdot \mathcal{Z}$, and to do so, it further requires w from $\mathcal{N} = w \cdot D$, where w is not known and D is a divisor of HECC. Subsequently, it is not feasible for $\mathbf{A}_1$ to solve HCDLP. Hence it is proved from the mentioned discussion that the designed scheme meets the security requirements of unforgeability against insider attackers.

Case 2 If $\mathbf{A}_1$ tries to forge a signature, it will need to calculate $\mathcal{Q}\ Do$ from $\mathcal{Q}\ Do + (V\ Do + w) \cdot \mathcal{Z}$ that further requires $\mathcal{Q}\ Do$ from $\mathcal{W}\ Do = \mathcal{Q}\ Do\ \cdot D$, where $\mathcal{Q}\ Do$ is a secret value of the DO and D is a divisor of HECC. Consequently, it is not achievable for $\mathbf{A}_{11}$ to solve HCDLP. Hence it is proved from the mentioned discussion that the designed scheme meets the security requirements of unforgeability against insider attack in case two.

6.3. Theorem of Antireplay Attack. A certificateless signature scheme is supposed to accomplish the security requirement of an antireplay attack, if there is no possible adversary that can capture some old communication messages and resent them again to the intended receiver.

Proof. In the proposed scheme, at first, the data consumer (DC) sends a request to the data owner (DO) with a fresh nonce τ. The DO then sends τ with the original signature computed by him. After the given process, the DO sends the signed message $= \mathcal{Q}\ Do + (Do + w) \cdot \mathcal{Z}$ to the DC. Therefore, the DC checks the freshness of τ. □

6.4. Theorem of Man-in-the-Middle Attack. A certificateless signature scheme is supposed to attain the security requirements of man-in-the-middle attack, if there is no possible adversary that can obtain the signature made by DO.

Proof. If the adversary tries to obtain the signature, it first needs to calculate $V\ Do$, w, and $\mathcal{Q}\ Do$ from $\delta = \mathcal{Q}\ Do + (V\ Do + w)\mathcal{Z}$. Though, it has been demonstrated in the abovementioned Theorem 1. Hence, we can claim that the designed scheme is safe against the security issue of man-in-the-middle attack. □

7. Performance Analysis

Here, we analyze the performance of the designed approach in contrast to Zhang et al. [34], Karati et al. [32], Rezaebagha et al. [37], and Xiong et al. [36]. Moreover, we will also discuss the efficiency of the proposed scheme over the previous schemes in terms of computation cost and communication overhead.

7.1. Computational Cost. For performance efficiency in terms of computation cost, we compared our proposed scheme with Zhang et al. [34], Karati et al. [32], Rezaebagha et al. [37], and Xiong et al. [36]. The results of the comparison are given in Table 2. Though, previous schemes utilized BPG and ECC very expensive for a resource-limited environment. Therefore, we used the HECC to reduce the computation cost for the IIoT.

From [41, 51], we observed the timing of the major observations used in the comparative analysis in terms of computation cost. According to [41, 51], a single bilinear pairing ($\mathcal{B}p$) operation will take 14.90 ms, paring-based point multiplication ($p\mathcal{B}\mathcal{M}$) will take 4.31 ms, scalar point multiplication ($\mathcal{E}pp\mathcal{M}$) will take 0.97 ms, and modular exponentiation ($\mathcal{M}\mathcal{E}$) will take 1.25 ms, respectively. Similarly, a single hyperelliptic curve divisor multiplication ($\mathcal{H}\mathcal{E}pp\mathcal{M}$) will take 0.48 ms [52, 53]. For measuring the efficiency, we take the MIRACL library with the given specifications: Intel Core i74510 CPU with 2.0 GHz processor, 8 GB RAM, and OS of 64 bits Windows 7 [41].

Similarly, we also compare the designed scheme with the scheme of Zhang et al. [34], Karati et al. [32], Rezaebagha et al. [37], and Xiong et al. [36] in terms of communication overhead. For our comparative analysis, we take the variables and their size as 1024 bits for bilinear pairing, 160 bits for elliptic curves, and 80 bits for the hyperelliptic curve. Moreover, the communication overhead of all the related schemes and the proposed scheme is given in Table 2.

The findings of the comparative analysis are shown in Table 3, Figures 3 and 4. Furthermore, Tables 4 and 5 show a clear improvement in both communication overhead and computation cost.

Table 2: Comparison in terms of costly operations.

Reference no.	Signing phase	Verification phase	Total computation cost	Ciphertext size in bits
[32]	$2\mathcal{ME}$	$2\mathcal{ME} + \mathcal{B}p$	$4\mathcal{ME} + \mathcal{B}p$	$2\|G\|$
[34]	$p\mathcal{B}p\mathcal{M}$	$\mathcal{B}p + p\mathcal{B}p\mathcal{M}$	$1\mathcal{B}p + 2p\mathcal{B}\mathcal{M}p$	$2\|G\|$
[36]	$1\mathcal{E}pp\mathcal{M}$	$6\mathcal{E}pp\mathcal{M}$	$7\mathcal{E}pp\mathcal{M}$	$3\|q\|$
[37]	$\mathcal{ME}$	$2\mathcal{B}p$	$1\mathcal{ME} + 2\mathcal{B}p$	$2\|G\|$
Proposed scheme	$2\mathcal{HE}pp\mathcal{M}$	$4\mathcal{HE}pp\mathcal{M}$	$6\mathcal{H}pp\mathcal{M}$	$2\|n\|$

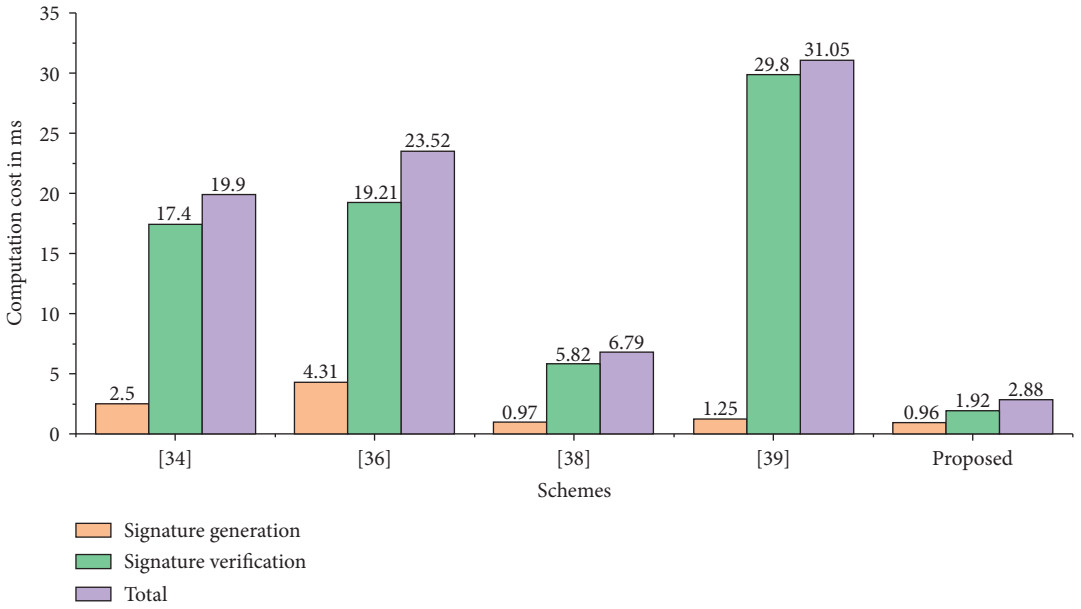

Figure 3: Computational cost analysis.

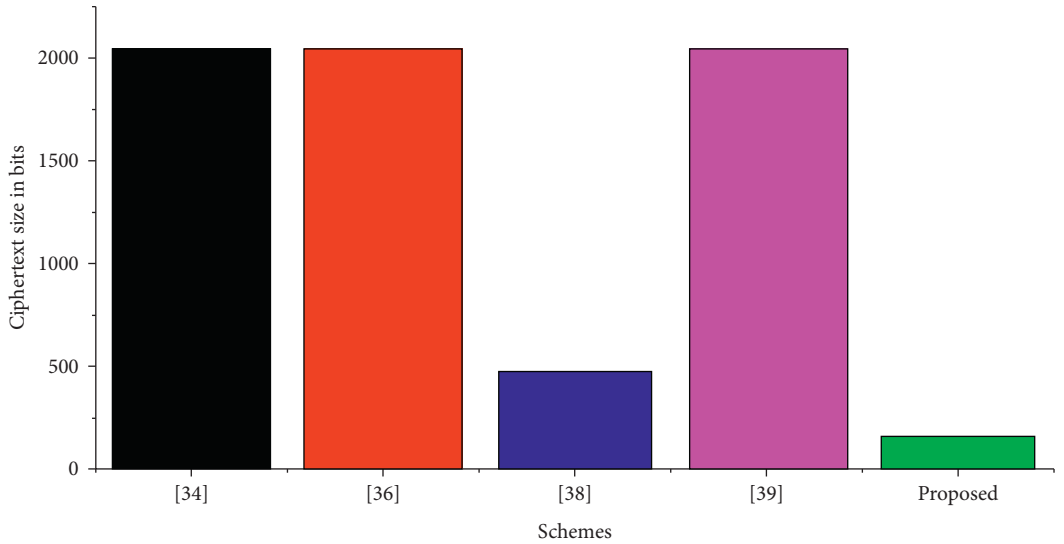

Figure 4: Communication cost analysis.

Table 3: Computational cost analysis in milliseconds.

Reference no.	Signature generation	Signature verification	Total
[32]	2.5	17.4	19.9
[34]	4.31	19.21	23.52
[36]	0.97	5.82	6.79
[37]	1.25	29.8	31.05
Proposed scheme	0.96	1.92	2.88

Table 4: Reduction of total computational cost.

Reference no.	Computational cost (x)	Computational cost (y)	Computational cost reduction (z) in percentage
[32]	19.9	2.88	85.52
[34]	23.52	2.88	87.75
[36]	6.79	2.88	57.58
[37]	31.05	2.88	90.72

Percentage change = $((x - y)/x) * 100$.

Table 5: Communicational overhead reduction.

Reference no.	Communication cost (x)	Communication cost (y)	Cost reduction in % (z)
[32]	2048	160	92.18
[34]	2048	160	92.18
[36]	480	160	66.66
[37]	2048	160	92.18

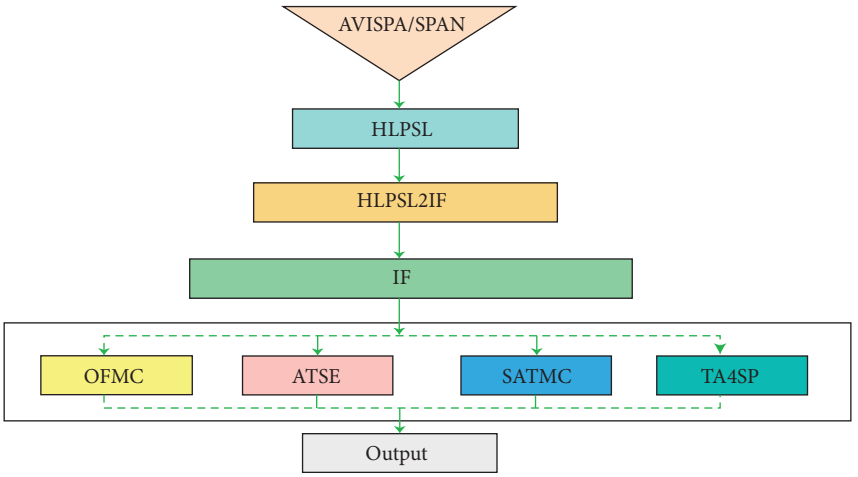

Figure 5: AVISPA basic structure.

Figure 6: Simulation results for on-the-fly model checker (OFMC).

8. Simulation Study (Appendix)

AVISPA [54], an industrial-grade security simulator, was used for security validation of the proposed scheme. The AVISPA simulator can be in one of two states: SAFE if the scheme is resistant to malicious attacks, and otherwise, UNSAFE (Figure 5).

For GUI support, AVISPA is combined with SPAN, and the rule-oriented high-level protocol specification language (HLPSL) is available for specifying a scheme. Through intermediate format (IF) specifications, an HLP2IF translator is used to compile HLPSL into machine language [46, 48]. Regarding the role of these IF specifications, they serve as inputs to the backend checker, which can be the SAT-based model-checker (SATMC), on-the-fly-model checker (OFMC), tree-automata-based protocol analyzer (TA4SP), or CL-based attack searcher (CL-AtSe). Based on the proposed cryptographic scheme's requirements, the functionality of every backend is distinctive [55]. DO and DC are the primary roles in the proposed scheme verification process, and the results indicate that the security of the scheme is grounded in CL-AtSe and OFMC. Information about the signature and verification codes and simulation results are presented in Figures 6–9 .

```
role role_Signer (Singer:agent, Varifier:agent, βdo:public_key,
βdc:public_key, SND, RCV:channel(dy))

played_by Singer
def =
        local
                State:nat, Non:text, Mul:hash_func, W:text, Z:text,M:text
        init
                State := 0
        transition
                1. State = 0 ∧ RCV(start) =|> State′:=1 ∧ SND(Signer. Varifier)
                2. State = 1 ∧ RCV(Varifier.{T′}_βdc) =|> State′:=2 ∧ W′:=new() ∧ Z′:=new()∧ M′:= new() ∧
SND(Signer.{(Mul(Z′.W′)}_inv(βdo))
end role
```

Figure 7: Signature using the HLPSL code.

```
role role_Varifier (Singer:agent, Varifier:agent, βdo:public_key,
βdc:public_key, SND, RCV:channel(dy))
Played_by Varifier
def =
    local
        State:nat, T:text, Mul:hash_func, Z:text, W:text, M:text
    init
        State := 0
    transition
        1. State = 0 ^ RCV(Signer. Varifier) =|> state′ := 1 ^ T′ := new0 ^ SND(Signer.{T}_βdc)
        6. State = 1 ^ RCV(signer.{Mul(W′.Z′)}_inv(βdo)) =|> State' := 2
end role
```

Figure 8: Verification using the HLPSL code.

Figure 9: Simulation results for AtSe.

9. Conclusion

This study presents an efficient scheme for IIoT using certificateless signature with the help of the hyperelliptic curve cryptosystem (HCC). The presented approach is proven to be unforgeable against the challenges of type I and type II attackers. The security of the proposed work is tested through a popular tool "AVISPA." A comprehensive comparative analysis against relevant schemes has been given which shows how our proposed scheme is better in terms of both communication and computation costs from them. Based on the above claims, we argue that the designed scheme will be the best option for the resource-limited devices in terms of cost consumptions.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

References

[1] J.-S. Pan, L. Kong, T.-W. Sung, P.-W. Tsai, and V. Snášel, "A clustering scheme for wireless sensor networks based on genetic algorithm and dominating set," *Journal of Internet Technology*, vol. 19, no. 4, pp. 1111–1118, 2018.

[2] J.-S. Pan, L. Kong, T.-W. Sung, P.-W. Tsai, and V. Snášel, "α-fraction first strategy for hierarchical model in wireless sensor networks," *Journal of Internet Technology*, vol. 19, no. 6, pp. 1717–1726, 2018.

[3] J. Sun, Y. Bao, X. Nie, and H. Xiong, "Attribute-hiding predicate encryption with equality test in cloud computing," *IEEE Access*, vol. 6, pp. 31621–31629, 2018.

[4] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2739–2750, 2018.

[5] Ericsson, *The Connected Future*, https://www.ericsson.com/en/mobility-report/internet-of-things-forecast, Ericsson, Kista, Stockholm, Sweden, 2021, https://www.ericsson.com/en/mobility-report/internet-of-things-forecast.

[6] J. C.-W. Lin, L. Yang, P. Fournier-Viger, and T.-P. Hong, "Mining of skyline patterns by considering both frequent and utility constraints," *Engineering Applications of Artificial Intelligence*, vol. 77, pp. 229–238, 2019.

[7] J. M.-T. Wu, M.-H. Tsai, and Y. Zhi Huang, "Applying an ensemble convolutional neural network with Savitzky–Golay

filter to construct a phonocardiogram prediction model," *Applied Soft Computing*, vol. 78, pp. 29–40, 2019.

[8] J. M.-T. Wu, J. C.-W. Lin, P. Fournier-Viger, Y. Djenouri, C.-H. Chen, and Z. Li, "The density-based clustering method for privacy-preserving data mining," *Mathematical Biosciences and Engineering*, vol. 16, no. 3, pp. 1718–1728, 2019.

[9] W. Gan, J. C. W. Lin, P. Fournier-Viger, H. C. Chao, and S. Y. Philip, "HUOPM: high-utility occupancy pattern mining," *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1195–1208, 2019.

[10] J. C.-W. Lin, Y. Zhang, B. Zhang, P. Fournier-Viger, and Y. Djenouri, "Hiding sensitive itemsets with multiple objective optimization," *Soft Computing*, vol. 23, no. 3, pp. 1–19, 2019.

[11] H. Sundmaeker, P. Guillemin, P. Friess, and S. WoelfflØ, "Vision and challenges for realising the internet of things," in *Cluster of European Research Projects on the Internet of Things*European Commision, Brussels, Belgium, 2010.

[12] T. Y. Wu, C. M. Chen, K. H. Wang, and J. M. T. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232–49239, 2019.

[13] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, Article ID 102481, 2020.

[14] S. Hussain, I. Ullah, H. Khattak et al., "A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for internet of things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[15] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys &Tutorials*, vol. 17, no. 3, pp. 1294–312, 2015.

[16] C. Kolias, G. Kambourakis, A. Stavrou, and J. M. Voas, "DDoS in the IoT: mirai and other botnets," *IEEE Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[17] G. Kambourakis, C. Kolias, and A. Stavrou, "The mirai botnet and the iot zombie armies," in *Proceedings of the 2017 IEEE Military Communications Conference*, pp. 267–272, Baltimore, MD, USA, October 2017.

[18] J. M. Voas, R. Kuhn, C. Kolias, A. Stavrou, and G. Kambourakis, "Cybertrust in the IoT age," *IEEE Computer*, vol. 51, no. 7, pp. 12–15, 2018.

[19] C. Kolias, W. Meng, G. Kambourakis, and J. Chen, "Security, privacy, and trust on internet of things," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 6452157, 3 pages, 2019.

[20] F. Amini, M. Khan, and J. V. Misic, "IEEE 802.15.4: signature-based intrusion detection in wireless sensor networks (WSNS)," *Encyclopedia of Wireless and Mobile Communications*, Taylor & Francis, Oxfordshire, UK, 2012.

[21] M. B. M. Noor and W. H. Hassan, "Current research on internet of things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[22] 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*, 2020.

[23] 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.

[24] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, and J. Ma, "Shake to communicate: secure handshake acceleration-based pairing mechanism for wrist worn devices," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5618–5630, 2019.

[25] 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.

[26] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in iot environment," *IEEE Internet Things of Journal*, vol. 4, no. 5, pp. 1634–1646, 2017.

[27] 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.

[28] H. Xiong, Y. Bao, X. Nie, and Y. I. Asoor, "Server-aided attribute-based signature supporting expressive access structures for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1013–1023, 2020.

[29] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," *IEEE Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[30] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Network*, vol. 20, no. 8, pp. 2481–2501, 2014.

[31] G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, and D. V. R. K. Reddy, "Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1641–1645, 2020.

[32] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3701–3711, 2018.

[33] B. Zhang, T. Zhu, C. Hu, and C. Zhao, "Cryptanalysis of a lightweight certificateless signature scheme for IIoT environments," *IEEE Access*, vol. 6, pp. 73885–73894, 2018.

[34] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5099–5108, 2019.

[35] W. Yang, S. Wang, X. Huang, and Y. Mu, "On the security of an efficient and robust certificateless signature scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 91074–91079, 2019.

[36] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Systems Journal*, vol. 14, no. 1, 2019.

[37] F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, and K. Huang, "Fully secure lightweight certificateless signature scheme for IIoT," *IEEE Access*, vol. 7, pp. 144433–144443, 2019.

[38] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, p. 3868, 2018.

[39] M. Yu1, J. Zhang, J. Wang et al., "Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, pp. 1–15, 2018.

[40] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, p. 352, 2018.
[41] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, Article ID 8405879, 17 pages, 2017.
[42] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, pp. 6428–6453, 2017.
[43] A. Omala, A. Mbandu, K. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," vol. 42, 2018.
[44] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *International Journal of Advanced Studies of Scientific Research*, vol. 3, 2019.
[45] V. Naresh, R. Sivaranjani, and N. V. E. S. Murthy, "Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks," *International Journal of Communication Systems*, vol. 31, Article ID e3763, 2018.
[46] A. Rahman, I. Ullah, M. Naeem, R. Anwar, H. Khattak, and S. Ullah, "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve," *International Journal of Advanced Computer Science and Applications*, vol. 9, 2018.
[47] K.-A. Shim, "Security vulnerabilities of four signature schemes from NTRU lattices and pairings," *IEEE Access*, vol. 8, 2020.
[48] 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.
[49] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-Proceedings of ASIACRYPT03, LNCS 2894*, pp. 452–473, Springer-Verlag, Berlin, Germany, 2003.
[50] I. Ullah, N. Ul Amin, M. Zareei et al., "A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications," *Symmetry*, vol. 11, p. 1386, 2019.
[51] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2019.
[52] M. A. Khan, I. Ullah, S. Nisar et al., "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[53] S. S. Ullah, I. Ullah, H. Khattak et al., "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with internet of things," *IEEE Access*, vol. 8, 2020.
[54] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, and J. Cuéllar, "The AVISPA tool for the automated validation of internet security protocols and applications," in *Proceedings of the 2005 17th International Conference on Computer Aided Verification*, pp. 281–285, Edinburgh, Scotland, UK, July 2005.
[55] J. Jung, D. Kang, D. Lee, and D. Won, "An improved and secure anonymous biometric-based user authentication with key agreement scheme for the integrated epr information system," *PLoS One*, vol. 12, no. 1, 2015.