Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7336279, 8 pages
https://doi.org/10.1155/2022/7336279

Research Article

Certificate-Based Signature Scheme for Industrial Internet of Things Using Hyperelliptic Curve Cryptography

Insaf Ullah,[1] Ali Alkhalifah,[2] Maha M. Althobaiti,[3] Fahd N. Al-Wesabi,[4] Anwer Mustafa Hilal,[5] Muhammad Asghar Khan,[1] and Jimmy Ming-Tai Wu[6]

[1]*Hamdard University Karachi, Islamabad Campus, Islamabad 44000, Pakistan*
[2]*Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia*
[3]*Department of Computer Science, College of Computing and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*
[4]*Department of Computer Science, College of Science & Art, King Khalid University, Abha, Saudi Arabia*
[5]*Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, AlKharj, Saudi Arabia*
[6]*College of Computer Science and Technology, Shandong University of Science and Technology, Shandong, China*

Correspondence should be addressed to Jimmy Ming-Tai Wu; wmt@wmt35.idv.tw

Received 27 October 2021; Revised 9 December 2021; Accepted 3 January 2022; Published 8 February 2022

Academic Editor: Zahid Khan

The Industrial Internet of Things (IIoT) is a technology that uses the Internet of Things (IoT) infrastructure to sense, process, and communicate real-time events in the industrial system to cut down on unnecessary operating costs and to speed up industrial automation of internal and external working processes. Since the IIoT system inherits the same cyber-physical vulnerabilities that the IoT system already encounters, it requires additional work to address security concerns owing to its heterogeneous nature. As a result, an efficient security mechanism is essential to protect against various and unknown cyber-attacks. In this article, we propose a certificate-based signature scheme based on hyperelliptic curve cryptography (HECC), with the aim of improving security while reducing computational and communication costs in the IIoT environment. The proposed scheme outperforms existing schemes in terms of both computational and communication costs, as well as offering better security.

1. Introduction

The term "Industrial Internet of Things" (IIoT) refers to the use of Internet of Things (IoT) devices and infrastructure to collect and communicate real-time events in industrial systems in order to reduce human efforts and operational costs while also improving manufacturing and industrial processes [1]. Chemical factories, for example, are a good example of industrial processes since they include highly sensitive processes that require real-time communication between machines and other entities [2]. One of the advanced tiers of networking design, termed Fifth Generation (5G) mobile networks, appears to give a worthy communication in the digital words of IIoT [3]. The International Data Corporation (IDC) report that globally 70% of companies spend $1.2 billion on 5G connectivity management solutions. When 5G and IIoT (5G-IIoT) are combined, a rapid, intelligent, and ubiquitous communication system emerges [4]. Additionally, 5G mobile networks support a cutting-edge technology known as cloud computing [5], which ensures the storage, processing, analysis, and exchange of data generated by IIoT devices. A traditional cloud computing paradigm, on the other hand, is incapable of effectively managing data directly. Because the sensor has limited resources, it will be unable to process the complicated intelligent algorithms. A mobile edge node with extra attributes of powerful processing and storage capacity will be employed to overcome this challenge. In Figure 1, collaborative technologies such as 5G, cloud server (CS), edge computing (EC), and bluetooth low energy (BLE) are used to create an infrastructure for an IIoT environment.

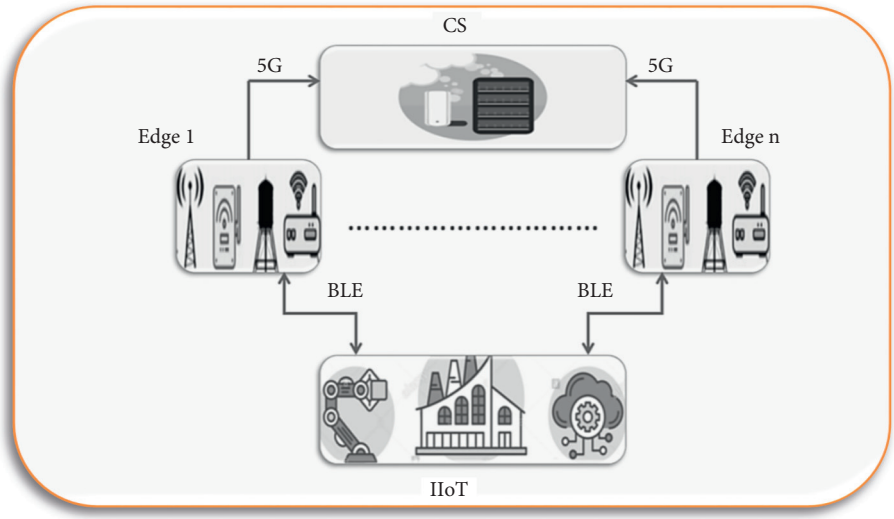

Figure 1: A collaborative technology architecture for IIoT.

However, in an IIoT setting, a malicious sensor can put the entire network at risk, necessitating the use of a robust authentication mechanism [6]. For the purpose of ensuring integrity and authenticity, the digital signature procedure is used [7]. Digital signatures are public key cryptographic primitives (PKCP), which are classified into three categories: public key environment (PKE), identity-based environment (IBE), and certificateless environment (CE). In the cryptography/information security field, PKE has got a lot of attention. It does, however, have severe flaws in terms of certificate management and revocations. Then, when a trusted agent (TA) or organization receives the participant identification, IBE removes certificate management and revocation concerns, and a trusted agent (TA) or organization creates the private key for participating devices. The secret key was provided with participants through a dedicated link by TA. However, if TA so desires, it will provide the opponent with the private key, so that he or she may generate a real signature of the participants. The CE resolves the issue of participant signature forgery in IBE by eliminating the process of private key generation from the TA and having the TA produce the partial private key (PPK) for the participating users, which is then shared with participants via a dedicated link. Sharing PPK with participants, on the other hand, necessitates a dedicated link with participants, which is a major concern in CE.

The certificate-based environment (CBE) is an enhanced version of PKCP that overcomes the limitations of PKE, IBE, and CE by removing the need for certificate management and revocations, as well as a dedicated link for exchanging private key and PPK with participants. The CBE is a hybrid of PKE and IBE in which the participant sends his identification to the TA, who subsequently generates a certificate using his private key and public parameters, as well as the participant's identity. Furthermore, instead of utilizing a dedicated link, TA provides the certificate to that user, and the participants create their private and public keys. PKCP security and efficiency are usually determined by mathematical parameters. Because it substitutes elliptic curve (EPC) with an extra package of low key and parameter size, the mathematical aspects of hyperelliptic curve (HPEC) have received increased attention when creating protocols for resource hungry environments [8]. As we all know, bilinear pairing is worse than EPC and RSA; thus, we can conclude that HPEC is the best option for building a scheme for the IIoT environment. As a result, using collaborative technologies such as 5G, cloud computing, and edge computing, we introduced a new intelligent certificate-based signature for IIoT in this article. The following are the study's key contributions:

(i) We propose a HECC-based certificate-based signature scheme for IIoT security, which improves security while having a small key size.

(ii) We introduce an edge computing architecture for IIoT that uses BLE to directly access data from IIoT devices and transmits it to a cloud server through a 5G wireless link.

(iii) We use the random oracle model (ROM) to undertake a formal security analysis of the proposed scheme, ensuring that it is secure against type 1 and type 2 adversaries.

(iv) We compare the computation and communication costs of the proposed scheme to some of the existing schemes, demonstrating that our scheme is more efficient.

The organization of the article is set out as follows. The related work on certificate-based signature schemes is presented in Section 2. We go through the network model in Section 3, which also includes network and threat models. In Section 4, the proposed model and algorithm are defined. Section 5, on the other hand, provides the proposed scheme's security analysis. In addition, we discuss performance analysis in Section 6. The conclusion is presented in Section 7.

2. Related Works

The major security measures rely on cryptographic concepts to ensure authenticity, confidentiality, and integrity. A well-designed data security strategy may greatly reduce the likelihood of data being compromised. Kang et al. [9] presented a certificate-based signature with the help of pairings on elliptic curves, and its security analysis is provided by utilizing the random oracle model. Then, Li et al. [10], analyzed the presented scheme in [9], and they say that it is suffering from key replacement attack. Furthermore, they proposed an enhanced certificate-based signature with the use of lower length operations. However, the scheme presented in [9, 10] will definitely suffer by higher computational cost due to expensive pairing operations. To avoid such limitations, Liu et al. [11] presented a new certificate-based signature by not entertaining the expensive operations of bilinear pairing. However, it can still be affected by exponential operations when we consider today's resource hungry IoT devices. Also, Zhang [12] stated that the scheme presented in [11] is suffering from certain security flaws and proposed new approach with the help of pairing operations. Ming and Wang [13] presented a new certificate-based signature by not entertaining the expensive operations of bilinear pairing. Li et al. [14] presented a new certificate-based signature by entertaining the expensive operations of bilinear pairing that can be suffered from greater computational operations. In 2013, Li et al. [15] proved that the scheme used in [13] is not secure from malicious certifier, and they further proposed a low processing time-oriented certificate-based signature. Lu and Li [16] presented a certificate-based signature by entertaining the expensive operations of bilinear pairing. Zhang et al. [17] presented a certificate-based signature by not entertaining the expensive operations of bilinear pairing. Li et al. [18] contributed a key-insulated certificate-based signature; however, Lu et al. [19] proved that the scheme of [18] is not secure from malicious certifier. Also, the proposed certificate-based signature is with improved nature. Lu and Li [20] presented a certificate-based signature by entertaining the expensive operations of bilinear pairing.

3. Network Model

The proposed scheme's network model comprised of four entities, as shown in Figure 2: certificate authority (CA), edge node, cloud server, IIoT devices, and data users. The following is the role of each entity:

(i) Certificate authority (CA): this entity can function as a trusted third party, creating system parameters for the whole network as well as certificates for IIoT devices and data users.

(ii) Cloud server (CS): this entity may be used to store data generated by IIoT devices and data users in a big resource-oriented database.

(iii) IIoT devices: these devices are responsible to generate data from different machines and send it to the edge node using BLE.

(iv) Edge node: this node will be responsible for producing certificate-based signatures on IIoT data after it obtains a certificate from a CA and generates his public and private key.

(v) Data users: data users are responsible for validating the received certificate-based signature from IIoT devices after receiving a certificate from a CA and creating his public and private key.

4. Proposed Certificate-Based Signature Scheme

Here, we first provide the symbols used in the proposed scheme, as given in Table 1; then, the proposed scheme is defined in detail in the phases that follow [21]:

Setup: suppose $\mathcal{O}$ is the given HECC security parameter with size of 80 bits. Then, CA performs the following steps for generating master secrete key ($\mathcal{Q}$), public key (δ), and global parameter set (σ).

(i) CA select $\mathcal{Q}$ randomly, where $1 \le \mathcal{Q} \le n$

(ii) It computes $\delta = \mathcal{Q}.\mathcal{D}$ and selects h^o and h^p as hash functions

(iii) Make $\sigma = \{n, \mathcal{O}, h^o, h^p, \delta, \mathcal{D}\}$ and get available in a network publicly

Key generation: given σ, an actor with identity (ID^a) select $\mathcal{U}^a$ randomly, where $1 \le \mathcal{U}^a \le n$ and compute $\mathcal{V}^a = \mathcal{U}^a.\mathcal{D}$. Then, an actor with identity (ID^a) set $\mathcal{U}^a$ as his private key and $\mathcal{V}^a$ as his public key.

Certificate generation: an actor with identity (ID^a) send ($\mathcal{V}^a, \mathrm{ID}^a$) to CA. Then, select $\mathcal{W}^a$ randomly, where $1 \le \mathcal{W}^a \le n$, compute $\mathcal{X}^a = \mathcal{W}^a.\mathcal{D}$, and compute $\mathcal{C}^a = \mathcal{W}^a + \mathcal{Q}.\ h^o\ (\mathrm{ID}^a, \mathcal{V}^a)$. Finally, CA dispatched $\mathcal{C}\mathrm{ert}^a = (\mathcal{C}^a, \mathcal{X}^a)$ to an actor with ID^a.

Signature generation: a sender can generate signature $(\mathcal{Z}, \mathcal{S})$ utilizing the following steps

(i) It selects $\mathcal{G}$ randomly, where $1 \le \mathcal{G} \le n$ and computes $\mathcal{N} = \mathcal{X}^s + \mathcal{G}.\mathcal{D}$

(ii) Compute $\mathcal{Z} = h^p\,(\mathcal{V}^s, \mathrm{ID}^s, \delta)$ and $\mathcal{S} = \mathcal{G} + \mathcal{U}^s.\mathcal{Z} + \mathcal{C}^s$

(iii) Send $(\mathcal{Z}, \mathcal{S})$ to receiver

Signature verifications: a receiver can verify the signature $(\mathcal{Z}, \mathcal{S})$ utilizing $\mathcal{S}.\mathcal{D} = \mathcal{N} + \delta.h^o\,(\mathrm{ID}^s, \mathcal{V}^s) + h^p\,(\mathcal{V}^s, \mathrm{ID}^s, \delta).\mathcal{V}^s$.

(i) Correctness

A receiver can verify the signature $(\mathcal{Z}, \mathcal{S})$ utilizing the following computations:

$\mathcal{S}.\mathcal{D} = \mathcal{G} + \mathcal{U}^s.\mathcal{Z} + \mathcal{C}^s.\mathcal{D} = \mathcal{G} + \mathcal{W}^s + \mathcal{Q}.h^o\,(\mathrm{ID}^s, \mathcal{V}^s) + \mathcal{U}^s.h^p \quad (\mathcal{V}^s, \mathrm{ID}^s, \delta).\mathcal{D} = \mathcal{G}.\mathcal{D} + \mathcal{W}^s.\mathcal{D} + \mathcal{Q}.\mathcal{D}.h^o\,(\mathrm{ID}^s, \mathcal{V}^s) + \mathcal{U}^s.\mathcal{D}.h^p\,(\mathcal{V}^s, \mathrm{ID}^s, \delta) \quad (\mathcal{G}.\mathcal{D} + \mathcal{X}^s +$

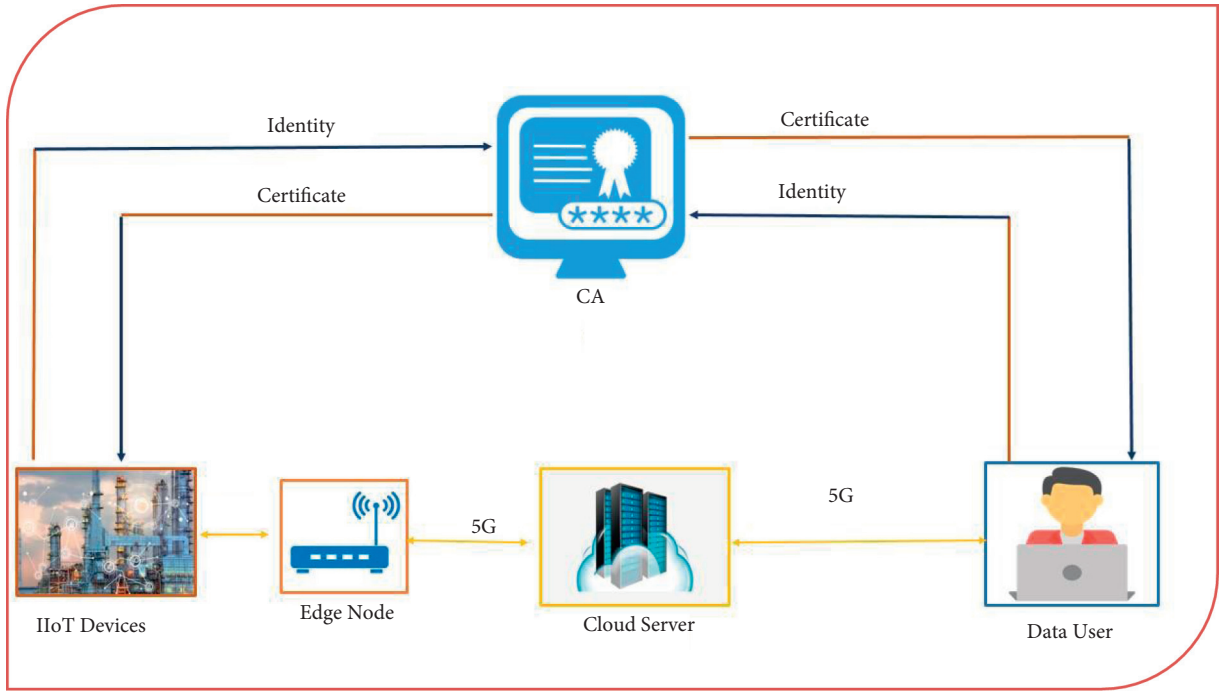

Figure 2: Network model of the proposed scheme.

Table 1: Symbols used in the proposed scheme.

No.	Symbol	Descriptions
1	$\mathcal{Q}$	Master secret key of CA which is picked from hyperelliptic curve finite field
2	δ	Master public key of CA which is the combination of $\mathcal{Q}$ and $\mathcal{D}$
3	$\mathcal{D}$	Devisor of hyperelliptic curve
4	h^o and h^p	These are two hash functions of a same nature and with same properties
5	$\mathcal{O}$	It is the selected security parameter from hyperelliptic curve
6	n	It is a finite number with range of 80 bits
7	$\mathcal{C}\text{ert}^s = (\mathcal{C}^s, \mathcal{X}^s)$	It show certificate of sender
8	$\mathcal{C}\text{ert}^r = (\mathcal{C}^r, \mathcal{X}^r)$	It show certificate of receiver
9	$\mathcal{V}^s$	It show the public key of sender
10	$\mathcal{V}^r$	It show the public key of receiver
11	$\mathcal{U}^s$	It show the private key of sender
12	$\mathcal{U}^r$	It show the private key of receiver
13	ID^s	It show the identity of sender
14	ID^r	It show the identity of receiver
15	$\mathfrak{f}^1$	A symbol used to represent type 1 adversary
16	$\mathfrak{f}^2$	A symbol used to represent type 2 adversary
17	$\mathcal{C}$	The symbol of a facilitator for type 1 and type 2 adversaries

$\delta.h^o(\text{ID}^s, \mathcal{V}^s) + \mathcal{V}^s h^p(\mathcal{V}^s, \text{ID}^s, \delta)) = \mathcal{N} + \delta.h^o \quad (\text{ID}^s, \mathcal{V}^s) + h^p(\mathcal{V}^s, \text{ID}^s, \delta).\mathcal{V}^s$.

5. Security Analysis

Here, the security analysis is totally based on the hardiness of the hyperelliptic curve discrete logarithm problem (HECDLP) that can be defined as follows: suppose $A = B.\mathcal{D}$, where $1 \le B \le n$, so finding B is said to be HECDLP. This section comprises the following two games that are playing for defending of our scheme signature against two types of adversaries, e.g., type 1 ($\mathfrak{f}^1$) and type 2 ($\mathfrak{f}^2$). Here, $\mathcal{C}$ acts as a facilitator for these adversaries. So, $\mathfrak{f}^1$ is the outsider attacker whose capability is to replace the user public key for generating the forge signature; furthermore, it is not capable to access the private key of CA. Moreover, $\mathfrak{f}^2$ is the insider attacker whose capability is to access CA private key, and it is not capable to replace user public key.

Game 1: in this game, by performing maximum number of queries (Q), using ROM, $\mathfrak{f}^1$ can forge our scheme signature with the help of $\mathcal{C}$, when it is to solve HECDLP utilizing the following advantages:

$$\text{Success}^{\mathfrak{f}^1} \geq \frac{1}{Q}\left(1-\frac{1}{Q}\right)^{Q}\xi, \tag{1}$$

where ξ represents the $\mathfrak{f}^1$ success advantages key generation, h^o (.), h^p (.), private key generation, certificate generation, and signature generation, respectively. The results of these queries include in the lists $\mathscr{L}^{\text{KG}}$ $\mathscr{L}^{h^0}$, $\mathscr{L}^{h^p}$ $\mathscr{L}^{\text{PKG}}$, $\mathscr{L}^{cg}$, and $\mathscr{L}^{\text{sig}}$. Also, $\mathscr{C}$ perform the following steps for generating master secrete key ($\mathscr{Q}$), public key (δ), and global parameter set (σ).

Proof. The instance $\Upsilon = \beta$ of HECDLP is given to $\mathfrak{f}^1$; then, $\mathfrak{f}^1$ make the queries such as

(i) It selects $\mathscr{Q}$ randomly, where $1 \leq \mathscr{Q} \leq n$ and gives it to $\mathfrak{f}^1$

(ii) It computes $\delta = \mathscr{Q}.\mathscr{D}$ and selects h^o and h^p as hash functions

(iii) Make $\sigma = \{n, \mathscr{O}, h^o, h^p, \delta, \mathscr{D}\}$ and get available in a network publicly

(iv) It also picks the index $\mathscr{J}$, where $1 \leq \mathscr{J} \leq h^p$ (.)

So, we discuss the queries in the following steps with their results.

Key generation query (.): $\mathfrak{f}^1$ sends ID^g $(1 \leq g \leq \text{KG})$ to key generation oracle (.), where KG represents the maximum number query. $\mathscr{C}$ includes the outputs in $\mathscr{L}^{\text{KG}}$. To reply, $\mathscr{C}$ look for $(\text{ID}^g, \mathscr{V}^g, \mathscr{U}^g)$ in $\mathscr{L}^{\text{KG}}$; if it exists, then $\mathscr{C}$ send $\mathscr{V}^g$ to $\mathfrak{f}^1$; otherwise, it performs the following steps.

(i) If $\mathscr{J} \neq g$, then it selects $\mathscr{U}^g$ randomly, where $1 \leq \mathscr{U}^g \leq n$ and compute $\mathscr{V}^g = \mathscr{U}^g.\mathscr{D}$

(ii) If $\mathscr{J} = g$, it sets $\mathscr{V}^g = \beta.\mathscr{D}$.

h^o (.): $\mathfrak{f}^1$ sends this query; to reply, $\mathscr{C}$ look for $(\text{ID}^g, \mathscr{V}^g, f)$ in $\mathscr{L}^{h^0}$; if it exists, then $\mathscr{C}$ send f to $\mathfrak{f}^1$. Otherwise, $\mathscr{C}$ select f randomly, send f to $\mathfrak{f}^1$, and store $(\text{ID}^g, \mathscr{V}^g, f)$ in $\mathscr{L}^{h^0}$.

h^p (.): $\mathfrak{f}^1$ sends this query; to reply, $\mathscr{C}$ look for $(\text{ID}^g, \mathscr{V}^g, \delta, h)$ in $\mathscr{L}^{h^p}$; if it exists, then $\mathscr{C}$ send h to $\mathfrak{f}^1$. Otherwise, $\mathscr{C}$ select h randomly, send h to $\mathfrak{f}^1$, and store $(\text{ID}^g, \mathscr{V}^g, \delta, h)$ in $\mathscr{L}^{h^0}$.

Private key generation query (.): $\mathfrak{f}^1$ send ID^g; to reply, $\mathscr{C}$ perform the following steps:

(i) If $\mathscr{J} \neq g$, $\mathscr{C}$ look for $(\text{ID}^g, \mathscr{V}^g, \mathscr{U}^g)$ in $\mathscr{L}^{\text{PKG}}$; if it exists, then $\mathscr{C}$ send $\mathscr{U}^g$ to $\mathfrak{f}^1$

(ii) If $\mathscr{J} = g$, then it selects $\mathscr{U}^g$ randomly, send $\mathscr{U}^g$ to $\mathfrak{f}^1$, and includes $(\text{ID}^g, \mathscr{V}^g, \mathscr{U}^g)$ in $\mathscr{L}^{\text{PKG}}$

Signature generation query (.): $\mathfrak{f}^1$ sends ID^g; in reply, $\mathscr{C}$ runs key generation query (.), private key generation query (.), h^o (.), and h^p (.) oracles. $\mathscr{C}$ perform the following steps.

(i) If $\mathscr{J} \neq g$, $\mathscr{C}$ runs certificate generation oracle (.) and run signature generation oracle (.); then, $\mathscr{C}$ send the resultant value to $\mathfrak{f}^1$

(ii) If $\mathscr{J} = g$, then it selects $\phi^{\mathscr{J}}, f^{\mathscr{J}}, \varrho^{\mathscr{J}}$, and $\mathscr{C}^{\mathscr{J}}$ randomly, and set $\mathscr{N}^{\mathscr{J}} = \mathscr{X}^{\mathscr{J}} + \Upsilon$, $f^{\mathscr{J}} = h^o(\text{ID}^{\mathscr{J}}, \mathscr{V}^{\mathscr{J}})$, and $\varrho^{\mathscr{J}} = h^p(\mathscr{V}^{\mathscr{J}}, \text{ID}^{\mathscr{J}}, \delta)$

Forgery: when we take Forking lemma [21] in account, $\mathscr{C}$ can output two signature that are $(\mathscr{X}^*, \mathscr{S}^*)$ and $(\mathscr{X}^{**}, \mathscr{S}^{**})$, and we have the following computations:

$$\begin{aligned}
\mathscr{S}^*.\mathscr{D} &= \mathscr{X}^{\mathscr{J}} + Y + \delta.f^{\mathscr{J}} + \varrho^{\mathscr{J}}.\mathscr{V}^{\mathscr{J}},\\
\mathscr{S}^{**}.\mathscr{D} &= \mathscr{X}^{\mathscr{J}} + Y + \delta.f^{\mathscr{J}} + \varrho^{\mathscr{J}}.\mathscr{V}^{\mathscr{J}}\\
\mathscr{S}^*.\mathscr{D} - \mathscr{S}^{**}.\mathscr{D} &= \mathscr{X}^{\mathscr{J}} + Y^* + \delta.f^{\mathscr{J}} + \varrho^{\mathscr{J}}.\mathscr{V}^{\mathscr{J}}\\
&\quad - \mathscr{X}^{\mathscr{J}} - Y^{**}\\
-\delta.f^{\mathscr{J}} - \varrho^{\mathscr{J}}.\mathscr{V}^{\mathscr{J}} &= \mathscr{S}^*.\mathscr{D} - \mathscr{S}^{**}.\mathscr{D} = Y^* - Y^{**}\\
&= \mathscr{S}^*.\mathscr{D} - \mathscr{S}^{**}.\mathscr{D}\\
&= \beta.\mathscr{D}^* - \beta.\mathscr{D}^{**} = (\mathscr{S}^* - \mathscr{S}^{**}).\mathscr{D}\\
&= \beta.(\mathscr{D}^* - \mathscr{D}^{**}) = \beta = \frac{(\mathscr{S}^* - \mathscr{S}^{**}).\mathscr{D}}{(\mathscr{D}^* - \mathscr{D}^{**})}.
\end{aligned} \tag{2}$$

Probability analysis: here, we define the following events:

(i) $\mathscr{E}^1$: during execution of this game, $\mathscr{C}$ is not abandon

(ii) $\mathscr{E}^2$: $\mathfrak{f}^1$ is succeeded

(iii) $\mathscr{E}^3$: target identity is supposed to forge the proposed scheme signature

So, $(\mathscr{E}^1) \geq (1 - (1/Q))^Q$, $(\mathscr{E}^1, \mathscr{E}^2) = \xi$, and $(\mathscr{E}^1, \mathscr{E}^3, \mathscr{E}^2) = 1/Q$. Therefore,

$$\text{Success}^{\mathfrak{f}^1} \geq \frac{1}{Q}\left(1-\frac{1}{Q}\right)^{Q}\xi, \tag{3}$$

where ξ represents the $\mathfrak{f}^1$ success advantages.

Game 2: in this game, by performing maximum number of queries (Q), using ROM, $\mathfrak{f}^2$ can forge our scheme signature with the help of $\mathscr{C}$, when it solves HECDLP utilizing the following advantages:

$$\text{Success}^{\mathfrak{f}^1} \geq \frac{1}{Q}\left(1-\frac{1}{Q}\right)^{Q}\xi, \tag{4}$$

where ξ represents the $\mathfrak{f}^2$ success advantages. □

Proof:. The instance $\Upsilon = \beta.\mathscr{D}$ of HECDLP is given to $\mathfrak{f}^2$; then, $\mathfrak{f}^2$ make the queries such as key generation, h^o (.), h^p (.), private key generation, and signature generation, respectively. Also, $\mathscr{C}$ perform the following steps for generating master secrete key ($\mathscr{Q}$), public key (δ), and global parameter set (σ). Then, $\mathscr{C}$ give all these parameters to $\mathfrak{f}^2$.

The proof is same like a game 1. □

Table 2: Major operations of proposed and existing schemes.

Schemes	Signature	Verification	Total
Lu and Li [16]	6EPL	2EPL + 3P	8EPL + 3P
Li et al. [18]	4EPL	4P	4EPL + 4P
Lu et al. [19]	5EPL	1EPL + 4P	6EPL + 4P
Lu and Li [20]	9EPL	1EPL + 4P	10EPL + 4P
Proposed scheme	2 HM	3 HM	5 HM

Table 3: Computational cost comparisons of the proposed scheme and existing method on the bases of mile seconds.

Schemes	Signature	Verification	Total
Lu and Li [16]	$6 * 1.25 = 7.5$	$2 * 1.25 + 3 * 14.90 = 47.2$	$8 * 1.25 + 3 * 14.90 = 54.7$
Li et al. [18]	$4 * 1.25 = 5$	$4 * 14.90 = 59.6$	$4 * 1.25 + 4 * 14.90 = 64.4$
Lu et al. [19]	$5 * 1.25 = 6.25$	$1 * 1.25 + 4 * 14.90 = 60.85$	$6 * 1.25 + 4 * 14.90 = 67.1$
Lu and Li [20]	$9 * 1.25 = 11.25$	$1 * 1.25 + 4 * 14.90 = 60.85$	$10 * 1.25 + 4 * 14.90 = 72.1$
Proposed scheme	$2 * 0.48 = 0.96$	$3 * 0.48 = 1.44$	$5 * 0.48 = 2.4$

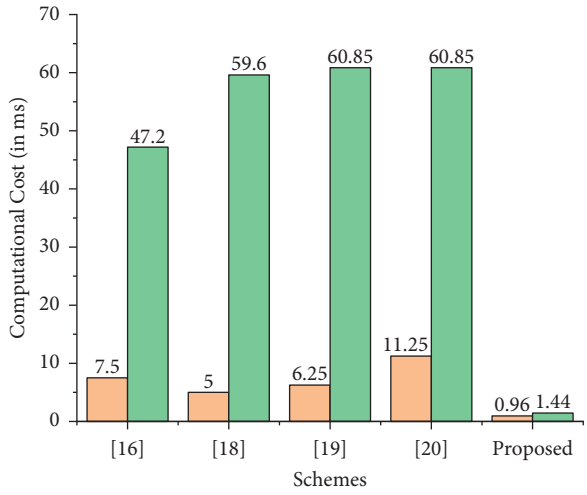

Figure 3: Computational cost comparison.

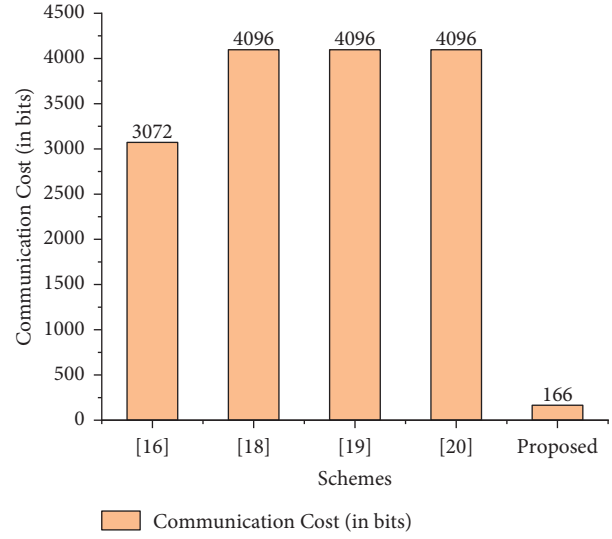

Figure 4: Communication cost comparison.

Table 4: Communication overhead comparisons of the proposed scheme and existing method on the bases of bits.

Schemes	Signature size	Signature size in bits
Lu and Li [16]	$3\|G\|$	$3 * 1024 = 3072$
Li et al. [18]	$4\|G\|$	$4 * 1024 = 4096$
Lu et al. [19]	$4\|G\|$	$4 * 1024 = 4096$
Lu and Li [20]	$4\|G\|$	$4 * 1024 = 4096$
Proposed scheme	$2\|n\|$	$2 * 80 = 160$

6. Performance Analysis

In this section, we provide details about computational and communication costs of the proposed scheme with its counterpart schemes.

6.1. Computational Cost. Here, we first provide major operations such as exponential (EPL), bilinear pairing (P), and hyperelliptic curve divisor multiplications (HM) in proposed certificate-based signature scheme and the other approaches such as by Lu and Li [16], Li et al. [18], Lu et al. [19], and Lu and Li [20], respectively, as given in Table 2. Then, we consider the time taken by each major operations from [1], in which EPL consumes 1.25 ms, P takes 14.90 ms, and HM utilizes 0.48 ms, respectively [22, 23]. So, on the bases of above-discussed consuming time of major operations, we make the comparisons of proposed certificate-based signature scheme and the other approaches such as by Lu and Li [16], Li et al. [18], Lu et al. [19], and Lu and Li [20], as given in Table 3. Thus, the clearer improvement in computational cost can be seen from Table 3 and Figure 3, and it means our scheme consumes less time during computational processing.

6.2. Communication Cost. Here, we provide the parameter considered for communication overhead bilinear pairing group (G) and hyperelliptic curve (n) in proposed certificate-

based signature scheme and the other approaches such as by Lu and Li [16], Li et al. [18], Lu et al. [19], and Lu and Li [20], respectively, as given in Table 3. Then, we consider the bits consumed by each parameter, in which G consumes 1024 bits and n take 80 bits. So, on the bases of above-discussed consuming bits by each parameter, we make the comparisons of proposed certificate-based signature scheme and the other approaches such as by Lu and Li [16], Li et al. [18], Lu et al. [19], and Lu and Li [20], as given in Table 4. Thus, the clearer improvement in computational communication overhead can be seen from Table 4 and Figure 4, which authenticates that our scheme ingests less bits during communications.

7. Conclusion

The Industrial Internet of Things (IIoT) has recently gained popularity for industrial applications. IIoT systems are vulnerable to a variety of cyber-attacks due to the wireless and widespread connectivity of IoT sensors and devices. Certificate-based signature methods are a better solution than other cryptographic schemes for solving the IIoT's security demands in terms of offering resilience to such attacks. As a result, certificate-based IIoT signature mechanisms are proposed in this study. We employed HECC, which is similar to RSA, bilinear pairing, and ECC, but has a smaller key size. After performing a comparison study, we found that our scheme outperforms its equivalent schemes in terms of computation and communication costs. In addition, the proposed scheme improves security against both known and unknown attacks.

Data Availability

The data generated or analyzed during this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work (RGP 2/209/42). The authors deeply acknowledge Taif University, Taif, Saudi Arabia, for supporting this research through Taif University Researchers Supporting Project Number (TURSP-2020/328).

References

[1] P. Lade, R. Ghosh, and S. Srinivasan, "Manufacturing analytics and industrial Internet of Things," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 74–79, 2017.

[2] T. Kumar, E. Harjula, M. Ejaz, and A. Manzo, "BlockEdge: blockchain-edge framework for industrial IoT networks," *IEEE Access*, vol. 8, pp. 154166–154185, 2020.

[3] T. K. Ahmad, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communication and Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[4] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, "A novel IoT architecture based on 5G-IoT and next generation technologies," in *Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 81–88, Vancouver, BC, 2018.

[5] H. Wang, W. Jia, A. Liu, and M. Xie, "MTES: an intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2020.

[6] M. Kumar, H. Kumar Verma, and G. Sikka, "A secure data transmission protocol for cloud-assisted edge-Internet of Things environment," *Transactions on Emerging Telecommunications Technologies*, 2020.

[7] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and F. Noor, "An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing," *Electronics*, vol. 9, no. 1, p. 30, 2019.

[8] M. A. Khan, I. Ullah, and N. Kumar, "An efficient and secure certificate-based access control and key agreement scheme for flying ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 70, 2021.

[9] B. G. Kang, J. H. Park, and S. G. Hahn, "A certificate-based signature scheme," in *in Topics in Cryptology-CT-RSA 2004*, T. Okamoto, Ed., vol. 2964, Springer, Heidelberg, Germany, 2004, Lecture Notes in Computer Science.

[10] J. Li, X. Huang, Y. Mu, W. Susilo, and Q. Wu, "Certificate-based signature: security model and efficient construction in public key Infrastructure," *Lecture Notes in Computer Science*, Vol. 4582, Springer, , Heidelberg, Germany, 2007.

[11] J. K. Liu, J. Baek, W. Susilo, and J. Zhou, "Certificate-based signature schemes without pairings or random oracles," in *in Information Security. ISC 2008*, T. C. Wu, C. L. Lei, V. Rijmen, and D. T. Lee, Eds., vol. 5222, Springer, Heidelberg, Germany, 2008, Lecture Notes in Computer Science.

[12] J. Zhang, "On the security of a certificate-based signature scheme and its improvement with pairings," in *Proceedings of the International Conference of Information Security Practice and Experience*, pp. 47–58, 2009.

[13] Y. Ming and Y. Wang, "Efficient certificate-based signature scheme," *IAS*, vol. 2, pp. 87–90, 2009.

[14] J. Li, X. Huang, Y. Mu, W. Susilo, and Q. Wu, "Constructions of certificate-based signature secure against key replacement attacks," *Journal of Computer Security*, vol. 18, no. 3, pp. 421–449, 2010.

[15] J. Li, Z. Wang, and Y. Zhang, "Provably secure certificate-based signature scheme without pairings," *Information Science*, vol. 233, pp. 313–320, 2013.

[16] Y. Lu and J. Li, "Improved certificate-based signature scheme without random oracles," *IET Information Security*, vol. 10, no. 2, pp. 80–86, 2016.

[17] Y. Zhang, J. Li, Z. Wang, and W. Yao, "A new efficient certificate-based signature scheme," *Chinese Journal of Electronics*, vol. 24, no. 4, pp. 776–782, 2015.

[18] J. Li, H. Du, and Y. Zhang, "Certificate-based key-insulated signature in the standard model," *Computer Journal*, vol. 59, no. 7, pp. 1028–1039, 2016.

[19] Y. Lu, J. Li, and J. Shen, "Weakness and improvement of a certificatebased key-insulated signature in the standard model," *Computer Journal*, vol. 60, no. 12, pp. 1729–1744, 2017.

[20] Y. Lu and J. Li, "A forward-secure certificate-based signature scheme with enhanced security in the standard model," *KSII*

Transactions on Internet and Information System, vol. 13, no. 3, pp. 1502–1522, 2019.

[21] G. K. Verma, N. Kumar, P. Gope, B. B. Singh, and H. Singh, "SCBS: a short certificate-based signature scheme with efficient aggregation for industrial-internet-of-things environment," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9305–9316, 2021.

[22] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for Internet of Things (IoT) in mobile health (M-Health) system," *Journal of Medical Systems*, vol. 45, p. 4, 2021.

[23] M. A. Khan et al., "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3416–3425, 2022.