IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 September 2022, accepted 20 September 2022, date of publication 3 October 2022, date of current version 10 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3211257

RESEARCH ARTICLE

Certificate-Based Signcryption Scheme for Securing Wireless Communication in Industrial Internet of Things

INSAF ULLAH[1], ABDULLAH ALOMARI[2], (Member, IEEE), AKO MUHAMMAD ABDULLAH[3], NEERAJ KUMAR[4,5,6,7], (Senior Member, IEEE), AMJAD ALSIRHANI[8], FAZAL NOOR[9], SADDAM HUSSAIN[10], AND MUHAMMAD ASGHAR KHAN[1]

[1]Hamdard Institute of Engineering and Technology, Islamabad 44000, Pakistan
[2]Department of Computer Science, Al-Baha University, Al Bahah 65799, Saudi Arabia
[3]Computer Science Department, College of Basic Education, University of Sulaimani, Sulaymaniyah 46001, Iraq
[4]Thapar Institute of Engineering and Technology, Patiala 147004, India
[5]King Abdul Aziz University, Jeddah 22233, Saudi Arabia
[6]School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand 248001, India
[7]Department of Electrical and Computer Engineering, Lebanese American University, Beirut 1100, Lebanon
[8]College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia
[9]Faculty of Computer and Information Systems, Islamic University of Madinah, Medina 400411, Saudi Arabia
[10]School of Digital Science, Universiti Brunei Darussalam, Gadong BE1410, Brunei Darussalam

Corresponding author: Neeraj Kumar (nehra04@gmail.com; neeraj.kumar@thapar.edu)

ABSTRACT The Industrial Internet of Things (IIoT) community is concerned about the security of wireless communications between interconnected industries and autonomous systems. Providing a cyber-security framework for the IIoT offers a thorough comprehension of the whole spectrum of securing interconnected industries, from the edge to the cloud. Several signcryption schemes based on either identity-based or certificateless configurations are available in the literature to address the IIoT's security concerns. Due to the identity-based/certificateless nature of the available signcryption schemes, however, issues such as key escrow and partial private key distribution occur. To address these difficulties, we propose a Certificate-Based Signcryption (CBS) solution for IIoT in this article. Hyperelliptic Curve Cryptosystem (HECC), a light-weight version of Elliptic Curve Cryptosystem (ECC), was employed to construct the proposed scheme, which offers security and cost-efficiency. The HECC utilizes 80-bit keys with fewer parameters than the ECC and Bilinear Pairing (BP). The comparison of performance in terms of computation and communication costs reveals that the proposed scheme provides robust security with minimal communication and communication costs. Moreover, we used Automated Validation of Internet Security Protocols and Applications (AVISPA) to assess the security toughness, and the results show that the proposed scheme is secure.

INDEX TERMS Certificate-based signcryption, industrial internet of things, wireless communication, HECC, AVISPA.

I. INTRODUCTION

Industrial Internet of Things (IIoT) refers to sensors, instruments, and other devices that are networked with industrial computer applications, such as production and energy management [1]. This connectivity enables the gathering, sharing, and analysis of data, which may facilitate productivity and efficiency gains as well as other economic benefits. This, in turn, will help manufacturers develop products more efficiently and sustainably. In addition, the resulting IoT-node-embedded devices will also be included into the IIoT; this will allow for more efficient resource use, hence boosting consumer satisfaction and product quality. In addition, with the integration of Cyber-Physical Systems (CPS) and modern networking technologies, the monitoring and control capabilities of industrial systems have considerably

The associate editor coordinating the review of this manuscript and approving it for publication was Ali Kashif Bashir.

improved [2], [3]. Industry 4.0 is a revolution in which wireless networking and CPS are coupled with sensors on products to monitor the whole product flow in order to make intelligent decisions [4], [5]. As the IIoT grows, new security risks emerge. Each new device or component that connects to the IIoT represents a potential vulnerability. It can be challenging to maintain security in the face of growing connectivity. Insecure IIoT systems can have serious adverse impact, including operational interruption and financial loss. Exposed ports, insufficient authentication procedures, and old software all contribute to the emergence of threats. The aforementioned unsatisfactory situation will result in the demise of industrial output. Therefore, a strong security mechanism is essential to ensure the security of data transfer between users and sensing equipment.

Signature and encryption are fundamental cryptographic procedures for secure communication [6]. Encryption provides confidentiality, whereas signature provides authenticity independently. If both signature and encryption are required simultaneously, signcryption [7] is used. The majority of signcryption schemes rely on cryptography certificates with public keys [8]. Therefore, a new collaboration in the form of an ID-based cryptosystem, in which the user's encryption key is the correct string for the user's identity [9]. However, as the Private Key Generator (PKGR) possesses all the information pertaining to the private keys of the individual members, this could result in an overwhelming Key Escrow (KE) problem [10], [11]. In 2003, Al-Riyami and Patterson [12] introduced the concept of a certificateless cryptosystem consisting of two components: the secret value and partial private key, in line with the KE. The Key Generation Center (KGC) offers a partial private key (PPK), while the participants determine the secret value. Similarly, certificateless cryptosystems are susceptible to the PPKDP problem inherent to certificateless cryptography, as the key distribution requires a secure connection between the KGCR and the recognised parties. In the same year, Gentry [13] introduced the concept of a certificate-based cryptosystem (CBC) in which a user can create his or her own private/public key pair while the Certifier Authority (CA) checks for a certain public key. Since the CA does not know the private keys of the participating users, the CBC avoids the KE. In addition, a secure connection between the user and the CA is not required.

Typically, computationally hard problems, such as Bilinear Pairing (BP), Revest-Shamir-Edelman (RSA), Diffie-Hellman (DFHMN), and ECC [14], [15], [16], [17], [18], [19], [20], are used to evaluate the performance of security schemes. The RSA cryptosystem operates with 1024-bit keys. Similarly, the BP is 14.31% worse than the RSA [21] because to its extensive map-to-point computation and operation features. Similarly, an ECC was devised to alleviate the drawbacks of RSA and BPRNG's high key sizes [22]. Compared to the supplied cryptosystems, the security efficiency and security hardness of the ECC depend on 160-bit short keys [23]. Even with 160-bit keys, the ECC is unsuitable for IIoT data collected from the public. Consequently, the HCC, a new type of cryptosystem that is essentially a generalization of the ECC, is presented. The HCC provides correspondent-level security for the BP, RSA, DFHMN, and HCC with keys that are accordingly 80 bits shorter [24], [25]. In light of the preceding considerations, an ECC is seen a good option for crowdsourcing IIoT data.

The above explanation encourages us to propose a new CBS for IIoT with the objective of removing the KE problem of identity-based cryptography and the PPKDP problem of certificateless cryptography with minimal cost and complexity. The proposed scheme is favorable to the environment since it employs the Hyperelliptic Curve Cryptosystem (HECC), which requires much smaller key sizes than bilinear pairing, RSA, and elliptic curves. Listed below are the characteristics of the proposed scheme.

- We provide a Certificate-Based Signcryption (CBS) solution for IIoT using Hyperelliptic Curve Cryptosystem (HECC), a lightweight variant of Elliptic Curve Cryptosystem. (ECC). Using small key sizes makes the proposed scheme lightweight, which is the most desirable characteristic of HECC.
- The proposed scheme offers confidentiality, unforgeability, integrity, anti-reply, forward secrecy, and non-repudiation as security characteristics.
- We also investigate the performance of the proposed scheme and compare it to relevant existing schemes in order to validate its computational and communication capabilities.
- The proposed scheme is validated using AVISPA, a well-known security verification and simulation tool. The findings demonstrate that the proposed scheme is SAFE in terms of the security claims based on the working idea of two back-end protocol checkers, OF-MC and CL-AtSe.

The rest of the article is organized as follows: in Section 2, related work is covered. The Preliminaries for the construction and complexity analysis are presented in Section 3. Section 4 demonstrates the construction of the proposed scheme. The section 5 security analysis is followed by the section 6 cost analysis. Section 7 concludes the study.

II. RELATED WORK

Information security is vital to the security of a communication systems. The fundamental security features highlight the confidentiality and authenticity of the data. In the literature, we have researched the proposed security schemes for IIoT infrastructure. A certificateless signature scheme for the IIoT infrastructure is proposed [27], however Zhang *et al.* [28] and Yang *et al.* [29] showed the scheme to be vulnerable against both Type 1 and Type 2 adversaries. In addition, the scheme makes use of BP's fragility, which has the worst potential in terms of cost complexity. Therefore, in [29], the authors strengthened the security of scheme [27] using ECC; nonetheless, the scheme is not suited for real IIoT applications due to PPKDP and ECC's larger key sizes. The authors assert in [29] that the public key replacement attack

exists in the method described in [28]. The authors then introduced the key insulated signature method using BP in [30]. Similarly, the presented method relied on ECC, which conducts intensive calculation and requires a larger bandwidth for transmission. Later, Qiao *et al.* [31] proposed a secure CBAS scheme for IIoT in order to enhance the CBAS scheme and offer a real implementation for it. In the random oracle model, based on the complexity of the discrete logarithm problem, the proposed scheme's security is demonstrated. Compared to prior CBAS schemes, the proposed scheme structure provides excellent security and computation and communication efficiency.

The aforementioned schemes provide the security feature of authentication solely. As the IIoT architecture needs confidentiality with authenticity. For this purpose, in 2017, Karate *et al.* [32], introduced a novel identity-based signcryption technique for IIoT crowdsourcing employing bilinear pairing. The presented method has an issue with over-reliance on PKG, which is inborn in identity-based signcryption schemes, because it requires the PKG to create a complete private key. Furthermore, the security of the system is substantially affected once the PKG is attacked. In addition, the given scheme does not meet with the security criteria of confidentiality and forward secrecy. Besides, the suggested technique also suffers from the use of high bandwidth use and significant computation cost due to the utilization of bilinear pairing.

In 2019, Ullah et al. [33], introduced a lightweight CLC scheme for crowdsourced IIoT applications with the aim of increasing security and minimizing communicational and computational expenses. However, the given scheme has an issue of PPKDP inborn with certificateless signcryption, since the key distribution needs a secure connection between KGCR and the respected participants. Unfortunately, the authors didn't offer a formal demonstration of the proposed scheme in any security model such as random oracle or standard model. In 2020, Dharminder et al. [34], introduces an identity-based signcryption system for IIoT crowdsourcing. Performance study with comparable schemes suggests that the offered strategy is efficient in terms of both computing and communicational expenses. However, the suggested strategy suffers from the use of high bandwidth use and hefty computation cost due to the employment of bilinear pairing.

All of the aforementioned approaches are proposed to secure the IIoT's infrastructure. However, the offered solutions suffer from significant computational costs and communication overheads, as well as key escrow and private key distribution issues. In addition, the security hardness of the aforementioned systems is based on ECC and bilinear pairing, which is appropriate for the Industrial Internet of Things. We proposed a new CBS strategy for IIoT crowdsourcing for this reason. The proposed scheme is effective and devoid of KE and PPKDP problems. Using the HECC, the proposed scheme reduces the high computational cost and communication overheads.

III. PRELIMINARIES

This section covers formal definitions, Threat model, and notions used in the proposed scheme in table form (Table.1).

A. HYPERELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM (HECDLP)

Suppose $\phi\ \varepsilon\{1, 2, 3, 4, 5, \ldots .z-1\}$ and $\Upsilon = \phi.D$, if finding ϕ is negligible, then it said to be ***HECDLP.***

Hyperelliptic Curve Computational Diffie-Hellman

Suppose $\phi\ \varepsilon\{1, 2, 3, 4, 5, \ldots .z-1\}$ and $\Upsilon = \phi.$ç.D, if finding ϕ and $\mathcal{R}$ are negligible, then it said to be ***HECDHP.***

B. THREAT MODEL

The Dolev-Yao adversary model, which distinguishes between adversary (AVR) and forger (*FR*), has been taken into account when designing our proposed scheme. To break the forward security, integrity, and confidentiality of the proposed scheme, AVR's job is to launch an attack against it. Meanwhile, *FR's* job is to make the signature of the proposed scheme compromised.

TABLE 1. Notations.

S. No	Symbol	Explanation
1	CA	Certification authority
2	F_γ	A finite field F_γ of order γ
3	Ψ	Public parameter set
4	ϑ	Private key of Certification authority
5	Υ	Public key of Certification authority
7	H_1, H_2, and H_3	Hash functions
8	D	Divisor of HEC
9	ID_{cs}, ID_{cus}	Identity of CB-Signcrypter and CB-Un- Signcrypter
10	P_{cs}, P_{cus}	Private key of the CB-Signcrypter and CB-Un- Signcrypter
11	B_{cs}, B_{cus}	Public key of the CB-Signcrypter and CB-Un- Signcrypter
12	C_{cs}, C_{cus}	Certificate of CB-Signcrypter and CB-Un- Signcrypter
13	$\mathcal{C}$	Ciphertext
	m	Plaintext
14	$\oplus$	Used as in encryption/decryption
15	n_r, n_s	Nonce for CB-Signcrypter and CB-Un- Signcrypter
16	$\mathcal{K}$	Encryption/decryption key for CB-Signcrypter and CB-Un-Signcrypter
17	ϕ	CB-signcrypted tuple
18	$EXPN$	Exponentiations
19	$BIPG$	bilinear pairing operation
20	$HYDM$	Hyper Elliptic Curve Divisor Multiplication operation
21	$\|m\|$	message size in bits
22	$\|G\|$	Parameter size in bilinear pairing
23	$\|n\|$	Parameter size in Hyper Elliptic Curve

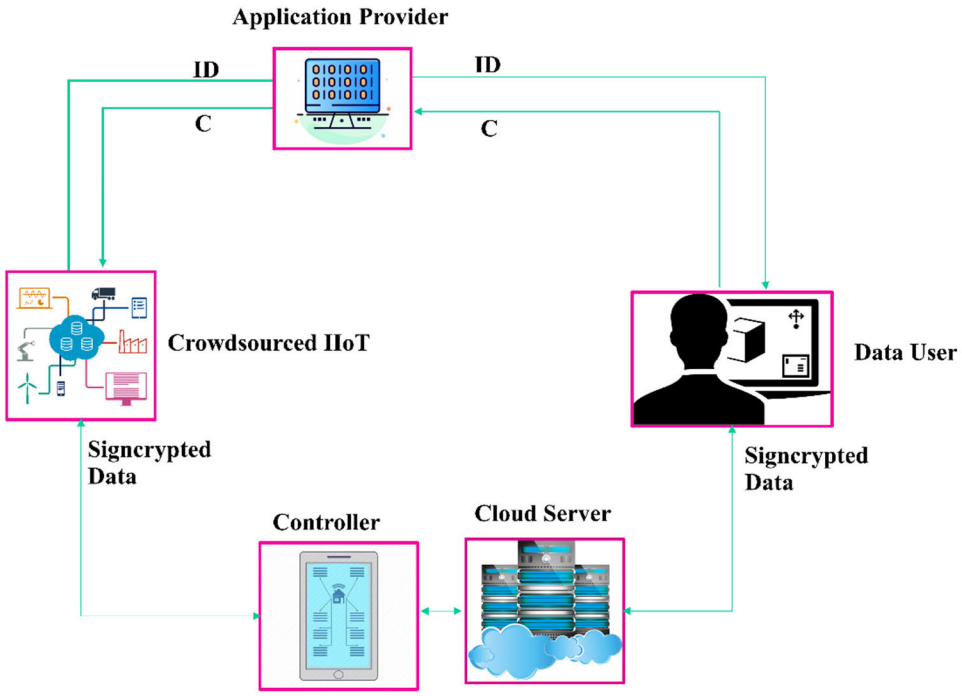

FIGURE 1. Proposed network model.

IV. CONSTRUCTION OF THE PROPOSED SCHEME

This section discusses the construction of the proposed scheme, including the syntax, network model, and proposed algorithm.

A. GENERIC SYNTAX

In this phase, we provide the definitions for the working structure of each part of CBS in the following steps.

Setup: The Certificate Authority (CA), initially pick a security parameter 1^{ε}, further outputs the secret key ϑ and global parameter set Ψ.

Public Number Generation: Given global parameter set Ψ and entity identity ID_e, it outputs the public number and the entity of identity ID_e transmits a pair (ID_e, β_e) to CA.

Certificate Generation: Assumed the entity identity ID_e, Ψ, and a pair (ID_e, β_e), it outputs a certificate C_e, and then sends a pair (C_e, μ) to an entity of identity ID_e in open network.

Key Generation: Assumed Ψ and a pair (C_e, μ), the entity of identity ID_e generates his private key P_e and public key B_e.

CB-Signcryption: Specified a plaintext m, global parameter param, the identities of the CB-Signcrypter and CB-Un- Signcrypter (ID_{cs}, ID_{cus}), the certificate and private key of CB-Signcrypter (C_{cs}, P_{cs}), the CB-Signcrypter and CB-Un- Signcrypter public keys (B_{cs}, B_{cus}), it outputs a CB-signcrypted tuple ϕ.

CB-Un Signcryption: Upon arrival ϕ, CB-Un- Signcrypter considerers the following is an input: identities of the CB-Signcrypter and CB-Un- Signcrypter (ID_{cs}, ID_{cus}), its own certificate and private key, its own public key and sender public key, and the global parameter param, it verifies the signature and outputs a plaintext m.

B. PROPOSED NETWORK MODEL

Fig. 1 depicts the five key entities that comprise the proposed network model: the Application Provider, the Crowdsourced Industrial internet of Things, the Controller, the Data User, and the Cloud Server These entities are capable of cellular network connectivity (3G/4G/5G). The sensors are linked through Bluetooth and Wi-Fi technologies. The following describes in detail the function of each entity.

Application Provider: This entity serves as a Certificate Authority (CA) and is responsible for generating a certificate for a requesting user.

Crowdsourced Industrial internet of Things: Utilizing intelligent devices to capture sensing data from industrial IoT devices, crowdsourced IIoT offers a paradigm for data collecting and sensing. The data from sensors/mobiles and crowd tasks are saved, processed, evaluated, and shown graphically. On the request of the controller, the collected data is then sent to the controller.

Controller: In the proposed network model, the mobile phone is considered a controller. This entity is responsible for calculating the signcryption of collected data from sensor nodes and transferring it to data user.

Data User: This entity plays the role of the end user and delivers a signcrypted access request query to the controller if it requires Crowd-sourced IIoT data.

Cloud Server: Cloud Server is only responsible for storing massive amounts of crowdsourced data if required; otherwise, it transfers the signcrypted text to the data user.

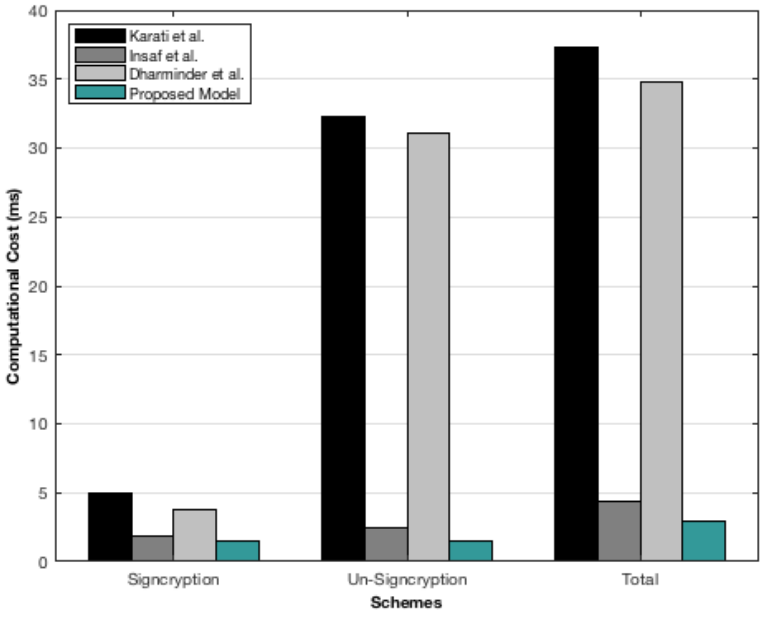

FIGURE 2. Computation cost (in ms).

TABLE 2. Operation and their timing.

Operation	EXPN	BIPG	HYDM
Cost in ms	1.25	14.90	0.48

TABLE 3. Major operations and their respective timing.

Schemes	Signcryption	Un-Signcryption
Karati et al.[32]	4 EXPN	2 EXPN + 2 BIPG
Insaf et.al [33]	4 HYDM	5 HYDM
Dharminder et al.[34]	3 EXPN	1 EXPN + 2 BIPG
Proposed scheme	3 HYDM	3 HYDM

TABLE 4. Computation cost analysis.

Schemes	Signcryption	Un-Signcryption	Total
Karati et al. [32]	**5**	**32.3**	**37.3**
Insaf et al.[33]	**1.92**	**2.4**	**4.32**
Dharminder et al.[34]	**3.75**	**31.05**	**34.8**
Proposed scheme	**1.44**	**1.44**	**2.88**

C. PROPOSED ALGORITHM

The proposed scheme contains the following steps.

Setup: The certificate authority (CA), initially picks a security parameter 1^{ε} and performs the following sub steps:

It chooses a hyper elliptic curve (HEC) over finite field of order F_{γ} with Genus $\delta \geq 2$

Picks a number $\vartheta \in \{1, 2, \ldots \ldots, \gamma-1\}$ as a secret key and computes $\gamma = \vartheta.\mathcal{D}$

Choose three one way hash functions: H_1, H_2, and H_3.

Finally, it outputs global parameter set as $\Psi = (\text{HEC}, F_{\gamma}, 1^{\varepsilon}, \delta, \Upsilon, H_1, H_2, \text{and } H_3)$

Public Number Generation: Given global parameter set Ψ and entity identity ID_e, it picks a number $\Omega_e \in \{1, 2, \ldots \ldots, \gamma - 1\}$ and computes $\beta_e = \Omega_e.\mathcal{D}$. Further, it computes $\omega_e = \Omega_e.\ \gamma$ and $EID_e = \omega_e \oplus (ID_e, \beta_e)$. An entity of identity ID_e sends the pair (EID_e, β_e) to CA.

Certification: CA recovers ID_e as $(ID_e, \beta_e) = \omega_e \oplus EID_e$, where CA computes $\omega_e = \Omega_e.\ \vartheta$. Then by considering as input ID_e, Ψ, and a pair (ID_e, β_e), it outputs a certificate by using the following computational steps:

It picks a number $\eta_e \in \{1, 2, \ldots \ldots, \gamma-1\}$ and computes $X_e = \eta_e.\mathcal{D}$

TABLE 5. Variables with their respective size.

Variables	Size in Bits
Bilinear pairing (G)	1024
Hyperelliptic curve (n)	80
Message (m)	512

TABLE 6. Communication cost analysis using major operation.

Schemes	Signcrypted Text Size
Karati et al. [32]	$\|m\| + 5\|G\|$
Insaf et al.[33]	$\|m\| + 3\|n\|$
Dharminder et al.[34]	$\|m\| + 3\|G\|$
Proposed scheme	$\|m\| + 2\|n\|$

TABLE 7. Communication cost comparison in bits.

Schemes	Signcrypted Text Size in bits
Karati et al. [32]	5632
Insaf et al.[33]	752
Dharminder et al.[34]	3584
Proposed scheme	672

Calculates a certificate $C_e = X_e + \beta_e$ and a value $\mu = \eta_e.H_1(C_e, ID_e) + \vartheta$

Then sends the pair (C_e, μ) to an entity of identity ID_e on an open network.

Key Generation: Upon arrival (C_e, μ), given Ψ, the entity of identity ID_e generates his private key P_e and public key B_e utilizing the below computations.

Computes $P_e = \Omega_e.H_1(C_e, ID_e) + \mu$ *and* $B_e = P_e.\mathcal{D}$

The private keyP_e and public key B_e will be acceptable in a condition if $B_e = C_e.H_1(C_e, ID_e) + \Upsilon$ is hold

CB-Signcryption*:* Specified a plaintext m, Ψ, the identities of the CB-Signcrypter and CB-Un-Signcrypter (ID_{cs}, ID_{cus}), the certificate and private key of CB-Signcrypter (C_{cs}, P_{cs}), the CB-Signcrypter and CB-Un- Signcrypter public keys (B_{cs}, B_{cus}), it outputs a CB-signcrypted tuple $\phi = (\mathcal{Q}, \mathcal{Z}, \mathcal{W})$ in the following computational steps:

It picks a number $\mathcal{V} \in \{1, 2, \ldots \ldots, \gamma - 1\}$ and computess $\mathcal{Y} = \mathcal{V}.\mathcal{D}$, a secret key $\mathcal{K} = \mathcal{V}.B_{cus}$ and $Z = (m, n_s) \oplus H_2(\mathcal{K})$, a hash value $\mathcal{Q} = H_3(C_{cs}, m, \mathcal{Y}, ID_{cs}, B_{cs})$, signature $\mathcal{W} = \mathcal{V} + \mathcal{Q}.P_{cs}$.

Sends a CB-signcrypted tuple $\phi = (\mathcal{Q}, \mathcal{Z}, \mathcal{W})$ to CB-Un-Signcrypter on an open network.

CB-Un Signcryption: Upon arrival ϕ, CB-Un-Signcrypter considerers the following parameters are set as an input:

Identities of the CB-Signcrypter and CB-Un- Signcrypter (ID_{cs}, ID_{cus}),

Its own certificate and private key (C_{cus}, P_{cus}), and its own public key and sender public key (B_{cus}, B_{cs})

The global parameter set Ψ, it verifies the signature and outputs a plaintext m as followed.

Computes $\mathcal{Y}^{/} = \mathcal{W}.\mathcal{D} - \Psi.\ B_{cs}$ and then computes the decryption key as $\mathcal{K}^{/} = \mathcal{Y}^{/}.P_{cus}$

Recover m as $(m, m_s) = \mathcal{Z} \oplus H_2\left(\mathcal{K}^{/}\right)$.

D. CORRECTNESS

In the following computations, the entity of identity can confirm the originality of private key P_e and public key B_e:

$$
\begin{aligned}
B_e &= C_e.H_1(C_e, ID_e) + \Upsilon \\
B_e &= P_e..\mathcal{D} = (\Omega_e.H_1(C_e, ID_e) + \mu).\mathcal{D} \\
&= (\Omega_e.H_1(C_e, ID_e) + \eta_e.H_1(C_e, ID_e) + \vartheta).\mathcal{D} \\
&= (\Omega_e.\mathcal{D}.H_1(C_e, ID_e) + \eta_e.\mathcal{D}.H_1(C_e, ID_e) + \vartheta.\mathcal{D}) \\
&= (\beta_e.H_1(C_e, ID_e) + X_e.H_1(C_e, ID_e) + \Upsilon) \\
&= ((\beta_e + X_e)H_1(C_e, ID_e) + \Upsilon) = C_e.H_1(C_e, ID_e) + \Upsilon
\end{aligned}
$$

Also, by using the following computations, CB-Un- Signcrypter can confirm the originality of ϕ.

$$
\begin{aligned}
\mathcal{Y}^{/} &= \mathcal{W}.\mathcal{D} - \mathcal{Q}.B_{cs} = (\mathcal{V} + \mathcal{Q}.P_{cs})\,.\mathcal{D} - \mathcal{Q}.P_{cs}.\mathcal{D} \\
&= (\mathcal{V}.\mathcal{D} + \mathcal{Q}.P_{cs}.\mathcal{D}) - \mathcal{Q}.P_{cs}.\mathcal{D} \\
&= \mathcal{V}.\mathcal{D} + \mathcal{Q}.P_{cs}\mathcal{D} - \mathcal{Q}.P_{cs}.\mathcal{D} = \mathcal{V}.\mathcal{D} = \mathcal{Y}
\end{aligned}
$$

V. SECURITY ANALYSIS

Theorem 1 ***← Confidentiality***

Confidentiality is that security property of this newly contributed scheme, in which the encryption key of legitimate sender cannot be compromised by any adversary $(\mathcal{AV}r)$.

Proof 1: An encryption key of $\mathcal{K} = \mathcal{V}.B_{cus}$ is first made by the sender in the proposed certificate-based signcryption scheme then by using $\mathcal{K}$ to encrypt the plaintext like $\mathcal{Z} = m \oplus H_2(\mathcal{K}).\mathcal{AV}r$, however, will need $\mathcal{K} = \mathcal{V}.B_{cus}$, which in turn wants $\mathcal{V}$ from $\mathcal{Y} = \mathcal{V}.\mathcal{D}$ in order to recover the contents of $\mathcal{Z}$.

This is not feasible for $\mathcal{AV}r$, and it is the same as hyperelliptic curve discrete problems. In addition, the $\mathcal{AV}r$ can recover the decryption key from $\mathcal{K}^{/} = \mathcal{Y}^{/}.P_{cus}$, which further needed P_{cus} from $B_{cus} = P_{cus}.D$. $\mathcal{AV}r$ cannot solve this problem, thus it equals a discrete hyperelliptic curve problem. As a result, the proposed certificate-based generalized signcryption scheme meets the confidentiality requirements.

Theorem 2 ***← Unforgeability***

It is expected that a CBS scheme will achieve unforgeability as long as there is no forger (*FR*) capable of compromising the sender's dedicated private key and forging the digital signature.

Proof 2: By using the public network, the sender must generate a $\mathcal{W} = \mathcal{V} + \mathcal{Q}.P_{cs}$ a signature, send the Ciphertext, and generate the hash value $\phi = (\mathcal{Q}, \mathcal{Z}, \mathcal{W})$ along with the signature.

FR however, must be capable of figuring out $\mathcal{W} = \mathcal{V} + \mathcal{Q}.P_{cs}$, if it attempts to produce a forgery signature, which further want $\mathcal{V}$ from $\mathcal{Y} = \mathcal{V}.\ \mathcal{D}$ and P_{cs} from $B_{cs} = P_{cs}.D$. Consequently, it is not feasible for *FR* and equals to process two times HECDLP. Thus, the scheme discussed above meets the unforgeability benchmarks as evidenced by the above discussion.

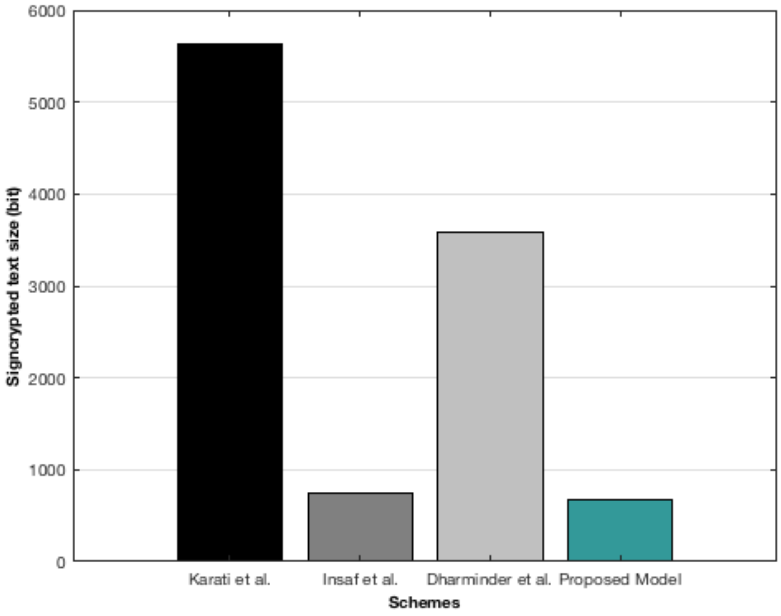

FIGURE 3. Communication cost analysis.

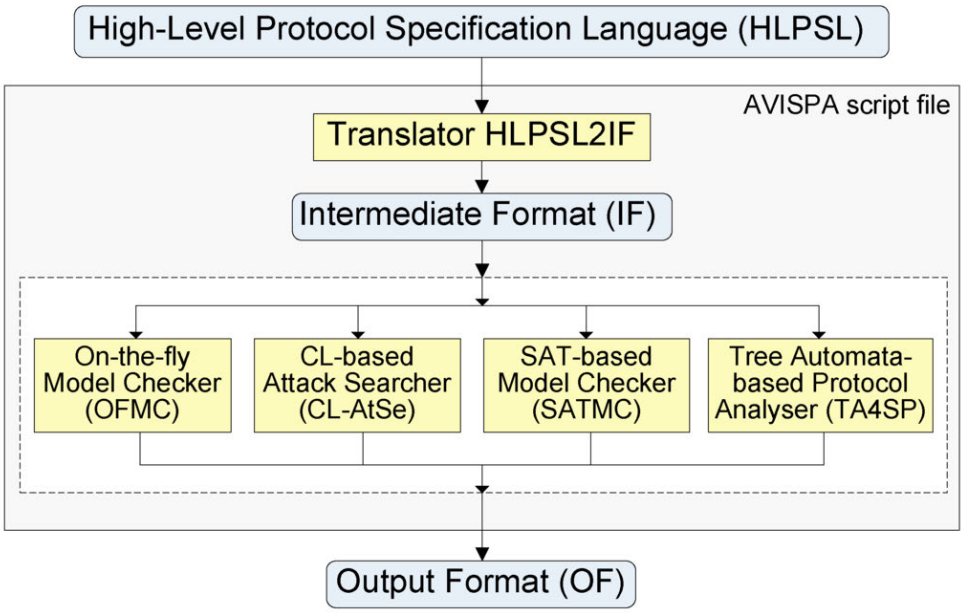

FIGURE 4. Top-down illustration of AVISPA [37].

Theorem 3 ← Integrity

CBS technique is most likely to obtain the integrity security package If there are no $\mathcal{AVr}$ that generates the same hash value for two distinct size/nature messages.

Proof 3: In our scenario, the sender generated the hash function of a plaintext as $\mathcal{Q} = H_3\,(C_{cs}, \mathcal{m}, \mathcal{Y}, ID_{cs}, B_{cs})$ and sent a Ciphertext and signature $\phi = (\mathcal{Q}, \mathcal{Z}, \mathrm{W})$ across an open channel to the receiver. Additionally, the $\mathcal{AVr}$ attempts to retrieve a plaintext from $\mathcal{Q} = H_3\,(C_{cs}, \mathcal{m}, \mathcal{Y}, ID_{cs}, B_{cs})$ for modification, which is not possible because to the irreversible nature of hash functions. In light of the preceding discussion, this method protected the property's integrity.

Theorem 4 ← Non- Repudiation

CBS technique is meant to succeed the security amenity of non-repudiation If a sender cannot reject his signcryptext former.

Proof 4: In our designed CBS method, the sender cannot revoke signature $\mathcal{W} = \mathcal{V} + \mathcal{Q}.P_{cs}$ that has been sent. Though,

TABLE 8. HLPSL code of the proposed scheme.

```
role
role_Cbsigncryption(Cbsigncryption:agent,Cbunsigncryption:agent,Bcs:public_key,Bcus:public_key,SND,RCV:channel(dy))
played_by Cbsigncryption
def=
        local

        State:nat,Pluss:hash_func,Q:text,V:text,Nr:text,M:text,Ns:text,Xor:hash_func,K:symmetric_key
        init
                State := 0
        transition
                1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Cbsigncryption.Cbunsigncryption)
                2. State=1 /\ RCV(Cbunsigncryption.{Nr'}_Bcs) =|> State':=2 /\ V':=new() /\ Q':=new() /\ K':=new() /\ Ns':=new() /\ M':=new() /\ secret(M',sec_2,{Cbsigncryption}) /\ witness(Cbsigncryption,Cbunsigncryption,auth_1,M') /\ SND(Cbsigncryption.{Xor(M'.Ns'.Nr')}_K'.{Pluss(Q'.V')}_inv(Bcs))
end role
role
role_Cbunsigncryption(Cbsigncryption:agent,Cbunsigncryption:agent,Bcs:public_key,Bcus:public_key,SND,RCV:channel(dy))
played_by Cbunsigncryption
def=
        local

        State:nat,Pluss:hash_func,Q:text,V:text,Nr:text,M:text,Ns:text,Xor:hash_func,K:symmetric_key
        init
                State := 0
        transition
                1. State=0 /\ RCV(Cbsigncryption.Cbunsigncryption) =|> State':=1 /\ Nr':=new() /\ SND(Cbunsigncryption.{Nr'}_Bcs)
                6. State=1 /\ RCV(Cbsigncryption.{Xor(M'.Ns'.Nr)}_K'.{Pluss(Q'.V')}_inv(Bcs)) =|> State':=2 /\ request(Cbunsigncryption,Cbsigncryption,auth_1,M') /\ secret(M',sec_2,{Cbsigncryption})
end role
role session1(Cbsigncryption:agent,Cbunsigncryption:agent,Bcs:public_key,Bcus:public_key)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_Cbunsigncryption(Cbsigncryption,Cbunsigncryption,Bcs,Bcus,SND2,RCV2) /\ role_Cbsigncryption(Cbsigncryption,Cbunsigncryption,Bcs,Bcus,SND1,RCV1)
end role
role session2(Cbsigncryption:agent,Cbunsigncryption:agent,Bcs:public_key,Bcus:public_key)
def=
        local
                SND1,RCV1:channel(dy)
        composition
                role_Cbsigncryption(Cbsigncryption,Cbunsigncryption,Bcs,Bcus,SND1,RCV1)
end role
role environment()
def=
```

TABLE 8. *(Continued.)* **HLPSL code of the proposed scheme.**

```
        const

        hash_0:hash_func,bcs:public_key,alice:agent,bob:agent,bcus:public_key,const_1:agent,const_a:public
_key,const_z:public_key,auth_1:protocol_id,sec_2:protocol_id
        intruder_knowledge = {alice,bob}
        composition
                session2(i,const_1,const_a,const_z) /\ session1(alice,bob,bcs,bcus)
end role
goal
        authentication_on auth_1
        secrecy_of sec_2
end goal
environment()
```

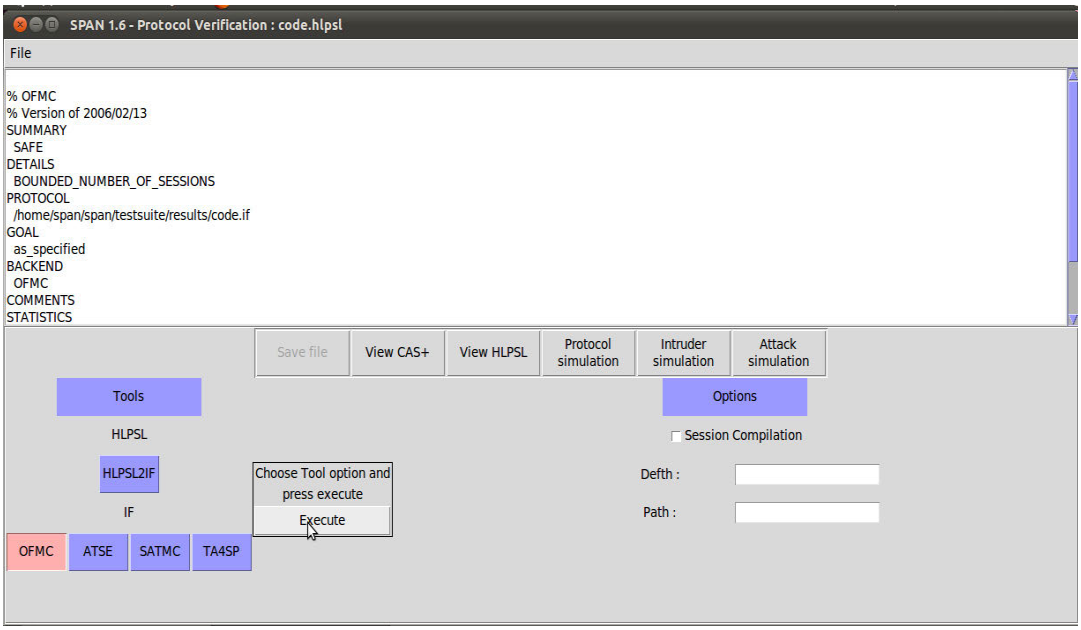

FIGURE 5. OFMC simulation result.

if the sender disputes the signature, the judge does the following computation to resolve the conflict between the receiver and the sender.

$$\begin{aligned} B_{cs} &= C_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \Upsilon \\ &= \left(X_{cs} + \beta_{cs}\right).H_1\left(C_{cs}, ID_{cs}\right) + \vartheta. \\ &= \mathcal{D}(X_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \beta_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \vartheta.\mathcal{D} \\ &= \eta_{cs}.\mathcal{D}.H_1\left(C_{cs}, ID_{cs}\right) + \Omega_{cs}.\mathcal{D}.H_1\left(C_{cs}, ID_{cs}\right) + \vartheta.\mathcal{D} \\ &= \mathcal{D}(\eta_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \Omega_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \vartheta) \\ &= \mathcal{D}(\eta_{cs}.H_1\left(C_{cs}, ID_{cs}\right) + \vartheta + \Omega_{cs}.H_1\left(C_{cs}, ID_{cs}\right)) \\ &= \mathcal{D}(\mu + \Omega_{cs}.H_1\left(C_{cs}, ID_{cs}\right)) = \mathcal{D}(P_{cs}) = B_{cs} \end{aligned}$$

Therefore, the foregoing computations conclude that the sender cannot dispute his signature, as he utilized his private key P_{cs} at the time of digital signature creation as $\mathcal{W} = \mathcal{V} + \mathcal{Q}.P_{cs}$, which is interconnected with their public key B_{cs}.

Theorem 5 ← Forward Secrecy

A CBS system is presumed to realise the security property of forward secrecy if there is no $\mathcal{AVr}$, which compromises message confidentiality by revealing the sender's private key.

Proof 5: Our technique employs a secret key $\mathcal{K}$ in addition to the sender's private key P_{cs}. Here, even $\mathcal{AVr}$ is compromised with the sender's private key P_{cs} however, it also requires the receivers secret key $\mathcal{K}/$, which is not possible for $\mathcal{AVr}$ because the $\mathcal{AVr}$ can recover the decryption key

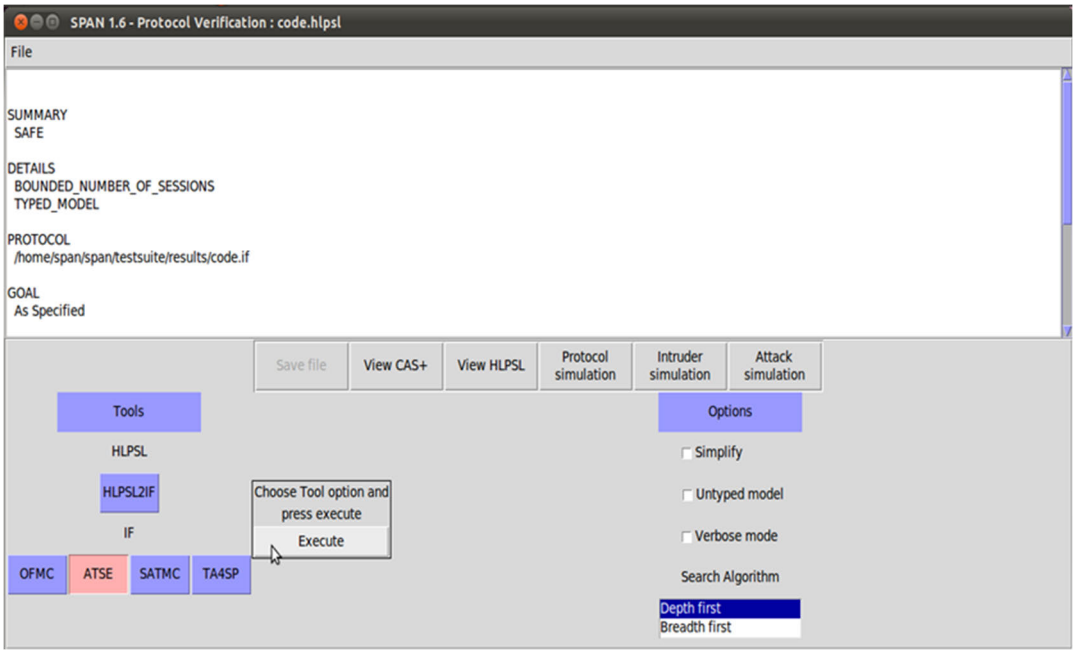

FIGURE 6. ATSE simulation result.

from $\mathcal{K}^{/} = \mathcal{Y}^{/}.P_{cus}$, which further needed P_{cus} from $B_{cus} = P_{cus}.D$. $\mathcal{AVr}$ cannot solve this problem, thus it equals a discrete hyperelliptic curve problem

Consequently, we can conclude from the preceding statements that this design possesses forward secrecy.

Theorem 6 ← ***Anti- Replay Attack***

If there is no $\mathcal{AVr}$, it is anticipated that a CBS Approach will replace the security asset of Anti-Replay Attack, which may be able to collect old messages and resend them to the intended recipient several times.

Proof 5: In the given approach, the receiver first encrypts a nonce n_r using the sender's public key, and then delivers it over to the sender. Once this nonce is decrypted, the recipient generates a new nonce and encrypts the two nonce values (n_r, n_s) and the message as $\mathcal{Z} = (m, n_r, n_s) \oplus H_2(\mathcal{K})$ with the secrete key $\mathcal{K}$. The recipient receives the cypher text $\mathcal{Z}$ from the sender after this operation. As a result, the receiver will verify the freshness of the new nonce n_s and the validity of the old n_r, and if it is true, the Ciphertext will be accepted as a new message; otherwise, the receiver will add this message to the revocation list. Since these two nonces (n_r, n_s) are renewed with each new session, our system is resistant to replay attacks.

VI. COST ANALYSIS

In this section, we compare the proposed scheme to that of Karati *et al.* [32], Ullah *et al.* [33], and Dharminder *et al.* [34] in terms of communication and computation costs. The computational efficiency is defined by the algorithm's computation cost, whereas the communication efficiency is determined by the length of the ciphertext. The symbols *EXPN*, *BIPG*,*HYDM*, $|m|$, $|G|$, and $|n|$ indicate, respectively, Exponentiation, bilinear pairing, Hyper Elliptic Curve Divisor Multiplication, message size in bits, group size in bilinear pairing, and Hyperelliptic Curve parameter size in bits. Here, we neglected the cost of other operations such as hashing, subtraction, and addition, since this operation requires far less time.

The operation and its time are detailed in Tab 2 below, per [35]. In addition, the simulation uses the following hardware and software: Intel Core i74510UCPU, Processor 2.0 with 8GB RAM, Windows 7 and C Library (MIRACL) [37]. HYDM will also need 0.48 milliseconds (ms) [36]. Tab 3 displays the principal operations and their respective costs in milliseconds.

Tab. 5 shows the variables and their corresponding sizes used in the comparative study of communication costs [1]. Tab 6 presents a comparison of communication costs based on our variable assumption. Tabs 4 and 6 provide a comparison of our work with Karati et al. [32], Ullah et al. [33], and Dharminder et al. [34] in terms of computation and communication overheads. According to our comparison study, the presented plan demonstrates the effectiveness of computational and communication overheads, as seen in Fig.2 and Fig. 3. In addition, Tab. 5 and Tab. 7 demonstrate a significant decrease in communication and computation costs.

VII. CONCLUSION

This paper proposes the formal development of an efficient signcryption scheme in a certificate-based IIoT environment. The proposed scheme can be used in large industrial settings. The proposed scheme satisfies confidentiality, unforgeability,

integrity, anti-replay attack, non-repudiation, and forward secrecy. Moreover, the proposed scheme is tested and simulated using AVISPA, a well-known security verification tool. On the basis of two back-end protocol checkers, OF-MC and CL-AtSe, the simulation results indicate that the proposed approach is SAFE in terms of its security assurances. To evaluate the cost-complexity of the proposed scheme, we assess the performance of the proposed scheme and compare it to a variety of relevant existing schemes. The results revealed that the proposed scheme is better in terms of computation and communication costs than the counterpart schemes.

APPENDIX A. IMPLEMENTATION OF THE PROPOSED SCHEME IN AVISPA

Using the popular simulation tool AVISPA [37], [38], we simulate the proposed scheme. AVISPA is a top-down formal validation and verification tool that uses an expressive and flexible High-Level Specification Protocol (HLPSL) [39] to activate the provided code and find security vulnerabilities in the provided protocol. To assess safety standards, the AVISPA tool incorporates four backends checkers, including On-the-fly Model-Checker (OFMC), Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP), and SAT-based Model-checker (SATMC) with HLPSL. The essential framework AVISPA is seen in Fig. 4 where the HLPSL is first converted to the Intermediate Format (IF) with the assistance of the HLPSL2IF translator. This IF is then allocated to the AVISPA back-end safety check tools. The result shows whether or not the suggested protocol is secure and usable in a real setting. In addition, Tabulator 8 and Figures 5 and 6 clearly demonstrate the scheme's safety.

REFERENCES

[1] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C.-M. Chen, and S. Kumari, "A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for industrial Internet of Things (IIoT)," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102625.

[2] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Comput. Secur.*, vol. 94, Jul. 2020, Art. no. 101863.

[3] S. Latif, Z. Zou, Z. Idrees, and J. Ahmad, "A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network," *IEEE Access*, vol. 8, pp. 89337–89350, 2020.

[4] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial Internet of Things: A comprehensive review," *Measurement*, vol. 151, Feb. 2020, Art. no. 107198.

[5] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 56, pp. 476–492, Mar. 2016.

[6] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3242–3254, Mar. 2021, doi: 10.1109/JIOT.2020.3002255.

[7] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)," in *Proc. Annu. Int. Cryptol. Conf.*, 1997, pp. 165–179.

[8] D. He, N. Kumar, and J.-H. Lee, "Privacy-preserving data aggregation scheme against internal attackers in smart grids," *Wireless Netw.*, vol. 22, no. 2, pp. 491–502, Feb. 2016.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," presented at the Workshop Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1984, pp. 47–53.

[10] A. Braeken, P. Shabisha, A. Touhafi, and K. Steenhaut, "Pairing free and implicit certificate based signcryption scheme with proxy re-encryption for secure cloud data storage," in *Proc. 3rd Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, Oct. 2017, pp. 1–7.

[11] H. Yu and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *Comput. J.*, vol. 60, no. 8, pp. 1187–1196, Aug. 2017.

[12] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in cryptology-ASIACRYPT 2003*. Cham, Switzerland: Springer, 2003, pp. 452–473.

[13] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2003, pp. 272–293.

[14] M. Suárez-Albela, P. Fraga-Lamas, and T. 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, no. 11, p. 3868, Nov. 2018.

[15] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, 2016.

[16] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, Aug. 2018.

[17] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Jul. 2020.

[18] 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," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, Dec. 2017.

[19] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.

[20] 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, Dec. 2019.

[21] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. Khanzada, H. Khattak, and M. A. Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Inf. Syst.*, vol. 2020, pp. 1–15, Jul. 2020.

[22] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *Int. J. Adv. Stud. Sci. Res.*, vol. 3, no. 8, 2019.

[23] V. S. Naresh, R. Sivaranjani, and N. V. E. S. Murthy, "Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 15, p. e3763, Oct. 2018.

[24] A. U. 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," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 5, 2018.

[25] S. S. Ullah, I. Ullah, H. Khattak, M. A. Khan, M. Adnan, S. Hussain, N. U. Amin, and M. A. K. Khattak, "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with Internet of Things," *IEEE Access*, vol. 8, pp. 98910–98928, 2020.

[26] A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[27] 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.

[28] 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 Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5099–5108, Sep. 2019.

[29] 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.

[30] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, vol. 14, no. 1, pp. 310–320, Mar. 2020.

[31] Z. Qiao, Q. Yang, Y. Zhou, B. Yang, Z. Xia, M. Zhang, and T. Wang, "An efficient certificate-based aggregate signature scheme with provable security for industrial Internet of Things," *IEEE Syst. J.*, early access, Jul. 19, 2022, doi: 10.1109/JSYST.2022.3188012.
[32] A. Karati, S. H. Islam, G. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2017.
[33] I. Ullah, N. Ul Amin, M. Zareei, A. Zeb, H. Khattak, A. Khan, and S. Goudarzi, "A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications," *Symmetry*, vol. 11, no. 11, p. 1386, Nov. 2019.
[34] D. Dharminder, D. Mishra, J. J. P. C. Rodrigues, R. A. L. Rabelo, and K. Saleem, "PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments," *Softw., Pract. Exper.*, vol. 52, no. 3, pp. 744–755, Mar. 2022.
[35] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Secur. Commun. Netw.*, vol. 2017, pp. 1–17, Dec. 2017.
[36] 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, Dec. 2019.
[37] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: May 2022. [Online]. Available: http://www.avispa-project.org
[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heam, O. Kouchnarenko, J. Mantovani, S. Modersheim, D. von Oheimb, M. Rusinowitch, Santiago, M. Turuani, L. Vigano, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *Computesr Aided Verification*, K. Etessami and S. K. Rajamani, Eds. Berlin, Germany: Springer, 2005, pp. 281–285.
[39] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, 2005, pp. 1–17.

INSAF ULLAH received the M.S. degree in computer sciences from the Department of Information Technology, Hazara University Mansehra, Pakistan, where he is currently pursuing the Ph.D. degree in computer sciences. He is currently serving as a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. He has published more than 25 articles in different journals and conferences. His research interest includes network security.

ABDULLAH ALOMARI (Member, IEEE) received the bachelor's degree in computer from Umm Al-Qura University, Saudi Arabia, in 2008, and the M.Sc. and Ph.D. degrees in engineering mathematics and internetworking from Dalhousie University, Halifax, NS, Canada, in 2012 and 2018, respectively. He is currently an Assistant Professor with the Department of Computer Science, Al-Baha University, Saudi Arabia. His research interests include cybersecurity, the IoT, and emergent technologies in communication networks. He is a member of the IEEE Communication Society and ACM.

AKO MUHAMMAD ABDULLAH received the B.S. degree (Hons.) in mathematics and computer science from the University of Sulaimani, in 2007, the M.S. degree in computer science from Glyndwr University, U.K., in 2010, and the Ph.D. degree in computer science from EMU University, Cyprus, in 2016. He is currently a Lecturer with the Department of Computer Science with the University of Sulaimani, Kurdistan Region, Iraq. His research interests include ad hoc networks, computer networks, wireless networks, and information security.

NEERAJ KUMAR (Senior Member, IEEE) is currently working as a Full Professor with the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India. He is also an Adjunct Professor with Asia University, Taiwan, King Abdul Aziz University, Jeddah, Saudi Arabia, and Newcatle University, U.K. He has highly-cited researcher from WoS, from 2019 to 2021. He has published more than 500 technical research papers (DBLP: https://dblp.org/pers/hd/k/Kumar_0001:Neeraj) in top-cited journals and conferences which are cited more than 32700 times from well-known researchers across the globe with current H-index of 99 (Google Scholar: https://scholar.google.com/citations?hl=en&user=gL9gR-4AAAAJ. He has guided many research scholars leading to the Ph.D. and M.E./M.Tech. He has also edited/authored ten books with international/national publishers such as IET, Springer, Elsevier, and CRC, *Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions* (ISBN-13: 978-1-78561-898-7), *Machine Learning in cognitive IoT* (CRC Press), *Blockchain, Big Data and Machine learning* (CRC Press), *Blockchain Technologies across industrial vertical* (Elsevier), *Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms, and Solutions* (ISBN: 978-981-13-8759-3), *Proceedings of First International Conference on Computing, Communications, and Cyber-Security* (IC4S 2019) (ISBN 978-981-15-3369-3), and *Probabilistic Data Structures for Blockchain based Internet of Things Applications* (CRC Press). One of the Edited text-book titled, *Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms, and Solutions* (Springer, 2019) is having 3.5 million downloads till 06 June 2020. His research is supported by funding from various competitive agencies across the globe. His broad research interests include green computing and network management, the IoT, big data analytics, deep learning, and cyber-security. It attracts attention of the Researchers across the globe (https://www.springer.com/in/book/9789811387586). He is serving as an Editors of *ACM Computing Surveys*, IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, *Computer Communications* (Elsevier), and *International Journal of Communication Systems* (Wiley). Also, he has organized various special issues of journals of repute from IEEE, Elsevier, and Springer. He has won the Best Paper Award from IEEE SYSTEMS JOURNAL in 2018 and 2020 and IEEE ICC 2018, Kansas, in 2018. He has also won the Best Paper Award from Elsevier *Journal of Network and Computer Applications*, in 2021, and IEEE Comsoc IWCMC 2021. He has won the Outstanding Leadership Award from IEEE Trustcom, in 2021. Moreover, he won the Best Researcher Award from parent organization every year from last eight consecutive years. He has been the Workshop Chair at IEEE GLOBECOM 2018, IEEE Infocom 2020 (https://infocom2020.ieee-infocom.org/workshop-blockchain-secure-software-defined-networking-smart-communities), and IEEE ICC 2020 (https://icc2020.ieee-icc.org/workshop/ws-06-secsdn-secure-and-dependable-software-defined-networking-sustainable-smart); and the Track Chair of Security and Privacy of IEEE MSN 2020 (https://conference.cs.cityu.edu.hk/msn2020/cf-wkpaper.php). He is also the TPC Chair and a member for various International Conferences such as IEEE MASS 2020 and IEEE MSN2020.

AMJAD ALSIRHANI received the M.C.S. and Ph.D. degrees from Dalhousie University, Canada, in 2014 and 2019, respectively. He is currently a Full Assistant Professor with Jouf University, Saudi Arabia. He is the Head of the Software Engineering Department, Faculty of Computer Science. He serves as a Chief Information Security Officer (CISO) at Jouf University. He also holds an adjunct professor position at Dalhousie University. His research interests include but are not limited to cybersecurity, network security, cloud computing security, distributed computing systems, and machine and deep learning.

FAZAL NOOR received the B.Eng. and M.Eng. degrees in electrical and computer engineering from Concordia University, Montreal, Canada, in 1984 and 1986, respectively, and the Ph.D. degree in engineering from McGill University, Montreal, in 1993. He is currently a Full Professor with the Faculty of Computer and Information Systems (FCIS), Islamic University of Madinah, Saudi Arabia. He has published numerous papers in various reputable international journals and conferences. He has been a reviewer for IEEE, Elsevier, Springer, and various other journals. He held the position of the vice dean of graduate studies and scientific research at FCIS. He was a Program Coordinator for Master of Computer Science program. He has received the Best Faculty Award in 2007. He has been a TPC member of many conferences. He is a fellow of IAER. He has been QA Evaluator for computer engineering program. His research interests include AI, FANETS, neural networks, embedded systems, signal processing, security, the IoT, optimization algorithms, and parallel and distributed computing.

SADDAM HUSSAIN received the bachelor's and master's degrees from the Islamia College, Peshawar, Pakistan, and Hazara University, Masehra, Pakistan, in 2017 and 2021, respectively. He is currently pursuing the Ph.D. degree from the School of Digital Science, Universiti Brunei Darussalam. He has published more than 60 papers in well-reputed journals, including IEEE, *Journal of Information Security and Applications* (Elsevier), Cluster Computing, Computer Communication, IEEE Internet of Things Journal, Hindawi, CMC, Sensors, Energies, and Electronics. He is a Reviewer in reputed journals, including IEEE Access, *International Journal of Wireless Information Networks*, Scientific Journal of Electrical Computer and Informatics Engineering, and CMC. His research interests include cryptography, network security, wireless sensor networking (WSN), information-centric networking (ICN), named data networking (NDN), blockchain, smart grid, the Internet of Things (IoT), IIoT, quantum computing, cloud computing, and edge computing.

MUHAMMAD ASGHAR KHAN received the Ph.D. degree in electronic engineering from the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He works as an Assistant Professor with the Electrical Engineering Department, Hamdard University, Islamabad. He is a reviewer for various journals published by IEEE, Elsevier, Springer, MDPI, and EURASIP. He has served as a guest editor for a number of international journals. He has published more than 100 technical and review articles in leading journals such as the IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, IEEE Internet of Things Journal, and has presented his work at multiple national and international conferences. His main research interests include Drones/UAVs with a focus on networks, platforms, security, as well as applications and services.