IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 26, 2020, accepted October 7, 2020, date of publication October 26, 2020, date of current version November 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3033758

A Lightweight and Secured Certificate-Based Proxy Signcryption (CB-PS) Scheme for E-Prescription Systems

INSAF ULLAH[1], NOOR UL AMIN[1], AHMAD ALMOGREN[2], (Senior Member, IEEE), MUHAMMAD ASGHAR KHAN[3], M. IRFAN UDDIN[4], AND QIAOZHI HUA[5]

[1]Department of Information Technology, Hazara University Mansehra, Mansehra 21120, Pakistan
[2]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]HIET, Hamdard University, Islamabad Campus, Islamabad 44000, Pakistan
[4]Institute of Computing, Kohat University of Science and Technology, Kohat 26000, Pakistan
[5]Computer School, Hubei University of Arts and Science, Xiangyang 441000, China

Corresponding authors: Qiaozhi Hua (11722@hbuas.edu.cn) and Ahmad Almogren (ahalmogren@ksu.edu.sa)

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

ABSTRACT Electronic prescription (E-prescription) is an emerging technology that allows health practitioners (doctors, physicians, pharmacists, or nurses) to electronically transmit prescriptions to pharmacies. E-prescription systems allow doctors to avoid traditional medical practices in which prescriptions are sent manually in handwritten form. Additionally, in cases in which a patient may not be able to collect the medication in person due to physical disabilities, the medications can be delivered to the patient's home directly. Furthermore, payments can also be made online (e.g., using credit cards or bank transfers). However, these distinctive features require a series of guidelines for the successful deployment of the E-prescription system due to stringent legal requirements and privacy regulations. Two major security requirements i.e. confidentiality and authentication need to be addressed. In general, the solution to ensuring confidentiality and authentication lies in the combination of both the encryption and digital signature functions in a single logic step called signcryption. Therefore, in this article, we present a lightweight and provable secured certificate-based proxy signcryption (CB-PS) scheme for e-prescription systems. The formal security verification uses the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool along with informal security analysis, which authenticates that the proposed CB-PS scheme can potentially be implemented in resource-constrained low-computing electronic devices in E-prescription systems.

INDEX TERMS E-prescription, smart pharmacy, certificate based signcryption, AVISPA, hyper elliptic curve.

I. INTRODUCTION

Electronic prescription (EP) is an emerging technology, which replaces the hand written prescription and allows the health care practitioners (Pharmacist, Doctor, Nurses, etc.) to electronically transmit prescriptions to the smart Pharmacies [1]. Before this ecosystem, the patients were checked by the doctor, diagnose the disease, and after that the patient collect medication from the Pharmacy. Therefore, in EP after examining the patient, a doctor generates an e-prescription and uploads this prescription to the medical database server (MDS)/smart pharmacy server (SPS). Later, the patient sends the medication request to the pharmacy electronically. Further, the pharmacy verifies the request, if the verification process is successfully done, then it downloads the prescription from the MDS/SPS and sends the medication to the patient [2]. Though, the transmission is done through open network (internet), in which the attacker can easily access to the message, reveal the actual contents, and injecting a new message to the network on behalf of the actual sender. To avoid the circumstances like that, the communication must be ensured with the security requirement of confidentiality, authenticity, non-repudiation, and unforgeability, respectively. To meet such type of security countermeasures

The associate editor coordinating the review of this manuscript and approving it for publication was Chunhua Su.

during transmission of prescription related data, one such solution is signcryption [3]. The signcryption combine a digital signature and encryption on prescription, in which the digital signature will ensure authenticity, non-repudiation, and unforgeability and encryption maintain confidentiality of messages.

Therefore, the problems will arise, if the patient may not able to collect their medication or send a request for medication to the smart Pharmacy. In this situation, the patient gives their medication collection rights to another person (agent), who communicates regarding the collection of the medication on behalf of the patient. This communication is known as proxy communication, which was first introduced by Membo in the form of a proxy signature [4]. The proxy signature enables an entity to give their digital signature capability to another entity (proxy) for a specific reason, i.e. (a lack of resources, temporary absence, or illness), then the proxy produces the digital signature in place of an actual entity.

In 1998, Gamage *et al.* [5] proposed a proxy signcryption (PS), which is the enhanced version of Membo scheme, i.e., [4], by providing authentication with confidentiality in one step. Normally, the proxy signcryption schemes are based on two main techniques, i.e., asymmetric cryptography and mathematical hard problems. First, we discuss some asymmetric cryptography, which are public key infrastructure (PKI), identity-based cryptography (IDBC), and certificateless cryptography (CC), respectively. However, the PKI is suffering from certificate management and it is very costly [6], because the certificate is bind with the public key users. The IDBC is affected by the key escrow problem; it means that if private key generation center (PKG) is malicious then he can easily generate a forge signature on the behalf of actual users, because in IDBC the PKG produces the private key for users [7]. The CC is designed to overcome the key escrow flaw of IDBC, in which the key generation center (KGC) makes the partial private key and distribute it by using secure channel that can also a problem [8]. Here, for removing the aforementioned flaws, one such solution is certificate-based cryptography (CBC) is available [9], which enables the users to generate their public and private key by themselves. Then, the users send their public keys with identities to the (CA) using an unsecure channel. After reception the identities and public keys of users, the CA generates a certificate for each user and delivers it by using an unsecure channel. The certificate is performing the work of decryption key as like in identity-based cryptography.

Second, we shortly explain the mathematical hard problems which are used for the efficiency and security hardiness of proxy signcryption schemes that are RSA, bilinear pairing (BP), elliptic curve (EC), and hyper elliptic curve (HEC), respectively. RSA is the widely used mathematical technique, which utilizes 1024 bits key while designing cryptographic algorithms [10]. Another method is bilinear pairing, which is used nowadays in most of the cryptographic schemes and it is observed from [11] that BP is

$$\mathbb{hEc} : Q^2 + U(V)Q = F(V) \bmod p, \tag{1}$$

approximately 13.3 milliseconds (ms) worse than RSA. To overcome the limitations like the high key size of BP and RSA, one good solution is provided by EC and it is best approximately 1 time from RSA and 13.3 times better than BP. In contrast, the hyper elliptic curve needs 0.48 ms [12], which can be the most suitable choice for the devices that are resource hungry.

Keeping in view the aforementioned discussion, we proposed a lightweight and provable secured certificate-based proxy signcryption (CB-PS) for an E-prescription system. We represent our contributions through the following steps.

- We first give the syntax of certificate-based proxy signcryption
- We provide the network model for E-prescription system utilizing the concept of our new certificate-based proxy signcryption (CB-PS) scheme
- We present the construction certificate-based proxy signcryption (CB-PS) algorithm using the concept of the hyper elliptic curve
- We perform the security analysis in two ways that are formal which are done through AVISPA and informal security analysis, i.e., warrant unforgeability, confidentiality, integrity, message unforgeability, non-repudiations, resists replay attacks, and forward secrecy, while the simulation results as well as security analysis shows our scheme safeguards all the measures attacks
- We provide the computing and communications cost comparison analysis against the existing related scheme and the results clearly shows our new scheme is ensuring better performance

A. PAPER ORGANIZATION

This article is organized as follows: section II presents the preliminaries, section III describes related work, section IV presents a system architecture, section V describes the construction of proposed scheme, section VI explains the implementation and validation of proposed scheme in AVISPA, section VII briefly explains the security analysis, and efficiency, and section VIII presents the conclusions.

II. PRELIMINARIES

In this phase, we explain some of the basic material and methods which are used in our proposed system that are hyper elliptic curve, syntax of certificate-based proxy signcryption, adversary model, and basics of AVISPA tool, respectively. So, we explain all these, one by one in the following subsections of this phase.

A. HYPER ELLIPTIC CURVE

The $\mathbb{hEc}$ is the compressed form of $\mathbb{Ec}$, which contains fewer key and parameters size [13], [14]. Equation 1 represents the $\mathbb{hEc}$ of genus $\mathcal{G} \succeq 2$ over a finite field $\mathcal{U}_p$.

Where $U, F \in [V]$, the degree of $(F) = 2\mathcal{G} + 1$, and the degree of $(U) \preceq \mathcal{G}$, F is monic. Equation 1 represents the $\mathbb{hEc}$ of $\mathcal{G}$ over K, where K is the algebraic closure of $\acute{K}$, and no point exists on the curve. Further, it must satisfy both partial derivatives like $2Q + U = 0$ and $F/\text{-}\ U/Q = 0$. This condition ensures that the $\mathbb{hEc}$ curve is non-singular. Also, we present the negative of a $P = (V, Q)$, which is -$P = (V, -Q, (V))$. Additionally, the $\mathbb{hEc}$ point cannot form a group like $\mathbb{Ec}$ points. The hyper elliptic curve forms an Abelian group [15] called a Jacobian group $J_{\mathbb{hEc}}(\mathcal{U}_p)$, and the order $(J_{\mathbb{hEc}}(\mathcal{U}_p))$ of the Jacobian as

$$\left|\left(\sqrt{p}-1\right)^{2\mathcal{G}}\right| \leq \mathcal{O}(J_{\mathbb{hEc}}(\mathcal{U}_p)) \leq \left|\left(\sqrt{p}+1\right)^{2\mathcal{G}}\right| \quad (2)$$

After making the Jacobian group $J_{\mathbb{hEc}}(\mathcal{U}_p)$, select an integer $\mathcal{D}$ as a divisor that is the generator of the group and represent it in the following Mumford form [16]:

$$D = (A(V), B(V)) = \left(\sum_{a=0}^{\mathcal{G}} A_a V^a, \sum_{a=0}^{\mathcal{G}-1} B_a V^a\right) \quad (3)$$

Suppose $\delta \in \{1, 2, 3 \ldots., p-1\}$ and $\mathcal{D}$ is the selected divisor from the Jacobian group $J_{HEC}(\mathcal{U}_p)$. Let the $\mathcal{N} = \delta.$, and finding δ from this equation is called the $\mathbb{hEc}$ discrete logarithm problem ($\mathbb{hEc}$ - $\mathbb{D}$-$\mathbb{LP}$) [17].

B. SYNTAX OF CB-PS

Our scheme consists of seven steps: setup, generate public variant (GPV), generate certificates (GC), generate a user key (GUK), generate delegation (GD), generate proxy signcryption (GPS), and verification and Unsigncryption (VU).

Setup: This step is normally processed by the certificate authority (CA) by taking as input the security parameter ($\mathcal{Y}$) and producing the public parameters param $\mathfrak{P}$, master secret key ($m\mathcal{s}\mathcal{k}$) and master public key ($mp\mathcal{k}$).

GPV: This step is processed by each participant (original user, proxy, and receiver) with its identity ($\mathrm{ID}_{\mathcal{U}}$) to generate the public variant $\mathcal{X}_{\mathcal{U}}$. So each participant with its identity ($\mathrm{ID}_{\mathcal{U}}$) transmits $\mathcal{X}_{\mathcal{U}}$ to CA using an insecure channel.

GC: Given $\mathrm{ID}_{\mathcal{U}}$, $\mathcal{X}_{\mathcal{U}}$, and $m\mathcal{s}\mathcal{k}$, the GC step is processed by the CA, to make a certificate ($\mathrm{Cert}_{\mathcal{U}}$) for each participant (user, proxy, and receiver) with identity ($\mathrm{ID}_{\mathcal{U}}$). Then CA transmits the certificate ($\mathrm{Cert}_{\mathcal{U}}$) along with some auxiliary variable ($\mathcal{N}_{\mathcal{U}}$) by using an insecure channel to each participant with identity ($\mathrm{ID}_{\mathcal{U}}$).

GUK: Given $\mathrm{ID}_{\mathcal{U}}$, $\mathrm{Cert}_{\mathcal{U}}$, and $\mathcal{N}_{\mathcal{U}}$, the GUK step is processed by each participant (user, proxy, and receiver) with identity ($\mathrm{ID}_{\mathcal{U}}$) to generate the public key ($\mathcal{J}_{\mathcal{U}}$) and private key ($\mathcal{Q}_{\mathcal{U}}$).

GD: Given the public and private key of the patient ($\mathcal{J}_{\mathrm{p}}$, $\mathcal{Q}_{\mathrm{p}}$), patient identity (ID_{p}), certificate of patient ($\mathrm{Cert}_{\mathrm{p}}$), and warrant message ($m_{\mathcal{W}}$). The GD step is processed by the original user (patient) to produce delegation Ψ of the warrant message ($m_{\mathcal{W}}$) and send through insecure channels to the proxy (agent).

GPS: This step is processed by the proxy (agent) to produce a proxy signcryption tuple ψ of the message (m) and send it through insecure channels to the receiver (Smart Pharmacy). This process takes as input the public and private key of agent ($\mathcal{J}_{\mathrm{a}}$, $\mathcal{Q}_{\mathrm{a}}$), patient and receiver identities (ID_{a}, $\mathrm{ID}_{\mathrm{sp}}$), certificate of agent ($\mathrm{Cert}_{\mathrm{a}}$), certificate of smart pharmacy ($\mathrm{Cert}_{\mathrm{sp}}$), public key of smart pharmacy ($\mathcal{J}_{\mathrm{sp}}$), and message ($m$).

VU: This step is processed by the receiver (smart pharmacy) to verify and decrypt the proxy signcryption tuple ψ of the message (m). This process takes as input the public and private key of smart pharmacy ($\mathcal{J}_{\mathrm{sp}}$, $\mathcal{Q}_{\mathrm{sp}}$), agent and smart pharmacy identities (ID_{a}, $\mathrm{ID}_{\mathrm{sp}}$), certificate of agent ($\mathrm{Cert}_{\mathrm{a}}$), public of agent ($\mathcal{J}_{\mathrm{a}}$), and proxy signcryption tuple ψ.

C. BASICS OF AVISPA

Automated validation of internet security protocol and applications (AVISPA) is a formal tool for checking the security claims of cryptographic algorithms [18]. It contains a graphical user interface (GUI) of the security protocol animator (SPAN) [19]. In Figure 1, we demonstrate the overall structure of an AVISPA tool. In a situation in which the user wants to check the security claims of his proposed algorithm, then he first produces the high-level protocol specification language (HLPSL) code in the SPAN of this algorithm [20]. Then, a translator (HLPSL2IF) translates the HLPSL code into an intermediate format (IF). Then, the IF of the code will be verified through four different embedded verification tools: The On-the-Fly-Model-Checker (OFMC) [21], CL-Constraint-Logic-based model-checker (ATSE) [22], SAT-based Model-Checker (SATMC) [23], and Tree Automata based on automatic approximations (TA4SP) [24]. These embedded tools, check the security claims of the said IF code of an algorithm for two types of attack, i.e. resists against the replay and man-in-the-middle attack. If the IF code resists against these two attacks, then the embedded tools (OFMC, ATSE, SATMC, TA4SP) give the result of SAFE, state; otherwise, it gives the UNSAFE state [25].

D. THREAT MODEL

We consider the Dolev-Yao adversary model for our proposed certificate-based proxy signcryption scheme, which means an adversary has full command of the communication channel [26]. Further, in this model, the adversary has the full ability to generate a forge signature on a warrant message; it means that an adversary has the full command to destroy the authentication process among original sender and proxy (agent). The adversary has the full ability to capture all the messages that are sent through Dolev-Yao model communication channel; it means that an adversary destroys the confidentiality of a transmitted Ciphertext. Once an adversary destroys the confidentiality of a transmitted Ciphertext, then it can easy for him/her to modify the Ciphertext. The adversary has also a command to generate a forge signature on a message; it means that an adversary has the full command to destroy the authentication process among proxy (agent) and receiver.

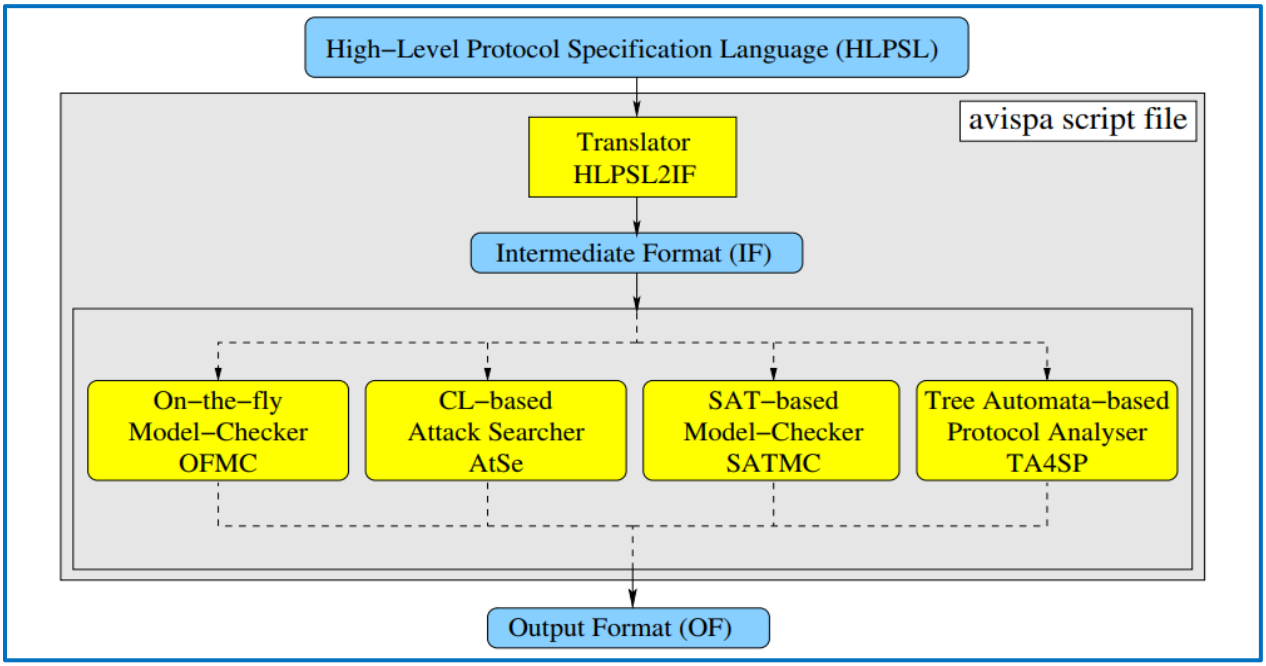

FIGURE 1. Structure of AVISPA.

III. RELATED WORK

In Table 1, we provide the limitations of existing PS schemes and the advantages of our new scheme.

In 1998, Gamage *et al.* [5] proposed a proxy signcryption (PS), which was the enhanced version of Membo scheme, i.e., [4], by providing authentication with confidentiality in one step. It allows the principle participant that delegates his signing capacity to another participant (proxy), and then proxy produces the signcryption for principle participant and transmits it to the legitimate recipients. However, the Gamage PS is affected by needing the secure network between principle participant and proxy. It is also affected by heavy exponential operations requirements. In 2004, Zhang *et al.* [27], designed a PS scheme with the claimed security requirement that are public verifiability, forward secrecy, and protected the proxy from principle participant forgery attack. It is also affected by heavy exponential operations requirements and suffering from certificate management issues.In 2006, Elkamshouchy *et al.* [28], removing the concept of secure channel between principle participant and proxy, designed a new PS scheme with the service of public verifiability. Nevertheless, the authors of the contributed scheme are failing to provide the security proofs and also failed by not includes the comparison in term computational as well as communication cost with existing PS schemes. It is also affected by heavy exponential operations requirements and suffering from certificate management issues.

In 2009, Elkamchouchi *et al.* [29], by using the concept of integer factorization, one-way hash function, discrete logarithm problem, and Diffie-Hellman problem and contribute a PS scheme, which provide public verifiability property not only between principle participant and proxy, but also among proxy and receiver. The scheme also meets the property of forward security and protect the proxy from principle participant. However, the certificate is binding with the public key of participant which is so costly process and further the exponential operation is required more power of computing time. In 2010, Lin *et al.* [30], designed a provable secured PS scheme and secure under the two main functionalities of random oracle model that are adaptive chosen-Ciphertext attacks (IND-CCA2) and existential forgery under adaptive chosen-message attacks (EF-CMA). However, the scheme is affected by the lack of certain security flaws that are Anti-replay attack and forward security. It's also affected by weighty bilinear pairing operations requirements and anguish from certificate management issues. In 2011, Elkamchouchi *et al.* [31], a light weight PS scheme for resource hungry devices that are mobile phone and pager, etc., however, the authors are failing to provide computational as well as communication cost comparisons with the relevant existing PS schemes. They also failed to provide any sort of security proofs such as formal and informal. Additionally, due to usage 160 bits key elliptic key size, it cannot be suitable for low power devices.

In 2013, Elkamchouchi *et al.* [32], contributed the two new PS schemes, in which they are claiming for better countermeasures with respect to cost and security. The first scheme is based on the old discrete problem and the second one realized on the mathematical functionality of elliptic curves. However, the elliptic curve and discrete logarithm problem need a more power consumption during the computation process. The authors are failing to provide some formal security proofs and

TABLE 1. Limitations of the literature.

S.No	Schemes	Year	Disadvantages
1	Gamage [5]	1999	• Effected by needing the secure network between principle participant and proxy • Affected by heavy exponential operations requirements
2	Zhang et al [27]	2004	• Suffering from certificate management issues • Affected by heavy exponential operations requirements
3	Elkamshoushy et al [28]	2006	• Failing to provide the security proofs • Not includes the comparison in term computational as well as communication cost with existing PS schemes • It is also affected by heavy exponential operations requirements • Suffering from certificate management issues
4	Elkamchouchi et al [29]	2009	• It is also affected by heavy exponential operations requirements • Suffering from certificate management issues
5	Han et al [30]	2010	• Lack of certain security flaws that are Anti-replay attack and forward security • Affected by weighty bilinear pairing operations requirements • Anguish from certificate management issues
6	Elkamchouchi et al [31]	2011	• The authors are failing to provide computational as well as communication cost comparisons with the relevant existing PS schemes • Also failed to provide any sort of security proofs such as formal and informal. • Due to usage 160 bits key elliptic key size, it cannot be suitable for low power devices
7	Elkamchouchi et al [32]	2013	• The elliptic curve and discrete logarithm problem need a more power consumption during the computation process. • The authors are failing to provide some formal security proofs • And also binding a certificate with the public key of a participant is very costly.
8	Lo and Tsai [33]	2014	• The issue of certificate management • Need more computing power and requires greater bandwidth space • Lack of forward secrecy and anti-replay attack
9	Ming and Wang [34]	2015	• It required more computing time due bilinear pairing heavy operations • Certificate management issue and requires greater bandwidth space • Lack of forward secrecy and anti-replay attack
10	Zhou [35]	2016	• The scheme has a lack of forward security and anti-replay attack security services • It also can be affected by the key escrow problem and heavy pairing operations
11	Abdelfatah [36]	2017	• Lack of formal security analysis and suffering from the absence of anti-replay attack security property • It can also be affected by elliptic curve point scalar multiplication, which need more time
12	Bhatia and Verma [1]	2017	• Lack of forward security and ant-replay attack • Affected by the public key replacement attack
13	Zhou et al [38]	2018	• Affected by greater consumption of pairing operations • It's not ensured the property of anti-replay attack and forward security
14	Huifang et al [39]	2018	• The scheme can be affected by the key escrow problem and substantial pairing operations
15	Li et al [2]	2018	• Affected by the need of secure link for the distribution of partial private key among the participants • It's also suffering from the absence of forward security and anti-replay attack

Advantages of Our Scheme

- **Our new scheme is formally validated through the AVISPA tool and the result shows that it is SAFE**
- **Also, it is not suffering from certificate management issue, key escrow issue, public key replacement issue, and secure channel need problem.**
- **The new scheme ensured the security requirements, i.e., Warrant Unforgeability, Confidentiality, Integrity, Unforgeability, Forward Secrecy, and Resists Replay Attack, respectively**
- **Our scheme is not affected by heavy computation because we used hyper elliptic curve which need very miner time for computations [11,12] instead of bilinear pairing and elliptic curve**
- **Our scheme is not affected by needing more bandwidth utilization because the hyper elliptic curve used very small size key (80 bits)**

also binding a certificate with the public key of a participant is very costly. In 2014, Lo and Tsai [33], a provable secured PS scheme is presented for efficient communication system. However, the scheme contains certain limitations that are the issue of certificate management, need more computing power, requires greater bandwidth space, lack of forward secrecy, and lack anti-replay attack.

Ming et al [2014], combined the concept of identity-based cryptography and bilinear pairing with proxy communication and make a new PS scheme, which is secured under standard model. However, the scheme has the limitation of key escrow and the private key distributions among the users and private key generation center needs secure network. Also, it can be affected by the heavy computation power need, if it is applied to the environment, which contain a resource limited device.

In 2015, Ming and Wang [34], a provable secured PS scheme under the theoretical analysis technique called standard model. However, the scheme is anguish from a number flaws that are it required more computing time due bilinear pairing heavy operations, certificate management issue, need more computing power, requires greater bandwidth space, lack of forward secrecy and lack anti-replay attack. In 2016, Insafullah *et al.* [17], designed a generalized hyperelliptic curve-based PS scheme. The authors of this scheme are failing to provide a formal security analysis and this new scheme also suffering the lack anti-replay attack. It's also affected by the certificate management problem.In 2016. Zhou [35], provides a three modes PS scheme, which provide encryption only technique, proxy signature in a single algorithm. The scheme has a lack of forward security and anti-replay attack security services. It also can be affected by the key escrow problem and heavy pairing operations.

In 2017. Abdelfatah [36], an elliptic curve based novel PS scheme is presented. The authors of this new PS, failing to provide formal security analysis and suffering from the absence of anti-replay attack security property. It can also be affected by elliptic curve point scalar multiplications, which need more time.In 2017, Bhatia and Verma [1], first did the cryptanalysis of Yanfeng *et al.* [37] and proved that it is not resisted against the forgery attack. They also provide a secure PS scheme for the E-prescription system. However, the scheme hasn't ensured the services of security, such as forward security and ant-replay attack. It's also affected by the public key replacement attack.

In 2018, Zhou *et al.* [38], provide a three mode PS scheme based on bilinear pairing. However, the scheme can be affected by greater consumption of pairing operations and it's not ensured the property of anti-replay attack and forward security. In 2018, Yu *et al.* [39], by using the concept of universal composability proposed identity-based PS scheme. However, the scheme can be affected by the key escrow problem and substantial pairing operations.In 2018, Li *et al.* [2], first of all proved that the scheme of Bhatia and Verma [1] is not resist against the public key replacement attack and then present a new Certificateless PS scheme for E-prescription system. However, the scheme is affected by the need of secure link for the distribution of partial private key among the participants. It's also suffering from the absence of forward security and anti-replay attack.

Thus, removing all the discussed flaws of the above discussed PS schemes, we present a new lightweight and provable secured certificate-based proxy signcryption (CB-PS) for an E-prescription system. Our new scheme is formally validated through the AVISPA tool and the result shows that it is SAFE. Also, it is not suffering from certificate management issue, key escrow issue, public key replacement issue, and secure channel need problem. The new scheme ensured the security requirements, i.e., Warrant Unforgeability, Confidentiality, Integrity, Unforgeability, Forward Secrecy, and Resists Replay Attack [40]–[43], respectively. Our scheme is not affected by heavy computation because we used hyper elliptic curve instead of bilinear pairing and elliptic curve which need very miner time for computations [11], [12]. Our scheme is not affected by needing more bandwidth utilization because the hyper elliptic curve used very small size key (80 bits).

IV. SYSTEM ARCHITECTURE

We present a new E-prescription system using certificate-based proxy signcryption, as shown in Figure 2. This setup consists of six entities: the certificate authority (CA), patient, agent, smart pharmacy (SP), prescriber (Doctor), and database server (DBS), respectively.

Note that, in our system the Doctor is pre-upload the prescription to DBS. So, the tasks of the other entities in the following steps are discussed.

Certificate Authority (CA): CA is responsible for creating all the public parameter which is used for making the algorithm. It is also responsible to make certificate for each participant if it is received, request for a certificate with an identity and public variable.

Patient: It plays the role actual participant and delegates the rights of signcryption on medication request query to the proxy (agent).

Proxy (agent): Upon the reception of a delegation from Patient, Proxy first verifies the delegation if it is true then, it generates a signcryption on medication request query and transmits it to the smart pharmacy (SP).

Smart Pharmacy (SP): Upon the reception of signcrypted medication request query, SP first performs the verification and decryption process if it is successfully done, then PS downloads the prescriptions from DBS and send the medication to Proxy accordingly. At the end of this section, we provide the symbols used in a proposed scheme in Table 2.

V. PROPOSED SCHEME CONSTRUCTIONS

A. PROPOSED CB-PS SCHEME

Our CB-PS includes the following seven algorithms.

Setup: In this algorithm, the CA first selects $\mathscr{k} \in \{1, 2, \ldots\ldots, p-1\}$ as a master private key and computes the master public key $\mathscr{mpk} = \mathscr{msk}.\ \mathcal{D}$. Also, it selects and

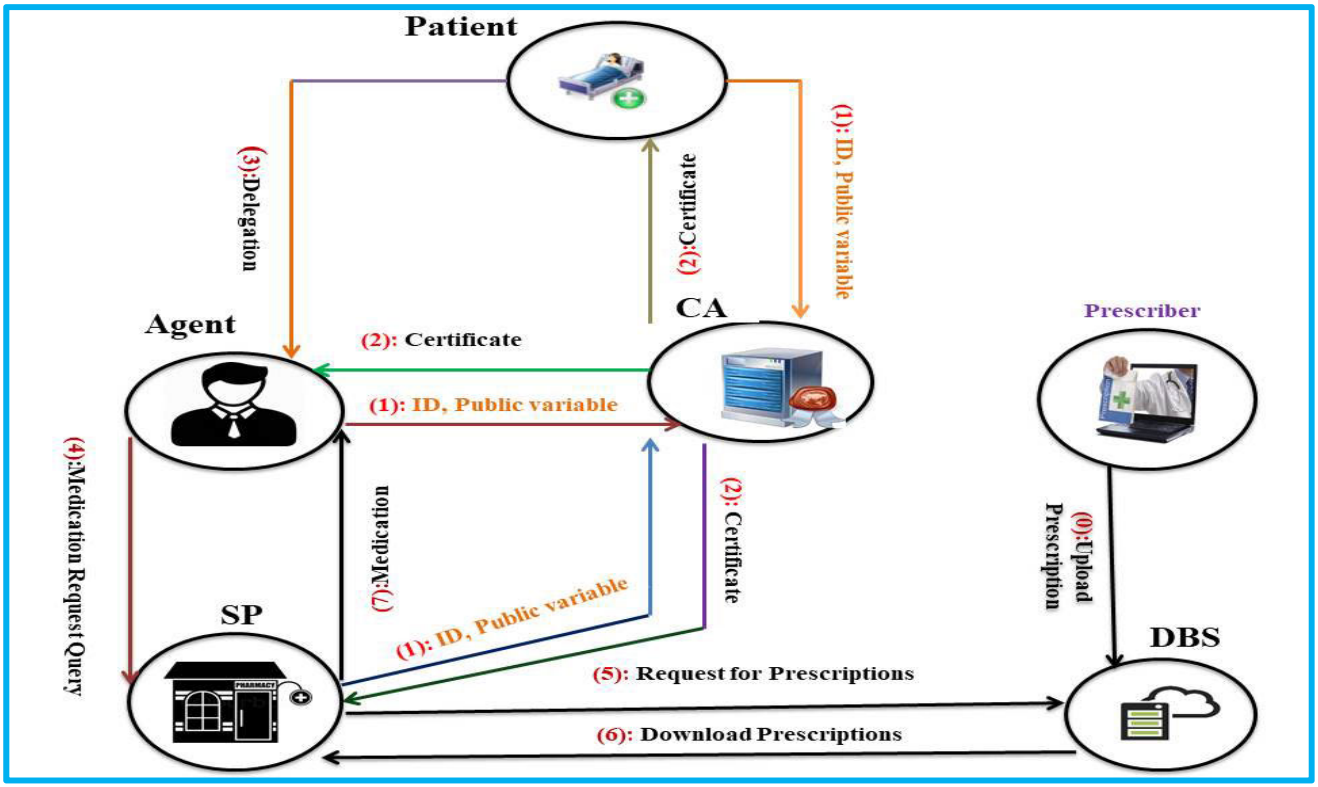

FIGURE 2. Proposed scheme flow.

publishes the public parameter set $\{m p\hbar, , \text{Cert}_{\mathcal{U}}, \mathcal{Y}, \text{ID}_{\mathcal{U}}, h_1, h_2, h_3\}$.

GPV: In this algorithm, each participant (original user, proxy, and receiver) with identity ($\text{ID}_{\mathcal{U}}$) selects a random number $\beta_{\mathcal{U}} \in \{1, 2, \ldots\ldots, p-1\}$ and computes the public variant $\mathcal{X}_{\mathcal{U}} = \beta_{\mathcal{U}}.\ \mathcal{D}$. Then, it sends the pair ($\text{ID}_{\mathcal{U}}$, $\mathcal{X}_{\mathcal{U}}$) to CA using an insecure channel.

GC: In this algorithm, the CA makes a certificate ($\text{Cert}_{\mathcal{U}}$) for each participant (user, proxy, and receiver) with identity ($\text{ID}_{\mathcal{U}}$) and then sends the $\text{Cert}_{\mathcal{U}}$ and auxiliary number $\mathcal{N}_{\mathcal{U}}$ using an insecure channel. The following steps denote the certificate generation process.

- CA first selects a random number $\vartheta_{\mathcal{U}} \in \{1, 2, \ldots\ldots, p-1\}$
- Compute $\Upsilon_{\mathcal{U}} = \vartheta_{\mathcal{U}}.\ \mathcal{D}$
- Define certificate $\text{Cert}_{\mathcal{U}} = \Upsilon_{\mathcal{U}} + \mathcal{X}_{\mathcal{U}}$
- Compute $\mathcal{N}_{\mathcal{U}} = h_1(\text{Cert}_{\mathcal{U}} \| \text{ID}_{\mathcal{U}})\vartheta_{\mathcal{U}} + m\hbar$
- Send pair $\Delta = (\text{Cert}_{\mathcal{U}}, \mathcal{N}_{\mathcal{U}})$ to each participant using an insecure channel

GUK: The GUK is processed by each participant (user, proxy, and receiver) with identity ($\text{ID}_{\mathcal{U}}$) to generate the public and private key pair ($\mathcal{J}_{\mathcal{U}}$, $\mathcal{Q}_{\mathcal{U}}$). A participant with identity ($\text{ID}_{\mathcal{U}}$) computes the private key as $\mathcal{Q}_{\mathcal{U}} = h_1(\text{Cert}_{\mathcal{U}} \| \text{ID}_{\mathcal{U}})\beta_{\mathcal{U}} + \mathcal{N}_{\mathcal{U}}$ and then generates the public key $\mathcal{J}_{\mathcal{U}} = \mathcal{Q}_{\mathcal{U}}.\ \mathcal{D}$.

GD: The GD is processed by the original user (patient) to produce delegation $\Psi = (m_{\mathcal{W}}, \mathcal{Z}, \text{JI})$ on warrant message ($m_{\mathcal{W}}$) and send it through insecure channels to the proxy (agent). This process takes as input the public and private key of patient ($\mathcal{J}_{\text{p}}$, $\mathcal{Q}_{\text{p}}$), patient identity (ID_{p}), certificate of patient (Cert_{p}), and warrant message ($m_{\mathcal{W}}$). The following steps denote the delegation generation process.

- The patient first selects a random number $\mathcal{L} \in \{1, 2, \ldots\ldots, p-1\}$
- Compute $\mathcal{Z} = \mathcal{L}.\ \mathcal{D}$ and $\text{T} = h_2(\text{Cert}_{\text{p}} \| \text{ID}_{\text{p}}, m_{\mathcal{W}}, \mathcal{Z})$
- Compute $\text{JI} = \mathcal{L}\text{-}\ \mathcal{Q}_{\text{p}}.\ h_2(\text{Cert}_{\text{p}} \| \text{ID}_{\text{p}}, m_{\mathcal{W}}, \mathcal{Z})$
- Send the tuple $\Psi = (m_{\mathcal{W}}, \mathcal{Z}, \text{JI})$ to the proxy using an insecure channel

GPS: after receiving $\Psi = (m_{\mathcal{W}}, \mathcal{Z}, \text{JI})$ from the patient, a GPS algorithm is processed by the proxy (agent) to produce a proxy signcryption tuple $\psi = (Q, \mathcal{C}, \mathcal{S})$ of the message (m) and send it through insecure channels to the receiver (Smart Pharmacy). This algorithm takes as input the public and private key of the agent ($\mathcal{J}_{\text{a}}$,$_{\text{a}}$), patient and receiver identities (ID_{a},ID_{sp}), certificate of agent (Cert_{a}), certificate of smart pharmacy (Cert_{sp}), public key of smart pharmacy ($\mathcal{J}_{\text{sp}}$), and message (m). The following steps denote the proxy signcryption generation process.

- The proxy first verifies $\mathcal{Z} \stackrel{?}{=} \text{JI}.\ \mathcal{D} + \mathcal{J}_{\text{p}}.\ h_2(\text{Cert}_{\text{p}} \| \text{ID}_{\text{p}}, m_{\mathcal{W}}, \mathcal{Z})$
- Also, it verifies $\mathcal{J}_{\text{sp}} \stackrel{?}{=} h_2(\text{Cert}_{\text{sp}} \| \text{ID}_{\text{sp}}) \text{Cert}_{\text{sp}} + m p\hbar$
- Select a random number $x \in \{1, 2, \ldots\ldots, p-1\}$
- Select a nonce Nonce_{a}

TABLE 2. Symbols of the proposed scheme.

S.NO	Symbol	Descriptions
1	$\mathbb{hEc}$ - $\mathbb{D}$-$\mathbb{LP}$	Hyper elliptic curve discrete logarithm problem
2	$\mathbb{hEc}$	Hyper elliptic curve
3	$\mathcal{G}$	Genus of Hyper elliptic curve
4	$J_{\mathbb{hEc}}(\mathcal{U}_p)$	Jacobian group on $\mathbb{hEc}$
5	$\mathcal{O}(J_{\mathbb{hEc}}(\mathcal{U}_p))$	Order of Jacobian group
6	$\mathcal{D}$	Divisor on $\mathbb{hEc}$
7	$\mathcal{y}$	Input security parameter selected from $\mathbb{hEc}$
8	$\mathcal{msk}$, $\mathcal{mpk}$	Master secret and public key of CA
9	ID_a, ID_p, ID_{sp}	Identities of Agent, Patient, and Smart Pharmacy
10	$\mathcal{X}_a$, $\mathcal{X}_p$, $\mathcal{X}_{sp}$	Public variants of Agent, Patient, and Smart Pharmacy
11	$Cert_a$, $Cert_p$, $Cert_{sp}$	Certificates for Agent, Patient, and Smart Pharmacy
12	$\mathcal{N}_a$, $\mathcal{N}_p$, $\mathcal{N}_{sp}$	Auxiliary variables for Agent, Patient, and Smart Pharmacy
13	$\mathcal{J}_a$, $\mathcal{J}_p$, $\mathcal{J}_{sp}$	Public keys of Agent, Patient, and Smart Pharmacy
14	$\mathcal{Q}_a$, $\mathcal{Q}_p$, $\mathcal{Q}_{sp}$	Private keys of Agent, Patient, and Smart Pharmacy
14	h_1, h_2,h_3	One-way hash functions
15	$\mathcal{E}_K$/ $\mathcal{D}_K$	Encryption and Decryption functions
16	$\mathcal{m}$/$\mathcal{C}$	Plain text and Ciphertext
17	$\|$	Used for concatenations
18	$Nonce_a$, Nsp	Fresh nonce of Agent and Smart Pharmacy

- Compute $Q = x.\mathcal{D}$ and secret key $K = x.\mathcal{J}_{sp}$
- Encrypt message $\mathcal{C} = \mathcal{E}_K(\mathcal{m} \| Nonce_a)$
- Generate a hash value $\mathcal{r} = h_3(\mathcal{m} \| Nonce_a)$
- Compute signature $\mathcal{S} = x\text{-}\mathcal{r}.\mathcal{Q}_a$
- Send a tuple $\psi = (Q, \mathcal{C}, \mathcal{S}, \mathcal{r})$ to the receiver (smart pharmacy) using an insecure channel
- VU: After receiving a proxy signcryption tuple $\psi = (Q, \mathcal{C}, \mathcal{S}, \mathcal{r})$ from an agent, a VU algorithm is processed by the receiver (smart pharmacy) to verify and decrypt the proxy signcryption tuple $\psi = (Q, \mathcal{C}, \mathcal{S}, \mathcal{r})$ of the message $(\mathcal{m})$. This algorithm takes as input the public and private key of smart pharmacy $(\mathcal{J}_{sp}, \mathcal{Q}_{sp})$, agent and smart pharmacy identities (ID_a, ID_{sp}), certificate of agent $(Cert_a)$, the public key of agent $(\mathcal{J}_a)$, and proxy signcryption tuple $\psi = (Q, \mathcal{C}, \mathcal{S}, \mathcal{r})$. The following steps describe the verification and decryption process.Select a fresh nonce Nsp
- First, verify $\mathcal{J}_a \stackrel{?}{=} h_2(Cert_a \| ID_a)Cert_a + \mathcal{mpk}$
- Compute $Q = \mathcal{S}.\mathcal{D} + \mathcal{r}.\mathcal{J}_a$
- Generate the secret key $K = Q.\mathcal{Q}_{sp}$
- Decrypt the cipher text $(\mathcal{m} \| Nonce_a) = \mathcal{D}_K(\mathcal{C})$
- Compute $\mathcal{r}^* = h_3(\mathcal{m} \| Nonce_a)$ and verify $\mathcal{r}^* \stackrel{?}{=} \mathcal{r}$ accept or otherwise reject it.

B. SCHEMES CORRECTNESS

The proxy verifies the public key of receiver from the following steps [8], if the public key of the receiver is successfully derived then it further generates the proxy signcryption.

$$\begin{aligned}
\mathcal{J}_{sp} &= (h_1(Cert_{sp} \| ID_{sp})Cert_{sp} + \mathcal{mpk}) = \mathcal{J}_{sp} = \mathcal{Q}_{sp}.\mathcal{D} \\
&= (h_1(Cert_{sp} \| ID_{sp})\beta_{sp} + \mathcal{N}_{sp}).\mathcal{D} = (h_1(Cert_{sp} \| ID_{sp})\beta_{sp} \\
&\quad + h_1(Cert_{sp} \| ID_{sp})\vartheta + \mathcal{msk}).\mathcal{D} \\
&= (h_1(Cert_{sp} \| ID_{sp})\beta_{sp}.\mathcal{D} \\
&\quad + h_1(Cert_{sp} \| ID_{sp})\vartheta_{sp}.\mathcal{D} + \mathcal{msk}.\mathcal{D}) \\
&= (h_1(Cert_{sp} \| ID_{sp})\mathcal{X}_{sp} + h_1(Cert_{sp} \| ID_{sp})\mathcal{Y}_{sp} + \mathcal{mpk}) \\
&= (h_1(Cert_{sp} \| ID_{sp})\mathcal{X}_{sp} + \mathcal{Y}_{sp} + \mathcal{mpk}) \\
&= (h_1(Cert_{sp} \| ID_{sp})Cert_{sp} + \mathcal{mpk})
\end{aligned}$$

The receiver verifies the public key of proxy from the following steps [8], if the public key of the receiver is successfully derived then it further generate verify and decrypt signcryption tuple.

$$\begin{aligned}
\mathcal{J}_a &= (h_1(_a \| ID_a)Cert_a + \mathcal{mpk}) = \mathcal{J}_a \\
&= \mathcal{Q}_a.\mathcal{D} = (h_1(Cert_a \| ID_a)\beta_a + \mathcal{N}_a).\mathcal{D} \\
&= (h_1(Cert_a \| ID_a)\beta_a + h_1(Cert_a \| ID_a)\vartheta + \mathcal{msk}).\mathcal{D} \\
&= (h_1(Cert_a \| ID_a)\beta_a.\mathcal{D} + h_1(Cert_a \| ID_a)\vartheta_a.\mathcal{D} + \mathcal{msk}.\mathcal{D}) \\
&= (h_1(Cert_a \| ID_a)\mathcal{X}_a + h_1(Cert_a \| ID_a)\mathcal{Y}_a + \mathcal{mpk}) \\
&= (h_1(Cert_{sp} \| ID_{sp})\mathcal{X}_{sp} + \mathcal{Y}_{sp} + \mathcal{mpk}) \\
&= (h_1(Cert_a \| ID_a)Cert_a + \mathcal{mpk})
\end{aligned}$$

The agent can verify the delegation tuple $\Psi = (\mathcal{m}_{\mathcal{W}}, \mathcal{Z}, \mathcal{JI})$ using the following computations.

$$\begin{aligned}
\mathcal{Z} &\stackrel{?}{=} \mathcal{JI}.\mathcal{D} + \mathcal{J}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&= \mathcal{JI}.\mathcal{D} + \mathcal{J}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&= (\mathcal{L} - \mathcal{Q}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z})).\mathcal{D} \\
&\quad + \mathcal{J}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&= (\mathcal{L} - \mathcal{Q}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z})).\mathcal{D} \\
&\quad + \mathcal{Q}_p.\mathcal{D} - h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&= \mathcal{D}(\mathcal{L} - \mathcal{Q}_p.h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&\quad + \mathcal{Q}_{p.}, h_2(Cert_p \| ID_p, \mathcal{m}_{\mathcal{W}}, \mathcal{Z}) \\
&= \mathcal{D}(\mathcal{L}) = \mathcal{L}.\mathcal{D} = \mathcal{Z}
\end{aligned}$$

The smart pharmacy can easily recover the secret key by performing the following steps.

$$\begin{aligned}
K &= Q.\mathcal{Q}_{sp} \\
&= Q.\mathcal{Q}_{sp} = (\mathcal{S}.\mathcal{D} + \mathcal{r}.\mathcal{J}_a)\mathcal{Q}_{sp} \\
&= ((x - \mathcal{r}.\mathcal{Q}_a).\mathcal{D} + \mathcal{r}.(\mathcal{Q}_a.\mathcal{D})\mathcal{Q}_{sp} \\
&= (\mathcal{D}(x - \mathcal{r}.\mathcal{Q}_a + \mathcal{r}.\mathcal{Q}_a))\mathcal{Q}_{sp} = (\mathcal{D}.x)\mathcal{Q}_{sp} \\
&= (\mathcal{Q}_{sp}.\mathcal{D}.x) = (\mathcal{J}_{sp}.x) = (x.\mathcal{J}_{sp}) = K
\end{aligned}$$

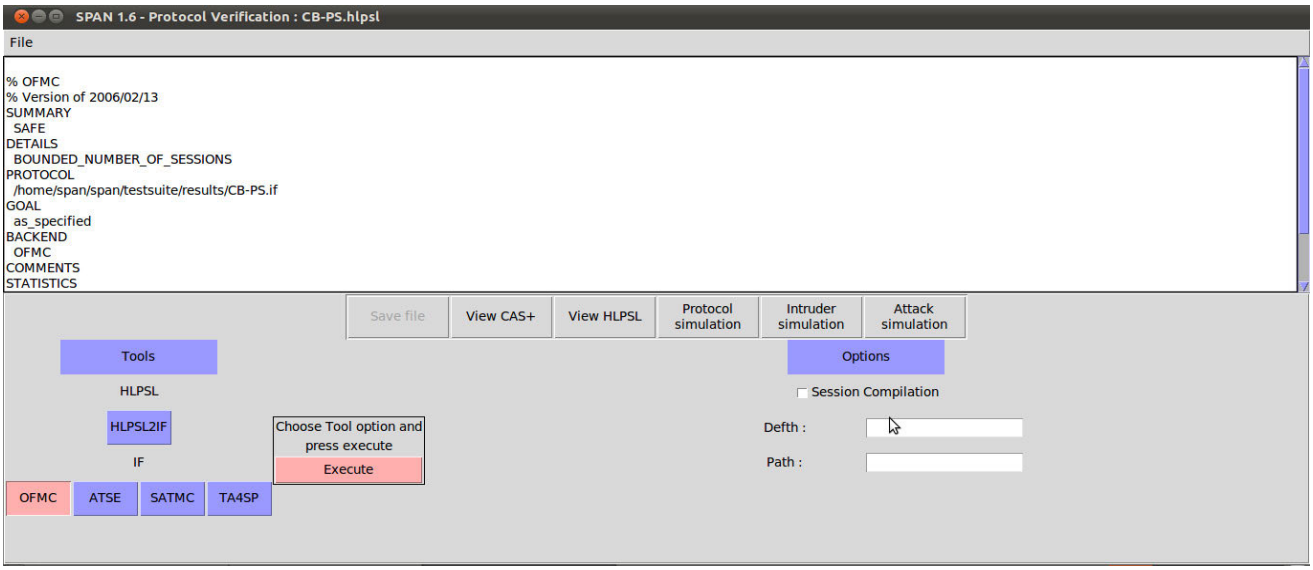

FIGURE 3. OFMC simulations.

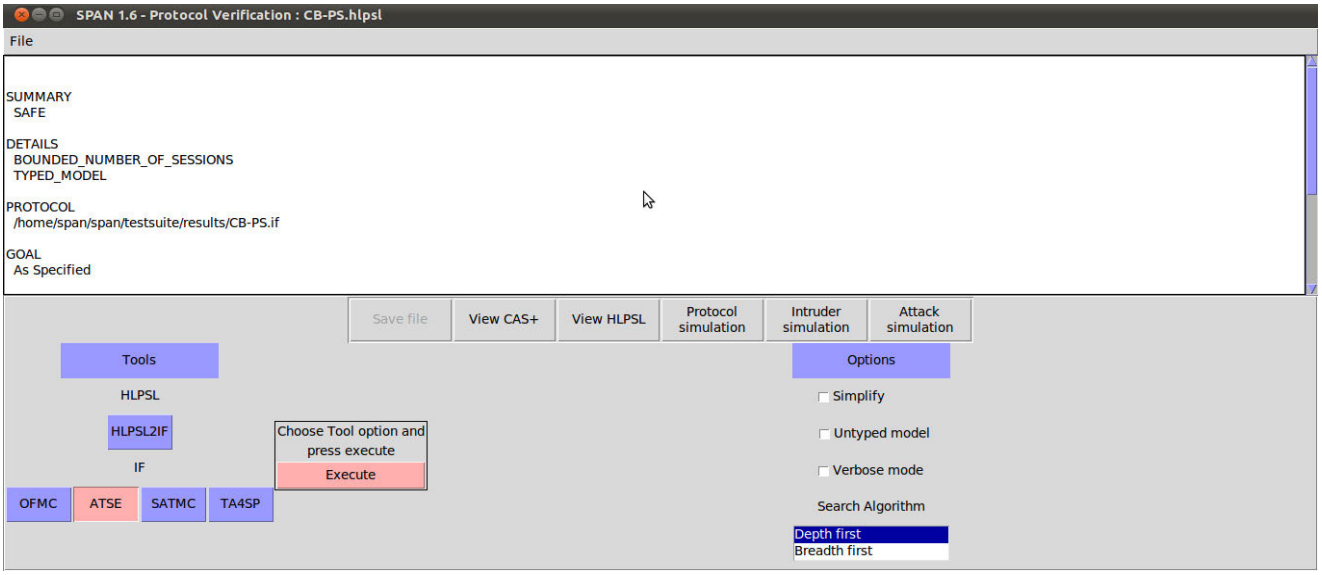

FIGURE 4. ATSE simulations.

VI. IMPLEMENTATION AND VALIDATION

This phase presents the implementation and validation of the proposed CB-PS scheme in the AVISPA tool. First, we generate the HLPSL code for our proposed CB-PS algorithm. Then, we check this code under the functionality of two embedded back-ends of AVISPA, i.e. OFMC and ATSE. We check our scheme 100 times, and it still gives the SAFE result under the OFMC and ATSE backend as shown in Figure 3 and 4. We performed this experiment using the hardware's resources such as Haier Win8.1 PC, Intel (R) Core (TM) i3-4010U CPU @ 1.70 GHz, supporting a 64-bit operating system, and x64-based processor. Also, the software's resources such as Oracle VM Virtual Box (version: 5.2.0.118431) and SPAN (version: SPAN-Ubuntu-10.10-light_1) are used. The HLPSL code of our CB-PS algorithm consists of five roles: role_Patient, role_Agent, role_Smart pharmacy, role session, and role environment.

In Table 3, we provide the HLPSL code for the patient role, and then we explain some of the symbols of this role. The symbol used before the arrow represents the symbol used in HLPSL, and the symbol after the arrow shows the symbol used in the CB-PS algorithm. Therefore, Noncea $\Rightarrow$ Nonce_a, Min,H1$\Rightarrow$ -, h_1, Idp $\Rightarrow$ ID_p, Certp $\Rightarrow$ Cert_p, Mw $\Rightarrow$ $m_{\mathcal{W}}$, L $\Rightarrow$ $\mathscr{L}$, Jp $\Rightarrow$ $\mathcal{J}_\text{p}$, and inv(Jp) $\Rightarrow$ $\mathcal{Q}_\text{p}$. In Table 4, we provide the HLPSL code for the Agent role, and then we clarify the symbol used in this role. So, X $\Rightarrow$ x, H3 $\Rightarrow$ h_3, M $\Rightarrow$ m, Nsp $\Rightarrow$ Nsp, E $\Rightarrow$ $\mathcal{E}$, K $\Rightarrow$ K, Ja $\Rightarrow$ $\mathcal{J}_\text{a}$, and inv(Ja) $\Rightarrow$ $\mathcal{Q}_a$. In Table 5, we provide the HLPSL code for the Smart Pharmacy role. The symbol of this role has already been explained above. At the end of this phase, we present

TABLE 3. HLPSL code for patient.

HLPSL CODE FOR PATIENT Role
role role_Patient(Agent:agent,Patient:agent, Smartpharmacy:agent,Ja:public_key,Jp:public_key, Jsp:public_key,SND,RCV:channel(dy)) played_by Patient def= local State:nat,Noncea:text,Min:hash_func, H1:hash_func,Idp:text,L:text,Certp:text,Mw:text init State := 0 transition 1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Patient.Agent) 2. State=1 /\ RCV(Agent.{Noncea'}_Jp) =|> State':=2 /\ Mw':=new() /\ secret(Mw',sec_2,{Patient}) /\ witness(Patient,Agent,auth_1,Mw') /\ Idp':=new() /\ Certp':=new() /\ L':=new() /\ SND(Patient.{Min(L').H1(L'.Certp'.Idp'.Mw')}_inv(Jp)) end role

TABLE 4. HLPSL code for agent role.

HLPSL CODE FOR AGENT Role
role role_Agent(Agent:agent,Patient:agent,Smartpharmacy:agent,Ja:public_key,Jp:public_key,Jsp:public_key,SND,RCV:channel(dy)) played_by Agent def= local State:nat,Noncea:text,H1:hash_func,Idp:text,L:text,Certp:text,Mw:text,X:text,Min:hash_func,H3:hash_func,M:text,Nsp:text,E:hash_func,K:symmetric_key init State := 0 transition 1. State=0 /\ RCV(Patient.Agent) =|> State':=1 /\ Noncea':=new() /\ SND(Agent.{Noncea'}_Jp) 3. State=1 /\ RCV(Patient.{Min(L').H1(L'.Certp'.Idp'.Mw')}_inv(Jp)) =|> State':=2 /\ request(Agent,Patient,auth_1,Mw') /\ secret(Mw',sec_2,{Patient}) /\ Nsp':=new() /\ M':=new() /\ secret(M',sec_4,{Smartpharmacy}) /\ witness(Agent,Smartpharmacy,auth_3,M') /\ X':=new() /\ K':=new() /\ SND(Agent.{E(M'.Nsp')}_K'.{Min(X').H3(M'.Nsp')}_inv(Ja)) end role

the results of the proposed CB-PS scheme in Figure 3 and 4. The results clearly show that our scheme gives a SAFE result under the two backends, i.e. OFMC and ATSE.

VII. SECURITY ANALYSIS

Our CB-PS meets the following security properties.

A. WARRANT UNFORGEABILITY

This means that an unauthorized participant (UP) cannot produce a falsified warrant signature that is similar to an original warrant signature, which is prepared by the real participant. Our CB-PS allows the user (patient) to generate a digital signature $\mathrm{JI} = \mathscr{L}\text{-}\ \mathcal{Q}_{\mathrm{p}}.\ h_2(\mathrm{Cert_p} \| \mathrm{ID_p}, m_{\mathcal{W}}, \mathcal{Z})$ by using his private key $\mathcal{Q}_{\mathrm{p}}$ and a randomly generated number $\mathscr{L}$ of a warrant message $m_{\mathcal{W}}$. If the UP tries to make a fake signature, then it is essential for the UP to get $\mathcal{Q}_{\mathrm{p}}$ from equation (4) and $\mathscr{L}$ from equation (5). The UP cannot produce the $\mathcal{Q}_{\mathrm{p}}$ and $\mathscr{L}$ because it is difficult and to solve the $\mathbb{hEc}$ - $\mathbb{D}$-$\mathbb{LP}$. So, from the above assumptions, we can conclude that our CB-PS ensures the unforgeability of a signature.

$$\mathcal{J}_{\mathrm{p}} = \mathcal{Q}_{\mathrm{p}}.\mathcal{D}, \tag{4}$$

$$\mathcal{Z} = \mathscr{L}.\mathcal{D}, \tag{5}$$

B. CONFIDENTIALITY

Protecting the actual content of a message from an unauthorized participant (UP) is called confidentiality. Our CB-PS

TABLE 5. HLPSL code for smart pharmacy role.

```
HLPSL CODE FOR Smart Pharmacy Role
role
role_Smartpharmacy(Agent:agent,Patient:agent,Smartpharmacy:agent,Ja:public_key,Jp:public_key,Jsp:public_key,SND,RCV:channel(dy))
played_by Smartpharmacy
def=
        local
                State:nat,X:text,Min:hash_func,H3:hash_func,M:text,Nsp:text,E:hash_func,K:symmetric_key
        init
                State := 0
        transition
                6. State=0 /\ RCV(Agent.{E(M'.Nsp')}_K'.{Min(X').H3(M'.Nsp')}_inv(Jp)) =|> State':=1 /\ secret(M',sec_4,{Smartpharmacy})
end role
```

enables the agent to generate a cipher text $\mathcal{C} = \mathcal{E}_K(m \| \text{Nonc}_a)$ of a message using the secret key K. If the UP tries to see the actual content of a message, then it is important for the UP to acquire the secret key K first. The UP can get the secret key K through methods described in the following cases.

Case 1: The UP can easily get the secret key K if he solves equation (6). In this process, the UP needs the randomly generated number x, which can be gotten from equation (7). So, the UP cannot get the number x from equation (7) because it is hard to solve and equal to solving the hyper elliptic curve discrete logrithm problem.

$$K = x.\mathcal{J}_{\text{sp}}, \tag{6}$$

$$Q = x.\mathcal{D}, \tag{7}$$

Case 2: The UP can also develop a secret key K if he computes equation (8). This process needs the private key $\mathcal{Q}_{\text{sp}}$ of a smart pharmacy from equation (8). Therefore, it is also hard and infeasible for the UP to get the smart pharmacy private key $\mathcal{Q}_{\text{sp}}$ from equation (9) because it is equal to solving the hyper elliptic curve discrete logrithm problem.

$$K = Q.\mathcal{Q}_{\text{sp}}, \tag{8}$$

$$\mathcal{J}_{\mathcal{U}} = \mathcal{Q}_{\text{sp}}.\mathcal{D}, \tag{9}$$

From the above discussion, we can claim that our CB-PS resists against confidentiality attack.

C. INTEGRITY

If the UP cannot alter the original message, it is called the integrity of the message. Our CB-PS permits the proxy (agent) to generate the irretrievable hash function $\mathcal{r} = h_3(m \| \text{Nonce}_a)$ of a message m before transmission. If the UP wants to alter the message m like m^*, then it is necessary for $\mathcal{C}$ to convert it to $\mathcal{C}^*$. Then, the hash value of m^* will be $\mathcal{r}^* = h_3(m^* \| \text{Nonce}_a)$, so it is not possible for the UP to generate the same hash value for two different values because of the collision resistance property of the hash function.

D. UNFORGEABILITY

This means that the UP Cannot produce a falsified signature that is similar to an original signature of actual participant made by the actual participant. Our CB-PS facilitates the proxy (agent) to generate a digital signature $\mathcal{S} = x\text{-}\mathcal{r}.\mathcal{Q}_a$ by using his private key $\mathcal{Q}_a$ and the randomly chosen number x. If the UP tries to make a forged signature, then it is necessary for the UP to get $\mathcal{Q}_a$ from equation (10) and x from equation (7). In this case, the UP cannot generate $\mathcal{Q}_a$ and x because it is difficult and is equal to computing the $\mathbb{hEc}$ - $\mathbb{D}$-$\mathbb{LP}$. So, from the above assumptions, we can conclude that our CB-PS ensures the unforgeability of a signature.

$$\mathcal{J}_{\text{a}} = \mathcal{Q}_{\text{a}}.\mathcal{D}, \tag{10}$$

E. FORWARD SECRECY

In this case, if the UP obtains the private key of the user, then the cipher text is still confidential, which is called Forward Secrecy. In our CB-PS, the encryption and decryption of message m are done through the secret key K, not through the private key of agent $\mathcal{Q}_{\text{a}}$. So, if the private key $\mathcal{Q}_{\text{a}}$ of an agent is compromised, then the cipher text $\mathcal{C}$ is still secure because it is encrypted through the secret key K. In this regard, our CB-PS ensures the forward secrecy property.

F. RESISTS REPLAY ATTACK

This means that the UP cannot send the older messages to the recipient again and again. Our CB-PS facilitates the proxy (agent) to send a fresh nonce Nonce_a within the cipher text $\mathcal{C} = \mathcal{E}_K(m \| \text{Nonce}_a)$. This nonce will be renewed in every session and sent along with the message or within the cipher text. In this regard, we can say that our CB-PS ensures the resists replay attack property.

G. EFFICIENCY

In this phase, we compare our CB-PS with the existing related schemes TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37] on the basis of three major parameters:

TABLE 6. Comparisons on the basis of security.

Schemes	Security Requirement							
	WUF	CON	INT	UF	FR	RRA	rom	VTAT
TBKAV [1]	✓	✓	✓	✓	⛶	×	✓	×
LXKXD [2]	✓	✓	✓	×	⛶	×	✓	×
CYL [38]	✓	✓	✓	✓	⛶	×	✓	×
HZJX [39]	✓	✓	✓	✓	⛶	×	✓	×
QTLG [37]	✓	✓	✓	✓	✓	×	×	×
Our CB-PS	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 7. Computational cost comparisons on the basis of major operations.

Schemes	Involves participants			
	Generate Delegation (GD)	**Generate Proxy Signcryption (GPS)**	**Verification and Unsigncryption (VU)**	**Total**
TBKAV [1]	2 ESM	5 ESM	4 ESM	11 ESM
LXKXD [2]	2 ESM	7 ESM	5 ESM	14 ESM
CYL [38]	3 PBM	2P + 1PBM	P+ 3PBM +E	3P+ 7PBM +E
HZJX [39]	2P+ 2PBM +E	P+ 3PBM +E	4P+ PBM +E	7P+ 6PBM +3E
QTLG [37]	-	5 ESM	10 ESM	15 ESM
Our CB-PS	2 HEM	6 HEM	4 HEM	12 HEM

security, computational cost, and communication overhead. The following are illustrations of the claimed performance parameters.

1) SECURITY

In Table 6, we explain the comparisons regarding the security requirement among proposed CB-PS and TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37]. The symbol × is used to obey the security requirement, the symbol *imes* is used for not satisfying the security property, and the symbol ⛶ for not mentioning the security property. Further, WUF, CON, INT, UF, FR, RRA, rom, and VTAT represents warrant unforgeability, confidentiality, integrity, unforgeability, forward secrecy, resists replay attack, random oracle model, and validation through the AVISPA tool, respectively. The schemes TBKAV [1], LXKXD [2], CYL [38], and HZJX [39] do not satisfy the security properties of FR, RRA, and the security requirements are proven using rom, which is not practical in a real scenario. The scheme QTLG [37] does not satisfy RRA property. In contrast to TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37], our CB-PS satisfies all the claimed security properties, as shown in Table 6. These security requirements are validated through the AVISPA tool.

2) COMPUTATIONAL COST

In Table 7, we give the computational cost comparison among our designed CB-PS and the existing ones, i.e. TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37] on the basis of major operations. We consider the major operation, i.e., bilinear pairing, pairing based scalar multiplication, exponential, hyper elliptic divisor multiplication and elliptic curve scalar multiplication in the proposed CB-PS and in TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37]. Further, P, PBM, E, HEM and ESM signify one pairing operation, one pairing based scalar multiplication operation, one exponential operation, one hyper elliptic curve divisor multiplication operation, and one elliptic curve scalar multiplication operation, respectively. Additionally, we create comparisons among the proposed CB-PS and TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37] on the basis of milliseconds (ms), which is shown in Table 8. We observed from [44] that the single ESM consumes 0.97 ms, P needs 14.90 ms, PBM consumes 4.31 ms, E needs 1.97 ms, and it is also assumed that HEM earnings consume 0.48 ms [8]. Our proposed CB-PS is $10.67 - 5.76 / 10.67*100 = 46.01\%$ quicker than TBKAV [1], $13.58 - 5.76 / 13.58*100 = 57.58\%$ quicker than LXKXD [2], $76.84 - 5.76 / 76.84*100 = 92.50\%$ quicker than CYL [38], $136.07 - 5.76 / 136.07 *100 = 95.76\%$ quicker than HZJX [39], and $14.55 - 5.76 / 14.55 *100 = 60.41\%$ quicker than QTLG [37].Further, in Figure 5, we provide a clear reduction of the computational cost of the proposed CB-PS from TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37].

3) COMMUNICATION OVERHEAD

Sending additional bits along with the actual cipher text is called communication overhead. If the additional bits are smaller in size, then the communication will be fast; otherwise, delays will occur in communications. In this phase, we compare our designed CB-PS with existing ones, i.e. TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37] on the basis of communication overhead. To make

TABLE 8. Computational cost comparisons on the basis of ms.

Schemes	Involves participants			
	Generate Delegation (GD)	**Generate Proxy Signcryption (GPS)**	**Verification and Unsigncryption (VU)**	**Total**
TBKAV [1]	1.8 ms	4.85 ms	3.88 ms	10.67 ms
LXKXD [2]	1.8 ms	6.97ms	4.85 ms	13.58 ms
CYL [38]	12.93ms	34.11ms	29.8 ms	76.84 ms
HZJX [39]	40.39ms	29.8ms	65.88 ms	136.07 ms
QTLG [37]	-	4.85ms	9.70 ms	14.55 ms
Our CB-PS	0.97 ms	2.88 ms	1.92 ms	5.76 ms

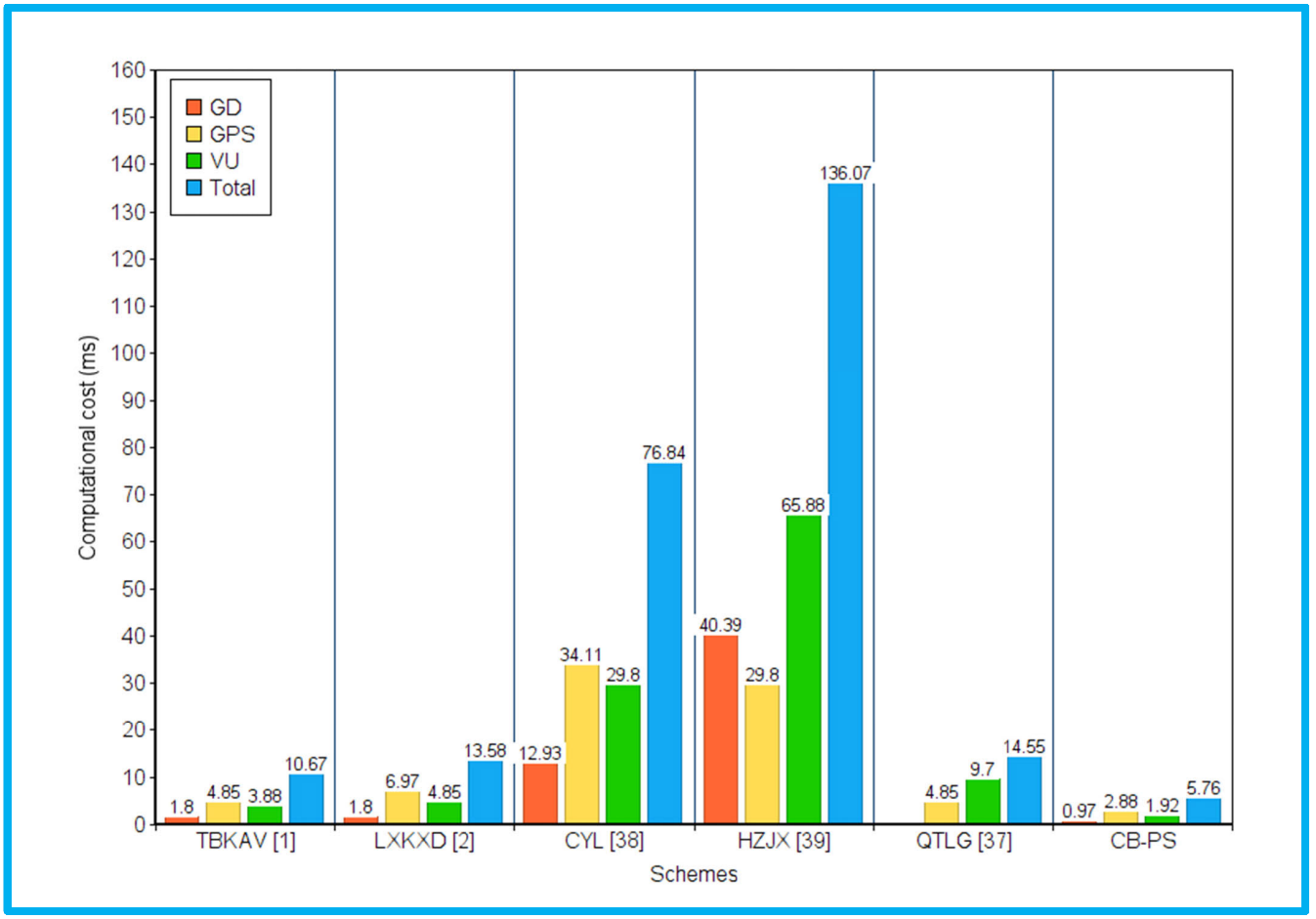

FIGURE 5. Computational cost comparison.

these comparisons, we suppose that $|H| \cong |\text{ID}| \cong |q| \cong 2^{160}$ bits, $|h| \cong |\text{ID}| \cong |p| \cong 2^{80}$ bits, $|\text{G}|$, and $|m_{\mathcal{W}}| \cong |m| \cong 1024$ bits. The communication overhead for the scheme TBKAV [1] is $2|m_{\mathcal{W}}| + |m| + 4|\text{ID}| + 11|q| = 2|1024| + |1024| + 4|160| + 11|160| = 5472$ bits, for the scheme LXKXD [2] it is $2|m_{\mathcal{W}}| + |m| + 6|\text{ID}| + 10|q| = 2|1024|+|1024|+6|160|+10|160| = 5632$ bits, for CYL [38] it is $2|m_{\mathcal{W}}| + |m| + 4|\text{G}| = 2|1024| + |1024| + 4|1024| = 7168$ bits, for HZJX [39] it is $2|m_{\mathcal{W}}| + |m| + 5|\text{G}| = 2|1024| + |1024| + 4|1024| = 8192$ bits, for QTLG [37] it is $2|m_{\mathcal{W}}| + |m| + 4|\text{ID}| + 12|q| = 2|1024| + |1024| + 4|80| + 12|160| = 5312$ bits, and for our proposed CB-PS it is $|m_{\mathcal{W}}|+|m|+|h|+4|p| = |1024|+|1024|+|80|+4|80| = 2448$ bits.

- Our designed CB-PS is $5472- 2448/ 5472 = 55.26\%$ fasters than TBKAV [1]
- $5632- 2448/ 5632 = 56.53\%$ fasters than LXKXD [2]
- $7168- 2448/ 7168 = 65.84\%$ fasters than CYL [38]
- $8192- 2448/ 8192 = 70.11\%$ fasters than HZJX [39]
- $5312- 2448/ 5312 = 53.91\%$ fasters than QTLG [37]

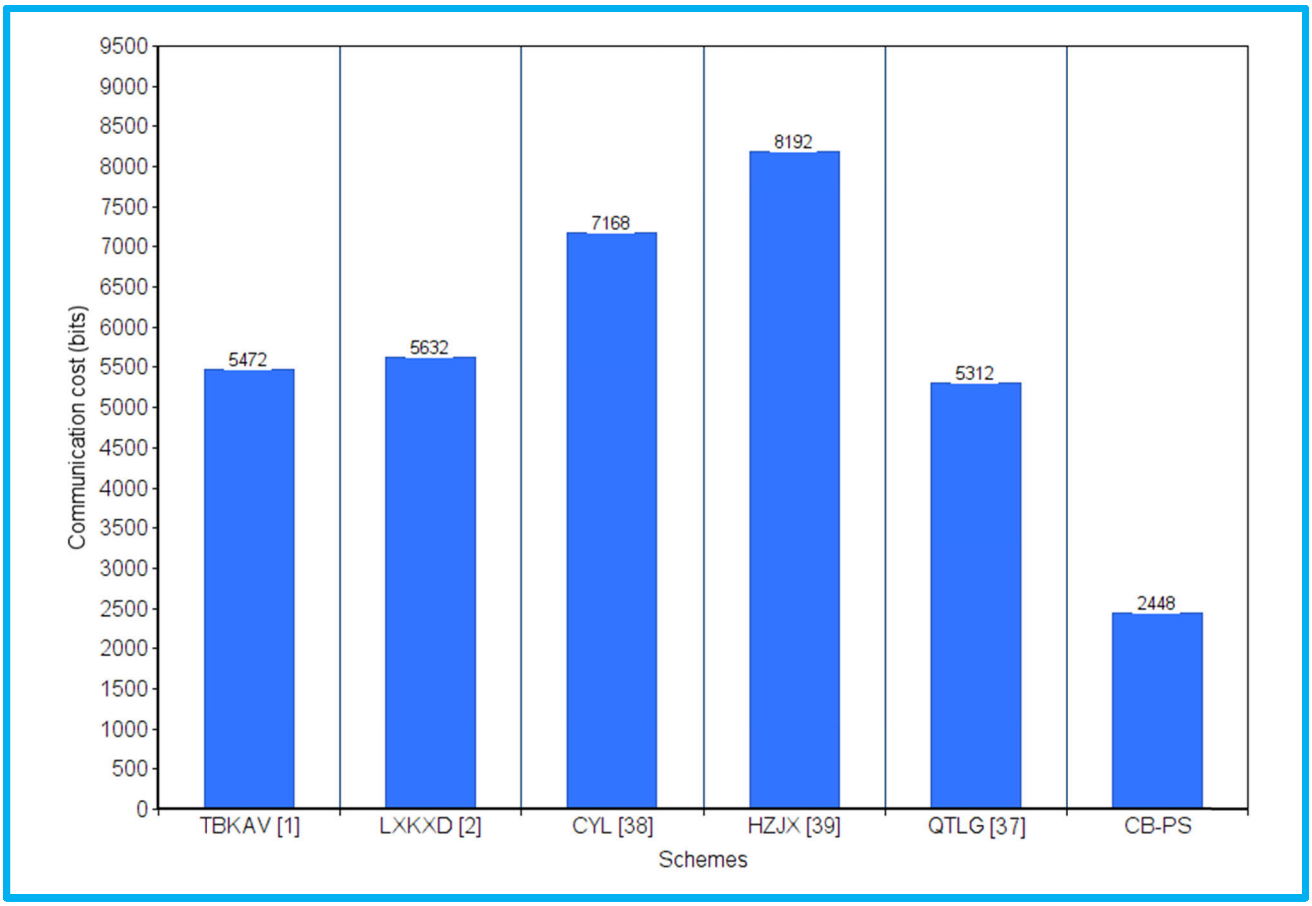

FIGURE 6. Communication cost comparison.

Additionally, in Figure 6, we show a pure decrease of the communication cost of the proposed CB-PS from TBKAV [1], LXKXD [2], CYL [38], HZJX [39], and QTLG [37].

VIII. CONCLUSION

E-prescription systems involve the computer-based electronic generation, transmission, and filling of a medical prescription that allows health practitioners (doctors, physicians, pharmacists, or nurses) to electronically transmit prescriptions to pharmacies. However, due to stringent legal requirements and privacy regulations, two major security concerns i.e. confidentiality and authentication need to be addressed. In general, the answer to ensuring confidentiality and authentication lies in the combination of both the encryption and digital signature functions in a single logic step called signcryption. Therefore, in this article, we presented a lightweight and provable secured certificate-based proxy signcryption (CB-PS) scheme for E-prescription systems. The proposed scheme is based on hyperelliptic curve, an advanced version of elliptic curve characterized by a small parameter and key size (80 bits) as compared to elliptic curve, in which the key size is 160 bits. A security analysis, including formal security verification, is performed using the widely recognized AVISPA tool, and in the findings our proposed scheme shows significant immunity against adversary attacks. To further complement these superiorities of our model, the presented scheme is also far more efficient in terms of computational and communication cost compared to the relevant existing schemes.

REFERENCES

[1] T. Bhatia and A. K. Verma, "Cryptanalysis and improvement of certificateless proxy signcryption scheme for e-prescription system in mobile cloud computing," *Ann. Telecommun.*, vol. 72, nos. 9–10, pp. 563–576, Oct. 2017.

[2] L. Li, S. Zhou, K.-K.-R. Choo, X. Li, and D. He, "An efficient and provably-secure certificateless proxy-signcryption scheme for electronic prescription system," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Aug. 2018.

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

[4] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in *Proc. 3rd ACM Conf. Comput. Commun. Secur. (CCS)*, 1996, pp. 48–57.

[5] C. Gamage, J. Leiwo, and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," in *Proc. 22nd Australas. Comput. Sci. Conf.*, 1999, pp. 420–431.

[6] C. Zhou, G. Gao, Z. Cui, and Z. Zhao, "Certificate-based generalized ring signcryption scheme," *Int. J. Found. Comput. Sci.*, vol. 29, no. 6, pp. 1063–1088, Sep. 2018, doi: 10.1142/s0129054118500211.

[7] A. Karati, C.-I. Fan, and R.-H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10431–10440, Dec. 2019, doi: 10.1109/jiot.2019.2939204.

[8] I. Ullah, A. Alomari, N. U. Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things," *Electronics*, vol. 8, no. 10, p. 1171, Oct. 2019.

[9] A. Braeken, "Pairing free certificate based signcryption schemes using ECQV implicit certificates," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 3, pp. 1546–1565, 2019.

[10] I. Ullah, N. Amin, J. Khan, M. Rehan, M. Naeem, H. Khattak, S. Khattak, and H. Ali, "A novel provable secured signcryption scheme PSSS: A hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, Jul. 2019.

[11] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, pp. 1–16, Jan. 2019.

[12] I. Ullah, N. U. 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.

[13] V. S. Naresh, R. Sivaranjani, and N. Murthy, "Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks," *Int. J. Commun. Syst.*, vol. 31, no. 15, p. e3763, 2018, doi: 10.1002/dac.3763.

[14] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *Int. J. Adv. Stud. Sci. Res.*, vol. 3, p. 5, Jan. 2019. [Online]. Available: https://ssrn.com/abstract=3315286

[15] S. Ullah, X.-Y. Li, and L. Zhang, "A review of signcryption schemes based on hyper elliptic curve," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, p. 10, doi: 10.1109/bigcom.2017.51.

[16] S. Ullah, M. Junaid, F. Habib, Sana, Insafullah, and Hizbullah, "A novel proxy blind signcryption scheme based on hyper elliptic curve," in *Proc. 12th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Aug. 2016, p. 10, doi: 10.1109/fskd.2016.7603481.

[17] I. Ullah, I. U. Haq, N. U. Amin, A. I. Umar, and H. Khattak, "Proxy signcrypion scheme based on hyper elliptic curves," *Int. J. Comput.*, vol. 20, no. 1, pp. 157–166, 2016.

[18] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain," *J. Inf. Secur. Appl.*, vol. 45, pp. 156–175, Apr. 2019, doi: 10.1016/j.jisa.2019.02.003.

[19] J. Cao, H. Li, M. Ma, and F. Li, "UPPGHA: Uniform privacy preservation group handover authentication mechanism for mMTC in LTE-A networks," *Secur. Commun. Netw.*, vol. 2018, pp. 1–16, Feb. 2018, doi: 10.1155/2018/6854612.

[20] P. K. Dhillon and S. Kalra, "A secure multi-factor ECC based authentication scheme for cloud-IoT based healthcare services," *J. Ambient Intell. Smart Environ.*, vol. 11, no. 2, pp. 149–164, Mar. 2019, doi: 10.3233/ais-190516.

[21] S. Yu, J. Lee, K. Lee, K. Park, and Y. Park, "Secure authentication protocol for wireless sensor networks in vehicular communications," *Sensors*, vol. 18, no. 10, p. 3191, Sep. 2018.

[22] M. S. Raniyal, I. Woungang, S. K. Dhurandher, and S. S. Ahmed, "Passphrase protected device-to-device mutual authentication schemes for smart homes," *Secur. Privacy*, vol. 1, no. 3, p. e42, 2018, doi: 10.1002/spy2.42.

[23] K. Pak, S. Pak, C. Ho, M. Pak, and C. Hwang, "Anonymity preserving and round effective three-party authentication key exchange protocol based on chaotic maps," *PLoS ONE*, vol. 14, no. 3, Mar. 2019, Art. no. e0213976.

[24] S. Qiu, G. Xu, H. Ahmad, and Y. Guo, "An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy," *PLoS ONE*, vol. 13, no. 3, Mar. 2018, Art. no. e0194072, doi: 10.1371/journal.pone.0194072.

[25] M. Ouaissa and A. Rhattoy "A secure model for machine to machine device domain based group in a smart city architecture," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 1, pp. 151–164, Feb. 2019.

[26] S. Qiu, G. Xu, H. Ahmad, G. Xu, X. Qiu, and H. Xu, "An improved lightweight two-factor authentication and key agreement protocol with dynamic identity based on elliptic curve cryptography," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 2, pp. 978–1002, 2019, doi: 10.3837/tiis.2019.02.027.

[27] Z. Zhang, Q. Dong, and M. Cai, "A new publicly verifiable proxy signcryption scheme," in *Progress on Cryptography*. 2004, pp. 53–57, doi: 10.1007/1-4020-7987-7_7.

[28] H. Elkamshouchy, A. K. AbouAlsoud, and M. Madkour, "New proxy signcryption scheme with DSA verifier," in *Proc. 23rd Nat. Radio Sci. Conf. (NRSC)*, 2006, pp. 1–8, doi: 10.1109/nrsc.2006.386345.

[29] H. Elkamchouchi, M. Nasr, and R. Ismail, "A new efficient strong proxy signcryption scheme based on a combination of hard problems," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2009, pp. 5123–5127, doi: 10.1109/icsmc.2009.5346018.

[30] H.-Y. Lin, T.-S. Wu, S.-K. Huang, and Y.-S. Yeh, "Efficient proxy signcryption scheme with provable CCA and CMA security," *Comput. Math. Appl.*, vol. 60, no. 7, pp. 1850–1858, Oct. 2010, doi: 10.1016/j.camwa.2010.07.015.

[31] H. M. Elkamchouchi, Y. Abouelseoud, and W. S. Shouaib, "A new proxy signcryption scheme using warrants," *Int. J. Intell. Eng. Inform.*, vol. 1, p. 309, Jan. 2011, doi: 10.1504/ijiei.2011.044100.

[32] H. M. Elkamchouchi, E. F. Abu Elkhair, and Y. Abouelseoud, "An efficient proxy signcryption scheme based on the discrete logarithm problem," *Int. J. Inf. Technol., Model. Comput.*, vol. 1, no. 2, pp. 7–19, May 2013.

[33] N.-W. Lo and J.-L. Tsai, "A provably secure proxy signcryption scheme using bilinear pairings," *J. Appl. Math.*, vol. 2014, pp. 1–10, May 2014, doi: 10.1155/2014/454393.

[34] Y. Ming and Y. Wang, "Proxy signcryption scheme in the standard model," *Secur. Commun. Netw.*, vol. 8, no. 8, pp. 1431–1446, May 2015, doi: 10.1002/sec.1092.

[35] C.-X. Zhou, "Identity based generalized proxy signcryption scheme," *Inf. Technol. Control*, vol. 45, no. 1, pp. 13–26, Mar. 2016.

[36] R. I. Abdelfatah, "A novel proxy signcryption scheme and its elliptic curve variant," *Int. J. Comput. Appl.*, vol. 165, pp. 36–43, 2017.

[37] Q. Yanfeng, T. Chunming, L. Yu, X. Maozhi, and G. Baoan, "Certificateless proxy identity-based signcryption scheme without bilinear pairings," *China Commun.*, vol. 10, no. 11, pp. 37–41, Nov. 2013, doi: 10.1109/cc.2013.6674208.

[38] C. Zhou, Y. Zhang, and L. Wang, "A provable secure identity-based generalized proxy signcryption scheme. I," *J. Netw. Secur.*, vol. 20, no. 6, pp. 1183–1193, 2018.

[39] H. Yu, Z. Wang, J. Li, and X. Gao, "Identity-based proxy signcryption protocol with universal composability," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Dec. 2018.

[40] Z. Guo, Y. Shen, A. K. Bashir, M. Imran, N. Kumar, D. Zhang, and K. Yu, "Robust spammer detection using collaborative neural network in Internet of Thing applications," *IEEE Internet Things J.*, early access, Jun. 19, 2020, doi: 10.1109/JIOT.2020.3003802.

[41] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.

[42] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 8, pp. 2072–2085, Aug. 2015.

[43] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77215–77226, 2020.

[44] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Secur. Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 8405879.

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.

NOOR UL AMIN received the master's degree in computer science from the University of Peshawar, Pakistan, in 1996, and the Ph.D. degree in computer science from the Department of Information Technology, Hazara University, Pakistan. He has been the Head of the Department of Information Technology and the Director of IT at Hazara University, for 11 years. He is currently the Chair of the Department of Telecommunication, Hazara University. He has completed recently a research and development project sponsored by the Ministry of Science and Technology, Pakistan, and established seven hi-tech research and development labs.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He has worked as the Vice Dean of development and quality with the College of Computer and Information Sciences (CCIS). He is currently a Professor with the Department of Computer Science, CCIS, King Saud University (KSU), Riyadh, Saudi Arabia. He is also the Director of the Chair of Cyber Security, CCIS, KSU. He has served as the Dean of the College of Computer and Information Sciences and the Head of the Academic Accreditation Council, Al-Yamamah University. His research interests include mobile-pervasive computing and cyber security. He has served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as IEEE CCNC, ACM BodyNets, and IEEE HPCC.

MUHAMMAD ASGHAR KHAN received the bachelor's degree in electronic engineering from Iqra University, Karachi, Pakistan, and the master's degree in electrical engineering from the Center of Advanced Studies in Engineering (CASE), Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in electronic engineering with the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He is currently serving as a Lecturer with the Department of Electrical Engineering, Hamdard University, Islamabad. He serves as a Reviewer for different journals. His research interests include UAVs/drones, with a focus on networks, platforms, security, as well as applications and services.

M. IRFAN UDDIN is actively involved with academia and research. He has worked as a Graduate Research Associate with the University of Peshawar, the University of Amsterdam, and the University of Turin. He was a Faculty Member with the Computer Science Faculty, Al-Yamamah University, Saudi Arabia. He is currently working with the Institute of Computing, Kohat University of Science and Technology, Kohat, Pakistan. He has participated in different research journals and conferences. He has published several research articles in well-reputed international journals and conference proceedings. He serves as a Reviewer for different journals. His research interests include machine learning, data science, deep learning, convolutional neural networks, reinforcement learning, computer vision, big data, and parallel computing.

QIAOZHI HUA received the B.E. degree in electrical communication from the Wuhan University of Science and Technology, China, in 2011, and the M.S. and Ph.D. degrees from Waseda University, Japan, in 2015 and 2019, respectively. He is currently a Lecturer with the Computer School, Hubei University of Arts and Science, Hubei, China. His research interests include game theory and wireless communication.