IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 26, 2020, accepted May 10, 2020, date of publication May 15, 2020, date of current version June 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2994988

A Lightweight and Formally Secure Certificate Based Signcryption With Proxy Re-Encryption (CBSRE) for Internet of Things Enabled Smart Grid

SADDAM HUSSAIN[1], INSAF ULLAH[2], HIZBULLAH KHATTAK[1], MUHAMMAD ADNAN[3], SARU KUMARI[4], SYED SAJID ULLAH[1], MUHAMMAD ASGHAR KHAN[2], AND SHAH JAHAN KHATTAK[5]

[1]IT Department, Hazara University Mansehra, Mansehra 21120, Pakistan
[2]HIET, Hamdard University, Islamabad Campus, Islamabad 44000, Pakistan
[3]Higher Colleges of Technology, Al Ain Men's College, Al Ain, United Arab Emirates
[4]Department of Mathematics, Chaudhary Charan Singh University, Meerut 250001, India
[5]Pakistan Engineering Council (PEC), Islamabad 44000, Pakistan

Corresponding author: Saddam Hussain (saddam_1993@hotmail.com)

ABSTRACT A smart grid is a new ecosystem, which is made by combining a number of smart Internet of Things (IoT) devices that manage wide energy sources by increasing the efficiency and reliability of the smart energy systems. As the IoT devices in the smart grid ecosystem generate a gigantic amount of data that needs to be stored and managed in the cloud server. On the other hand, the stored data in the cloud server can be accessible to a number of data users, therefore the data need authenticity and secrecy. Here, to fulfill the security requirements of such type of communication, signcryption with proxy re-encryption technique is the most suitable option where a semi-trusted third party can alter a ciphertext that has been encrypted for one user into another ciphertext without seeing the original content of the message. However, the existing signcryption with proxy re-encryption schemes for the smart grid environment is suffering from more bandwidth space and greater computational time requirements. Thus, in this paper, we propose a lightweight certificate-based signcryption with a proxy re-encryption (CBSRE) scheme for smart grid based-IoT devices with the intention of reducing the computational and communicational costs. For the security and efficiency of the proposed CBSRE scheme, we used a hyperelliptic curve cryptosystem that uses small parameters with a key size of 80-bits. Furthermore, the proposed scheme provides the security requirements of confidentiality (IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II), unforgeability (EUF-CBSRE-CMA-I and EUF-CBSRE-CMA-II) and forward secrecy. Additionally, we compared our proposed CBSRE scheme with the existing proxy signcryption with re-encryption schemes and the final results show that the new scheme provides strong security with the expanse of minimal computational and communications resources.

INDEX TERMS Smart grid, IoT, cloud computing, signcryption with proxy re-encryption, hyperelliptic curve.

I. INTRODUCTION

Electricity is the main source of energy which plays a vital role in the power industry. As the complex traditional electricity systems have been developed more than 100 years ago which are not able to scale down the dynamic changes of the modern era [1], [2]. However, the smart grid (SG) is a new technology system that can manage wide energy sources and increases the reliability and efficiency of an entire energy system which can be a sustainable solution for the transmission, generation, distribution, and consumption of electricity [3], [4]. The SG ecosystem is actually made by combining a number of smart devices, i.e. smart metering and monitoring systems that are able to generate enormous amounts of data and transmits it to the network by using the Internet [5].

Nowadays, the Internet of Things (IoT) involves in almost every domain of modern society. About 30 billion smart objects will be connected to the internet in 2020 which includes physical devices, vehicles, sensors, software,

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

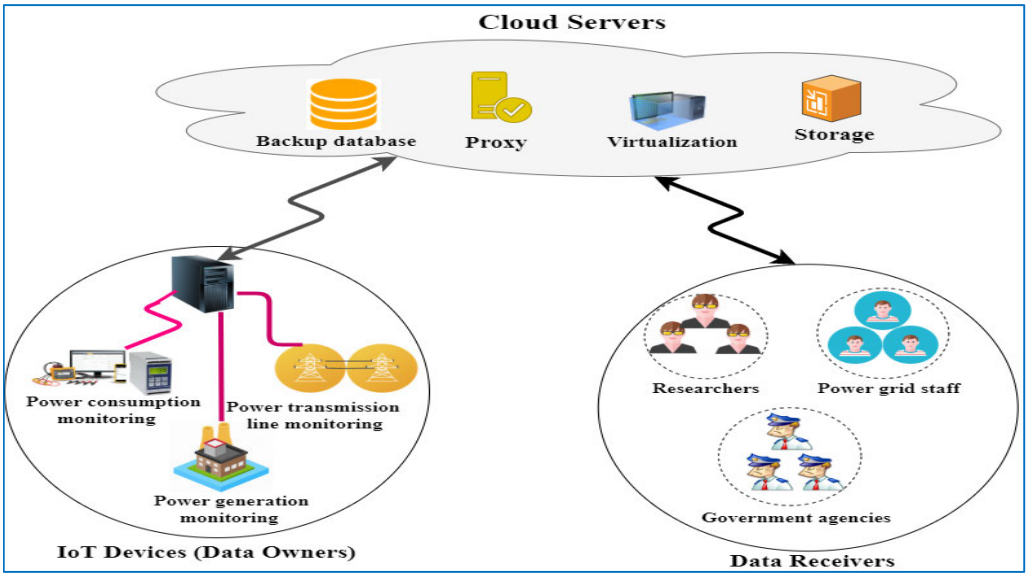


FIGURE 1. Illustration of IoT enabled SG with Cloud server.

actuators, embedded object, and home appliances [6]. The IoT is a network of smart devices that provide connectivity for these smart devices through which they can exchange data and commands. Similarly, the IoT technology can be applied in SG technology will effectively integrate the infrastructure of the power system as well as facilitates the communication resources [7]. Besides, there is a need for IoT big data analytics platform which is proficient for managing and transforming the gigantic household energy consumption data into some actionable insights [8]. It is conspicuous that cloud computing owns the potential capability which can improve the reliability of SG systems by allowing the data-driven services to encounter the challenges of data storage, processing and classification analysis [9]. Furthermore, an IoT enabled Cloud-based platform for SG application, is shown in Figure 1 below, in which the IoT devices are responsible for data attainment, while the substantial amount of data collected by IoT devices is stored and managed in the cloud server (CS). Here, the commercial nature of a CS and the sensitivity of grid-related data collected by IoT Devices enquires strong security measures during the transmission process [10]. The stored data in the CS can be accessible to multiple data users such as researchers, government agencies and power grid staff, etc. the government agencies and researchers analyze the stored data for future policymaking or investigation purposes. However, the power grid staff can access the collected data for monitoring the status of the power grid respectively [11].

The data can be accessible to anyone so there is a need for authenticity and data security. The authenticity can be ensured by applying a digital signature [12], while the data security can be gained from encryption [13]. However, the high communication and computation cost of encryption and digital signature makes a way for signcryption. In 1997, Zheng for the first time proposed the concept of signcryption which logically combines the functions of digital signature and encryption in a single step with minimal costs [14]. As the data collected from IoT smart devices are sent for processing and storage purposes to the cloud server where the cloud service provider can check the authentication of data only. Here, the involvement of such a third-party service provider arises a new trust-related issue for SG systems. For this purpose, in 1998, Blaze at Euro crypt [15], introduced the concept of Proxy re-encryption (P-RE) cryptosystem which allows a third party to alter a ciphertext that has been encrypted for one user, such that another user may also be able to decrypt it. The given concept was later enhanced by Ateniese and Hohenberger in 2005 [16], by introducing a proxy-re signature (P-RS) cryptosystem, in which a proxy is able to transform a signature computed under Bob's private key into another signature that can be verified under Alice's public key. Later, in 2008, Chandrasekar *et al.* [17], combined signcryption with proxy re-encryption (SP-RE) which provides the security features like confidentiality and authentication with P-RE capabilities in an efficient and cost-effective way.

However, most of proxy re-encryption, proxy-re signature, and signcryption with proxy re-encryption (SP-RE) schemes are based on old public-key cryptography (PKC), identity-based cryptography (IBC), and certificateless cryptography (CLC), respectively. Unfortunately, the PKC is not a suitable choice for IoT devices due to certificate management issues such as certificate revocation and renewing [18]. Besides, the IBC suffers from an eminent key escrow problem (KEP), as the private keys of all the participants are known to the private key generation center [19]–[21]. Furthermore, the CLC also suffers from the partial private key distribution problem (PPKDP), as the distribution of partial private keys needs a secure channel between the key generation center and all the participants [21], [22].

In contrast to the aforementioned cryptosystems, to remove the certificate management issues such as certificate revocation and renewing of PKC, the KEP of IBC, and the PPKDP of CLC, Gantry [23], proposed the concept of certificate-based cryptography (CBC). The CBC is based on the old concept of PKC, in which the participants in a network have their public and private keys. The public key used by the certifier's authority (CsA), based on that the CsA generates a certificate for each participant using the concept of IBC. Furthermore, the certificate assigned by CsA acts as a partial private key and also used as a decryption key on the receiver side [19].

Note that, here in CBC the certificate distribution among the users does not need any secure channel.

The security and efficiency of the signcryption with re-encryption schemes by utilizing the aforementioned cryptography (PKC, IBC, CLC, and CBC) is normally based on computational hard problems i.e. RSA, Bilinear pairing (BP), and elliptic curve cryptosystems (ECC). However, the RSA suffers from a large factorization problem with a 1024 key size while the BP is 14.31 times worse than the RSA due to its large pairing computation [24], [25]. The ECC uses a 160-bit key to reduce the computation hard problem to some extent [26]. Likewise, a 160-bit key is still not affordable for the resource-constrained devices which generate a huge amount of random data. For this purpose, a new type of cryptosystem is introduced in [27], [28], called the hyperelliptic curve cryptosystem (HEC), which offers the correspondent level security of RSA, ECC, and BP, using 80-bit key. The small key size with strong security better suits it for the SG based-IoT devices.

The aforementioned discussion motivates us, to contribute a new scheme called certificate-based signcryption with proxy re-encryption (CBSRE), with the intention to remove the limitations of existing SP-RE, in terms of security and efficiency. The CBSRE scheme can be lightweight in nature because it uses the concept of HEC which needs fewer key sizes as compared to RSA, ECC, and BP. Furthermore, the proposed scheme removes the shortcomings such as certificate management issues, KEP, and the PPKDP, respectively. The salient features of the CBSRE scheme are as follows.

- First, we provide the syntax for the proposed CBSRE scheme.
- Second, we provide a proper algorithm for the proposed CBSRE scheme.
- Our proposed scheme provides the security requirements of confidentiality (IND-CBPSE-CCA2-I and IND-CBPSE-CCA2-II), unforgeability (EUF-CBPSE-CMA-I and EUF-CBPSE-CMA-II) and forward secrecy.
- We also compared our proposed CBSRE scheme with the existing SP-RE schemes on the bases of computational cost and communicational overhead, the final results show that our proposed scheme consumes less computational and communicational resources as compared to the previous schemes.

A. PRELIMINARIES

1) HYPERELLIPTIC CURVE (HEC)

The HEC is a class of algebraic curves, introduced by Koblitz [29]. It can also be viewed as a generalized form of elliptic curves (EC) [30]. Unlike EC, the points of HEC cannot be derived from a group [31]. The HEC computes the additive Abelian group which can be derived from a devisor. The lower parameter size with the same level security in contrast with RSA, bilinear pairing and EC, the HEC attracts the resource-constrained devices [32].

The curve whose genus value is 1, usually, known as EC. An HEC with a genus greater than 1 is shown in Figure 2 [33]. Similarly, the group order of the finite field ($\mathbb{F}_{\mathbb{q}}$) for the (genus $=$ 1), required 160-bits long operands, that at least needs $\mathbb{g}.\mathbb{l}\mathbb{o}\mathbb{g}_2(\mathbb{q}) \approx \mathbb{2}^{\mathbb{160}}$, where, $\mathbb{g}$ is the genus of the curve over $\mathbb{F}_{\mathbb{q}}$ which is a set of a finite field of order $\mathbb{q}$. Similarly, for the curve with (genus $=$ 2), required 80-bits long operands. Furthermore, for curve with (genus $=$ 3), required 54-bits long operands [34].

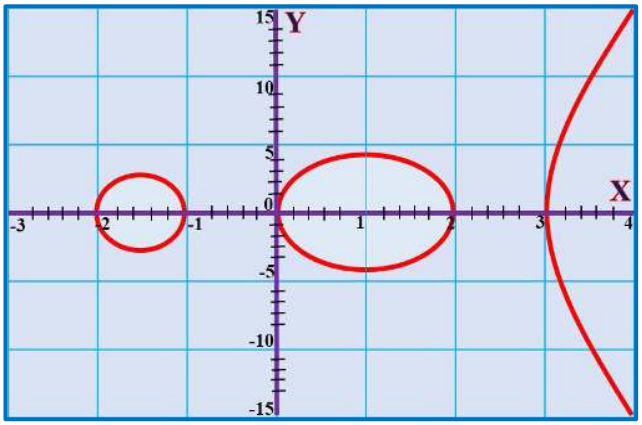


FIGURE 2. Genus = 2 of Hyperelliptic curve [33].

Suppose $\mathbb{F}$ be a finite field with $\overline{\mathbb{F}}$ to be the algebraic closure of the field F. An HEC of a genus ($\mathbb{g} > 1$) over $\mathbb{F}$ is a set of solution $(\mathbb{x}, \mathbb{y})\mathcal{E}\overline{\mathbb{F}}$ x $\overline{\mathbb{F}}$ to the following equation of the curve.

$$\text{HEC} : y^2 + h(x)\, y = f(x)$$

If there are no pairs of $(\mathbb{x}, \mathbb{y})\mathcal{E}\overline{\mathbb{F}}$ x $\overline{\mathbb{F}}$ then such a curve is considered to be non-singular, further, it needs to satisfy the aforementioned curve equation at the same time with the following given partial differential equation.

$$2y + h(x) = 0 \quad \text{and} \quad h'(x)\, y - f'(x) = 0$$

The polynomial h (x) $\mathcal{E}\mathbb{F}$[u] is a degree of $\mathbb{g}$ and h (x) $\mathcal{E}\mathbb{F}$[u] is the monic polynomial of degree $2\mathbb{g} + 1$ [35].

2) COMPLEXITY ASSUMPTIONS

While conducting the analysis, we made the following assumptions;

- The $\mathbb{F}_{\mathbb{q}}$ is a finite field with order $\mathbb{q}$, where $\mathbb{q} \approx \mathbb{2}^{\mathbb{80}}$

- The D is a divisor of an HEC, which is a finite sum of points as $D = \sum p_{i\varepsilon HEC}\, m_i p_i$, where $m_i \varepsilon \mathbb{F}_q$.

3) ASSUMPTIONS OF HYPERELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM (HECDLP)

We made the following supposition for HECDLP.

- ∂ belongs to $\{1, 2, 3, \ldots\ldots, q-1\}$
- The probability computation ∂ from $\mathcal{R} = \partial.D$ is negligible.

4) COMPUTATIONAL DIFFIE-HELLMAN ASSUMPTION OF HYPERELLIPTIC CURVE (*HCCDHP*)

For *HCCDHP*, we make the following suppositions.

- The ∂ and Q belongs to {1, 2, 3,……., q-1}
- The probability computation of ∂ and Q from $\Gamma = \partial.Q.D$ is negligible.

B. SYNTAX OF CERTIFICATE-BASED SIGNCRYPTION WITH PROXY RE-ENCRYPTION (CBSRE) SCHEME

Our proposed CBSRE scheme is an extended version of Manzoor *et al.* [36] and Yang and Jiguo [22] schemes. The syntax includes nine algorithms (i.e. Setup, Certifications, Key Generations, Signcryption, Re-encryption Key Generation, Re- encryption, Unsigncryption, and Decryption) which are discussed below.

1) SETUP

In this phase, the CsA takes the security parameter π is input and generates the common parameter set $\mho = (\mathcal{HC}, \hbar_0, \hbar_1, \hbar_2, n = 2^{80}, Z_n, \mathcal{R})$ and published it to the network.

2) KEY GENERATION

A user with an identity $ID_\mho$ will produce his private and public key as: it selects the private key $\alpha_\mho \epsilon Z_n$ and set $\mathcal{PK}_\mho = \alpha_\mho$, then calculate a partial public key $\mathcal{PP}\beta_\mho$. It takes π and $\mho$ as an input

3) CERTIFICATIONS

Given $\mho$, $\mathcal{R}$, $ID_\mho$, and $\mathcal{PP}\beta_\mho$, C_sA randomly pick $\delta_\mho \epsilon Z_n$ and compute a full public key for the user with $ID_\mho$ as: $\mathcal{FP}\beta_\mho$ and certificate $\mathcal{C}er_\mho$.

4) SIGNCRYPTION

Provide as an input, $\mho$ the sender identity ID_s, receiver's ID_r, sender private key $\mathcal{PK}_s$ and massage (m), respectively. This algorithm creates the signcrypted cipher text $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$.

5) RE-ENCRYPTION KEY GENERATION

Provide as an input $\mho$, the sender certificate $\mathcal{C}er_s$, sender identity ID_s, receiver's ID_r, and sender private key $\mathcal{PK}_s$, respectively. It generates a re-encryption key $\mathcal{RK}_{s \longmapsto r}$ and send it with ψ to the (proxy) Cloud Server (CS).

6) RE-ENCRYPTION

Given an input $\mho$, $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$ and a re-encryption key $\mathcal{RK}_{s \longmapsto r}$, the CS generates $\phi = (\mathcal{C}^{/}, \Upsilon^{/}, \mathcal{Z}, \mathcal{G})$ as a second level cipher text.

7) UNSIGNCRYPTION

Given an input $\mho$, sender certificate $\mathcal{C}er_s$, sender identity ID_s, sender private key $\mathcal{PK}_s$, and $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$, the sender performs the Unsigncryption process.

8) DECRYPTION

Given an input, receiver,s certificate $\mathcal{C}er_r$, sender identity ID_s, receiver identity ID_r, sender public key $\mathcal{PUK}_{sI}$, receiver private key $\mathcal{PK}_r$, $\phi = (\mathcal{C}^{/}, \Upsilon^{/}, \mathcal{Z}, \mathcal{G})$, the receiver performs the decryption process.

C. THREAT MODEL

For the security explanation of certificate-based cryptosystems, two types of adversaries need to considered i.e. Type-one adversary ($\mathcal{A}_I$) and Type-two adversary ($\mathcal{A}_{II}$), respectively [22], [23], [38]. The $\mathcal{A}_I$ adversary shows an uncertified contestant that doesn't know the certificate of the target contestants and the master secret key, while $\mathcal{A}_{II}$ adversary shows an honest-but-curious certificate authority that has complete control of the master secret key and also controls the generation of certificates for the contestants. Moreover, we are going to use the following 6 oracles which can be accessed by the adversaries in an adaptive manner to simulate the attacking scenarios.

1) $\theta^{\text{CREATECONT}}$ QUERIES

Upon receiving the identity ID_i, the challenger (ξ) will respond with the public key $\mathcal{FP}\beta_i$. However, if the ID_i somehow doesn't exist, then the ξ generates a key pair of the public and private key ($\mathcal{FP}\beta_i$, $\mathcal{PK}_i$) for the recipient ID_i and outputs the $\mathcal{FP}\beta_i$. In this scenario, a contestant is created with an identity ID_i. Further, for simplicity purposes, we presume that identity will be responded only by the following mentioned oracles when it has been created.

2) θ^{CORRUPT} QUERIES

Upon receipting an identity ID_i, ξ will output a private key $\mathcal{PK}_i$ in response to the identity ID_i.

3) $\theta^{\text{CERTIFICATE}}$ QUERIES

Upon receiving an identity ID_i, the challenger will output a certificate $cert_i$ in response to the identity ID_i. The $\mathcal{A}_{II}$ adversary doesn't need to make any sort of queries to this particular oracle, because it uses the master secret key to generate a certificate for the users.

4) $\theta^{\text{SIGNCRYPT}}$ QUERIES

Upon receiving the message m the ξ runs the signcryption algorithm and produces the respective signcrypted text ψ.

5) $\theta^{\text{RE-ENCRYPT-KEY}}$ QUERIES

While receiving two dissimilar identities (ID_i, ID_j), ξ will output re-encryption key ($\mathcal{RK}_{i \longmapsto j}$).

6) $\theta^{\text{RE-ENCRYPTION}}$ QUERIES

On receiving the original ciphertext ($\mathcal{C}_i$), and two dissimilar identities (ID_i, ID_j), ξ will output re-encrypted ciphertext ($\mathcal{C}_i$).

7) θ DECRYPT

upon receiving an original ciphertext $\mathcal{C}_i$ or re-encrypted ciphertext $\mathcal{C}_j^{/}$, and identity ID_i, the challenger will output the decryption of original ciphertext $\mathcal{C}_i$.

Definition 1: The CBSRE is considered to be indistinguishable against the adaptive chosen-ciphertext attacks (IND − CCA2 secure) if there is no adversary that can take a non-negligible advantage in the followed IND-CBSRE-CCA2-I and IND-CBPSE-CCA2-II games.

The indistinguishable security against an adaptive-chosen-ciphertext attack (IND-ACCA2 security) of CBSRE can be explained by two adversaries games IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II in which the challenger will make interaction with Type-one adversary ($\mathcal{A}_I$) and Type-two adversary ($\mathcal{A}_{II}$).

The IND-CBSRE-CCA2-I is a game played between the adversary $\mathcal{A}_I$ and the challenger. The Oracle − I means that the $\mathcal{A}_I$ adversary can adaptively make any sort of queries to oracles ($\theta^{\text{createcont}}$, θ^{corrupt}, $\theta^{\text{certificate}}$, $\theta^{\text{signcrypt}}$, $\theta^{\text{re-encrypt-key}}$, $\theta^{\text{re-encryption}}$, θ^{Decrypt}) with the given restrictions i.e. 1) on identity ID_{chl} it never queries the $\theta^{\text{certificate}}$ oracle. 2) On the (ID_{chl}, $\mathcal{C}_{chl}$) and its derivatives it never queries the θ^{Decrypt} oracle.

Similarly, the IND-CBSRE-CCA2-II is a game played between the adversary $\mathcal{A}_{II}$ and the challenger. The Oracle − II means that the $\mathcal{A}_{II}$ the adversary can adaptively make any sort of queries to oracles ($\theta^{\text{createcont}}$, θ^{corrupt}, $\theta^{\text{signcrypt}}$, $\theta^{\text{re-encrypt-key}}$, $\theta^{\text{re-encryption}}$, θ^{Decrypt}) with the given restrictions i.e. 1) on identity ID_{chl} it never queries the θ^{corrupt} oracle. 2) On the (ID_{chl}, $\mathcal{C}_{chl}$) and its derivatives it never queries the 0^{Decrypt} oracle.

Here, in both the games i.e. (IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II), if $\mathcal{Z}^{/} = \mathcal{Z}$, then we can say that the game is won by the adversary. Moreover, the winning advantage of the adversary's in the game is to be: $|\mathcal{P}_{\mathcal{R}\mathcal{O}\mathcal{B}}\left[\mathcal{Z}^{/} = \mathcal{Z}\right] - \frac{1}{2}|$.

Definition 2: A CBSRE is considered to achieve the security requirement of the forward secrecy if the confidentiality of the message is still achieved if the private key of the signers is compromised in the aforementioned IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II games.

Definition 3: The CBSRE is considered to be unforgeable against existential forgery under adaptive chosen-message attacks (EUF − CBSRE − CMA) secured if there exists no probabilistic polynomial-time forger's in both the following games i.e. (EUF − CBSRE − CMA − I and EUF − CBPSE − CMA − II), has a non-negligible advantage.

The EUF − CBSRE − CMA − I is a game played between the forger f_I and ξ.

Proof: Here we are going to show that, how the algorithm ξ can interact with f_I to solve *HCCDHP*. So, the ξ can interact with f_I by utilizing the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly, Select master secret key and compute master public key and Compute common perimeter param. Then provide master public key and param to f_I.

Training Phase: In this game, the same steps are performed for different queries oracles are the same as in the game IND-CBSRE-CCA2-I among f_I and ξ.

Forgery: At the end of the above process, f_I can make a signcrypted text $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$. Here, note that when f_I the capacity to win this game if the result of decryption has is valid and it holds the following conditions

1) On identity ID_s it never queries the oracle $\theta^{\text{certificate}}$.
2) ψ is not produced by the oracle $\theta^{\text{signcrypt}}$.

The EUF − CBPSE − CMA − II is a game played between the forger f_{II} and ξ.

Proof: Here we are going to show that, how the algorithm ξ can interact with f_{II} to solve *HCCDHP*. So, the ξ can interact with f_{II} by utilizing the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly, Select master secret key and compute master public key and Compute common perimeter param. Then provide a master public key, secret key, and param to f_{II}.

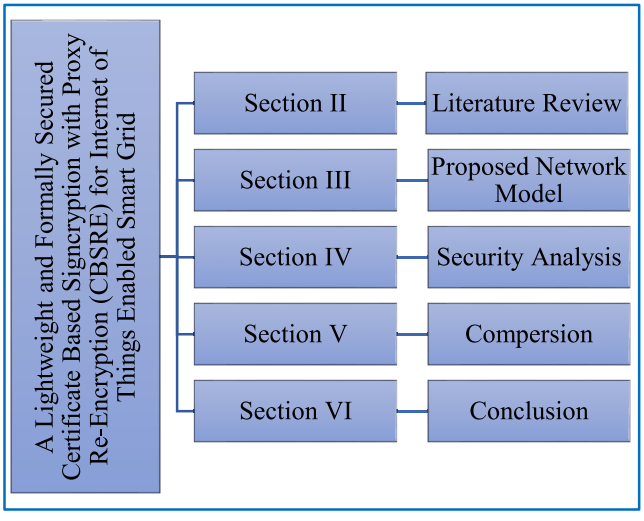
Training Phase: In this game, the same steps are performed for different queries oracles are the same as in the game IND-CBSRE-CCA2-II among f_{II} and ξ.

Forgery: At the end of the above process, f_I can make a signcrypted text $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$. Note that when f_I has the capacity to win this game if the result of the decryption is valid and holds the following conditions

1) On identity ID_s it never queries the oracle θ^{corrupt}
2) ψ is not produced by the oracle $\theta^{\text{signcrypt}}$.

D. PAPER ORGANIZATION

The organization of the paper is shown in the following chart.



II. LITERATURE REVIEW

Hayden *et al.* [40], proposed an Identity (ID)-based Signcryption (IBS) mechanism which assumes a unique identification number available from every device that can be used by the central authority holding a master key and can

produce a unique secret key also. The proposed work is helpful because it does not require a separate configuration of each device. However, the given scheme requires a secure channel for private key distribution between the key-generating server (KGS) and SG devices. Moreover, both the sender and receiver need a huge amount of computational efforts due to Tate pairing with EC. In addition, the scheme can be affected by larger bandwidth requirements.

Chen and Zhang [41], coined the concept of data aggregation with identity-based signcryption to facilitate the SG technology. The authors use a pseudonym technology for achieving the identity of the user. Furthermore, the scheme performs the efforts for reducing the computational cost at the same time with data security during communication. However, the given scheme doesn't meet the security requirement of forward secrecy and suffers from the KEP. Additionally, the scheme is based on BP which can cause the worst efficiency regarding the communication bandwidth and computation efforts.

Alishahi *et al.* [42], presented a free pairing certificateless signcryption scheme based on EC for preserving privacy and integrity of data between data producers and utility servers. Though, the given scheme removes the certificates related issues and key escrow problem. However, the scheme is based on EC which requires a huge amount of communicational and computational resources. Furthermore, it can also be affected by the partial private key distribution problem (PPKDP) i.e. needs a secure channel for partial keys.

Hu *et al.* [43], tossed an attribute-based signcryption scheme for secure multicast communication systems. The author's claim that the scheme provides the security properties of data confidentiality, collusion resistivity, verification of message, and unforgeability. Unfortunately, the scheme was constructed upon BP therefore the computation cost is too high for SG systems.

Umar and Amin [44], proposed a key establishment scheme with secure and critical message dissemination for multicast communications in SG applications. The authors claim that the proposed work provides the security requirements of confidentiality, authentication, and secure message communication. However, the scheme suffers from the requirement of greater computation power due to the use of EC. Furthermore, the author didn't provide any sort of formal network model. Moreover, the authors didn't prove the security of the proposed scheme. Additionally, the scheme suffers from certificate management issues.

Chen and Ren [45], proposed an aggregate signcryption scheme in which the signcryption of multiple messages is combined to generate one signcrypted text. In the proposed scheme the user can signcrypt there data by adding masking random number, then the building gateway combines these multiple signcrypted messages, and forward it to the control center (CC). The CC then verifies the signcrypted messages before aggregation. However, the given scheme is affected by the need for a secure channel for partial private key distribution among the users and high computation cost requirements.

Hu *et al.* [46], proposed a Ciphertext-Policy Attribute-based signcryption scheme for pull and pushed based secure multicast communication in SG. The given scheme provides resistance against the collusion attack and can achieve the security requirements of authentication, confidentiality, and unforgeability. However, the scheme is based on BP which can cause the worst efficiency regarding communication bandwidth and computation efforts.

Sedaghat *et al.* [47], proposed a Ciphertext-policy attribute-based signcryption for data sharing in the SG to reduce computation cost and perform lighter pairing. Moreover, the author outsourced the functionality of signcryption for the end-user, where the storage center transfers the ciphertext to simple cipher (partial designcryption) which requires less computation during designcryption. The proposed scheme provides the security properties of authentication, privacy, and unforgeability. Unfortunately, the proposed scheme is based on BP which is not efficient for the devices with limited resources.

Jin *et al.* [48], proposed a heterogeneous signcryption (HS) scheme to secure the communication between smart meters (SM) and utility servers. In the proposed approach the SM uses the services of IBC and the utility server uses the services of PKI. The authors claim that the given scheme provides the property of integrity, authentication, confidentiality, non-repudiation, and ciphertext anonymity. However, the proposed scheme suffers from certificates management issues and KEP.

Wan *et al.* [49], presented a multi-authority attribute-based signcryption scheme in order to enable the SG operators and electricity suppliers to communicate securely with their respective users in a (downlink). The given scheme provides confidentiality, authentication, and non-repudiation security properties. However, the scheme lacks forward secrecy as a security requirement respectively.

Baoyi *et al.* [50], tossed a certificateless aggregate signcryption scheme to resolve the privacy leakage problem in advance metering infrastructure, which protects the user information and diminishes the amount of data transmission through data concentrator with aggregation. However, the proposed scheme suffers from PPKDP.

Huige *et al.* [51], proposed an ID-based proxy re-signcryption (IDB-PRS) scheme that combines the idea of signcryption with proxy re-encryption. Unfortunately, their scheme is not correct from a mathematical point of view [52]. Furthermore, it also suffers from the KEP, because the private keys for the participated users are generated by KGC.

Rawat and Shrivastava [53], proposed an IDB-PRS scheme to improve the given work of Huige *et al.* [51]. In the proposed scheme the authors use different secure hashing functions message-digest-5 (MD5), secure hash algorithm 1(SHA-1), and secure hash algorithm 256 (SHA-256) separately. The final results show that the SHA-1 algorithm gives high performance as compared to the remaining algorithm. However, the proposed scheme suffers from KEP because the private for the participated users are generated by KGC.

Wang and Ye [54], proposed a new IDB-PRS scheme which uses a semi-trusted party for the conversion among ID decryption and ID verification. Unfortunately, the proposed scheme suffers from the KEP as well as based on BP which can cause the worst efficiency regarding communication bandwidth and computation efforts.

Braeken *et al.* [19], proposed an ID-based signcryption scheme for securing cloud data storage. In the proposed scheme the user can store the signed and encrypted data in the cloud storage server. However, the cloud storage service provider can only check the authenticity of data. When a user request for a particular data access, the data generator first checks the authorization of the requested user and then provides an encryption key to the CS to re-encrypt the stored data for that particular user. However, the given scheme suffers from the KEP as well as the scheme is based on EC which requires a heavy amount of computation and communication cost.

Manzoor *et al.* [36], proposed a blockchain-based proxy re-encryption scheme in which a distributed cloud, stores the data generated by IoT devices after encryption. In the given scheme a system creates a smart contract to share the collected IoT data between the sensor and data users with the interaction of the third party. Moreover, it also uses a proxy re-encryption mechanism that allows visibility to data owners and smart contract holders. Unfortunately, the scheme is based on EC which requires a heavy amount of computation and communication cost. Further, the authors did not validate the security of the scheme in any formal validation tool.

Ahene *et al.* [55], tossed a data access control scheme based on certificateless signcryption with proxy re-encryption for SG in which a data user can securely access customer data with the help of a gateway known as an energy service interface (ESI). The ESI works as a proxy that can re-encrypt data for authorized users based on some delegation commands from the data owner. The given scheme provides the security properties of authentication, confidentiality, integrity, and non-repudiation. However, their scheme suffers from PPKDP. Additionally, it also suffers from more computational power consumption and the need for more bandwidth due to EC.

Ahene *et al.* [56], proposed a data access control scheme based certificateless signcryption with proxy re-encryption for cloud-based SG. In the given scheme, a CS is used to store the encrypted grid-related data. Further, a data user can securely access customer data with the help of the CS. The cloud works as a proxy which re-encrypt data for authorized data users. The proposed scheme provides confidentiality, integrity, and authentication security requirement. However, the proposed scheme suffers from PPKDP. Additionally, the suffer from more computational and consumption power due to BP.

III. PROPOSED CBSRE SCHEME NETWORK MODEL

The smart grid technology manages a wide energy source which increases the efficiency and reliability of the energy system that is a sustainable solution for the transmission, generation, distribution, and consumption of electricity. For security and authenticity in smart grid technology, a number of schemes have been proposed in the literature [19], [36], and, [40]–[56], the proposed schemes provide some useful security features but still have some limitations as mentioned in Table 1. Recently, Ahene *et al.* [55], [56] propose an access control schemes for smart grid-based IoT. The schemes provide security features like confidentiality, integrity, authentication, and non-repudiation for SG based-IoT. However, these schemes are affected form the PPKDP. Furthermore, it also suffers from more computational and communicational powers that need more bandwidth due to the use of BP and ECC. On the other hand, the resource-constrained nature of SG based-IoT devices cannot afford these types of heavy computational and communications operations. To cover the above-mentioned limitation and keeping the demand of SG based-IoT devices motivate us to design a lightweight CBSRE scheme for SG based-IoT.

We present the mechanism for the IoT Enabled SG with certificate-based signcryption with proxy re-encryption for both data sharing and secure data access respectively. For this purpose, we consider four entities, namely certifier authority (C_sA), controller, cloud service provider, and data user as also shown in Figure 3. The SG based-IoT devices sense data and forward it to the controller. The C_sA takes control of the registration process by generating certificates for both the controller and data users based on their identities. The controller ensures the security of gathered data from IoT enabled smart grid devices through signcryption. Further, the controller also ensures the secure transmission of the signcrypted data to the cloud service provider. The cloud service provider is capable of providing high computation and storage facilities. In addition, it also provides services like virtualization, proxy re-encryption, and backup storage merged with many other services that are efficient and beneficial for IoT enabled SG devices. Whenever a data user wants to access some specific data, it simply requests for that particular data to the controller. The controller then issues a special command to the cloud service provider to re-encrypt that particular data for the requested data users. After receiving the signcrypted data, the data user verifies the received signcrypted data and simply performs decryption in order to obtain the desired data.

A. PROPOSED ALGORITHMS FOR CBSRE

This section contains the construction of the proposed CBSRE scheme algorithm and its sub-phases such as Setup, Certifications, Key Generations, Signcryption, Re-encryption Key Generation, Re- encryption, Unsigncryption, and Decryption, respectively. Further, the basic symbols which are used in the construction of the proposed algorithm are shown in Table 2.

The new CBSRE scheme is actually the extended version of Manzoor *et al.* [36] and Yang and Jiguo [22] and contains nine steps that can be seen from the following sub-phases also.

TABLE 1. Advantages and limitation of the literature review.

Schemes	Advantages	Limitations
Hayden et al. [40]	• Does not require a separate configuration of each device • Provides encryption and authentication	• The scheme does not provide a secure channel for private key distribution between KGS and SG devices • Sender and receiver need a huge amount of computational efforts due to Tate pairing with EC
Chen and Zhang [41]	• Reduces the computation burden for the aggregator • Ensure communication security	• Suffer from the KEP • Based on BP which can be causing the worst efficiency
Saeed et al. [42]	• Removes the certificates related issues and KEP • Provides confidentiality and authentication	• Based on EC which requires a heavy amount of computation and communication cost
Hu et al. [43]	• The scheme provides access control, data confidentiality, and authentication • Provide resistance against collusion attack	• Based on BP which require heavy pairing powers
Nizamuddin et al. [44]	• Provides confidentiality and authentication • Minimizes computational and communicational cost	• Suffers from certificates management issues • Lack of formal security analysis. • Lack of network model
Juqin and Xiaoxi [45]	• Reduces the communication cost • The scheme simplifies the process of encryption and decryption	• Suffer from the PPKDP • High computation cost requirements
Chunqiang et al. [46]	• Provide resistance against the collusion attack • Provides authentication, unforgeability, and confidentiality	• Based on BP that requires a heavy amount of computation and communication cost
Sedaghat et al. [47]	• Storage center performs partial designcryption that reduces the load from the end-users	• Based on BP which is not efficient for resource-constrained devices
Jin et al. [48]	• Provides confidentiality, integrity, authentication, non-repudiation • Reduces communication overhead and energy consumption	• Suffers from certificates distribution issues and KEP
Alsharif et al. [49]	• Provides data confidentiality, authentication, and nonrepudiation • Reduces computational cost	• Lack of public verifiability, forward secrecy, and anti-replay attack security
Baoyi et al. [50]	• Diminishes the amount of data transmission the use of data concentrator through aggregation • Protects user information	• Suffer from PPKDP
W. Huige et al. [51]	• Provide confidentiality and unforgeability	• Suffers from KEP • Based on BP that requires a heavy amount of computation and communication cost • Mathematically not correct
Rawat and Shrivastava [53]	• Provides confidentiality and authenticity	• Suffers from KEP • Based on BP that requires a huge amount of computation and communication cost
Wang et al. [54]	• Shows efficiency in performance than the previous schemes	• Lack of formal security analysis in standard tool • Suffers from KEP • Based on BP that required heavy pairing operations
Braeken et al. [19]	• Ensures secure data access to the cloud storage server	• Suffers from KEP • Based on EC which requires a heavy amount of computation and communication cost
Manzoor et al. [36]	• Ensures a secure transfer of data to the user • Provide scalability to improve trust issues	• Based on EC which requires a huge amount of computation and communication cost • Didn't Validate their scheme in any validation tools.
Ahene et al. [55]	• Data users can securely access customer data • Provides integrity, confidentiality, authentication, and non- repudiation	• Suffers from PPKDP • Suffers from more computational power consumption and the need for more bandwidth due to EC
Ahene et al. [56]	• Data users can securely access customer data with the help of the CS • Provides confidentiality, integrity, authentication	• Suffers from PPKDP • Suffers from more computational and consumption power due to BP

TABLE 2. Notations used in CBS-RE algorithms.

S.NO	Symbol	Explanation
1	$\mathcal{HC}$	A genus two generalized elliptic curve with 80-bit key and parameter size
2	$\mho$	Common parameter set
3	$\mathcal{D}$	A genus two generalized elliptic curve divisor
4	Z_n	A finite field and n=2^{80}
5	$\mathscr{b}$	Master private key
6	$\mathcal{R}$	Master public key
7	$\mathcal{FP}\beta_s$	Sender public key
8	$\mathcal{FP}\beta_r$	Receiver public key
9	$\mathcal{h}_0, \mathcal{h}_1, \mathcal{h}_2, \mathcal{h}_3, \mathcal{h}_4$	SHA512
10	$\mathcal{CER}_s$	Sender certificate
11	$\mathcal{CER}_r$	Receiver's certificate
12	ID_s	Sender identity
13	ID_r	Receiver identity
14	$\mathcal{Pk}_s$	Sender private key
15	$\mathcal{Pk}_r$	Receiver private key
19	$\mathcal{RK}_{s\mapsto r}$	Re- encryptions key
22	m	Message
23	$\oplus$	Encryption/Decryption
24	$\mathcal{C}^{/}$,$\mathcal{C}$	Level two and one ciphertexts
25	ψ	First level Signcryption text
26	ϕ	Second level Signcryption text

1) SETUP

This phase is executed by Certifiers Authority (C_sA), it takes the security parameter π is an input. Also, it generates a common parameter set by completing the following.

- Select a genus two hyperelliptic curve ($\mathcal{HC}$) with an 80-bit key and parameter size.
- Select three one-way collision resistance functions, i.e., $\mathcal{h}_0, \mathcal{h}_1, \mathcal{h}_2, \mathcal{h}_3, \mathcal{h}_4$ and the nature of these functions is SHA512.
- Select $\mathscr{b}\epsilon Z_n$ and compute $\mathcal{R} = \mathscr{b}.\mathcal{D}$ as a master public key, where n = 2^{80}
- Compute $\mho = (\mathcal{HC}, \mathcal{h}_0, \mathcal{h}_1, \mathcal{h}_2, \mathcal{h}_3, \mathcal{h}_4,$ n= 2^{80}, $Z_n, \mathcal{R})$ and published it to the network.

2) KEY GENERATIONS

A user with an identity $ID_\mho$ will produce his private and public key as: it selects the private key $\alpha_\mho \epsilon Z_n$ and set $\mathcal{Pk}_\mho = \alpha_\mho$, then calculate a partial public key $\mathcal{PP}\beta_\mho = \alpha_\mho.\mathcal{D}$. It takes as an input π and $\mho$.

3) CERTIFICATIONS

Given $\mho$, $\mathcal{R}$, $ID_\mho$, and $\mathcal{PP}\beta_\mho$, C_sA randomly pick $\delta_\mho \epsilon Z_n$ and compute a full public key for the user with $ID_\mho$ as: $\mathcal{FP}\beta_\mho = (\mathcal{Puk}_{\mho I}, \mathcal{Puk}_{\mho II}) = (\mathcal{PP}\beta_\mho, \delta_\mho.\mathcal{D})$ and certificate $\mathcal{Cer}_\mho = \delta_\mho + \mathscr{b}\mathcal{h}_0(ID_\mho, \mathcal{FP}\beta_\mho)$.

4) SIGNCRYPTION

Provide as an input $\mho$, sender identity ID_s, receiver's ID_r, sender private key $\mathcal{Pk}_s$ and massage (m), respectively. This algorithm creates the signcrypted cipher text $\psi = (\mathcal{C}_s, \mathcal{G}, \mathcal{Z})$ through the following computations.

- Select $\mathcal{k}\epsilon Z_n$ and compute $\mathcal{W} = \mathcal{k}.\mathcal{D}$
- It Select $\eta\epsilon\{0, 1\}^\gamma$
- Compute $\dagger = \mathcal{h}_1(\eta, ID_s, m)$
- Compute $\Upsilon = \dagger.\mathcal{D}$
- Compute $\mathcal{Q}_s = \mathcal{Puk}_{sI} + \mathcal{Puk}_{sII} + \mathcal{h}_0(ID_s, \mathcal{FP}\beta_s).\mathcal{R}$.
- Generate a Ciphertext as $\mathcal{C} = (\eta, ID_s, m) \oplus \mathcal{h}_2(\dagger.\mathcal{Q}_s)$
- Compute $\mathcal{G} = \mathcal{h}_3(\mathcal{W}, \Upsilon, \mathcal{C})$
- Compute $\mathcal{Z} = \dagger - \mathcal{G}.\mathcal{Pk}_s$
- The final signcrypted ciphertext is computed as; $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$

5) RE-ENCRYPTION KEY GENERATIONS

Provide as an input $\mho$, sender certificate $\mathcal{Cer}_s$, sender identity ID_s, receiver's ID_r, and sender private key $\mathcal{Pk}_s$, respectively. It computes $\mathcal{S} = \mathcal{h}_4(ID_s, ID_r, \mathcal{Pk}_s(\mathcal{Puk}_{rI} + \mathcal{Puk}_{rII} + \mathcal{h}_0(ID_r, \mathcal{FP}\beta_r).\mathcal{R}))$ and re-encryption key as $\mathcal{RK}_{s\longmapsto r} = \frac{\mathcal{Pk}_s + \mathcal{Cer}_s}{\mathcal{S}}$. It is easy to presume that $\mathcal{RK}_{s\longmapsto r} = \frac{\mathcal{Pk}_s + \mathcal{Cer}_s}{\mathcal{h}_4(ID_s, ID_r(\mathcal{Pk}_r + \mathcal{Cer}_r)}$.

6) RE-ENCRYPTION

Given an input $\mho$, $\psi = (\mathcal{C}, \Upsilon, \mathcal{W},)$ and a re-encryption key $\mathcal{RK}_{s\longmapsto r}$, the CS performs the following steps.

- It first checks if $\Upsilon \stackrel{?}{=} \mathcal{Z}.\mathcal{D} + \mathcal{G}.\mathcal{PP}\beta_s$ holds, then set $\mathcal{C}^{/} = \mathcal{C}$.
- Compute $\Upsilon^{/} = \mathcal{RK}_{s\longmapsto r}\Upsilon$
- Set $\phi = (\mathcal{C}^{/}, \Upsilon^{/}, \mathcal{Z}, \mathcal{G})$ as a second level cipher text.

7) UNSIGNCRYPTION

Given an input $\mho$, sender certificate $\mathcal{Cer}_s$, sender identity ID_s, sender private key $\mathcal{Pk}_s$, and $= (\mathcal{C}, \Upsilon, \mathcal{G}, \mathcal{Z})$, the sender performs the following steps.

- It first checks if $\Upsilon \stackrel{?}{=} \mathcal{Z}.\mathcal{D} + \mathcal{G}.\mathcal{PP}\beta_s$ holds
- Then decrypts $(\eta, ID_s, m) = \mathcal{C} \oplus \mathcal{h}_2(\mathcal{Pk}_s + \mathcal{Cer}_s)\Upsilon)$.

8) DECRYPTION

Given an input, receivers certificate $\mathcal{Cer}_r$, sender identity ID_s, receiver identity ID_r,sender public key $\mathcal{Puk}_{sI}$, receiver private key $\mathcal{Pk}_r$, $\phi = (\mathcal{C}^{/}, \Upsilon^{/}, \mathcal{Z}, \mathcal{G})$, the receiver performs the following steps.

- It first checks if $\Upsilon \stackrel{?}{=} \mathcal{Z}.\mathcal{D} + \mathcal{G}.\mathcal{PP}\beta_s$ holds
- Compute $\mathcal{S}^{/} = \mathcal{h}_4(ID_r, ID_s(\mathcal{Pk}_r + \mathcal{Cer}_r)\mathcal{Puk}_{sI})$.
- Then decrypts $(\eta, ID_s, FNs, m)^{/} = \mathcal{C}^{/} \oplus \mathcal{h}_2(\mathcal{S}^{/}\Upsilon^{/})$.

B. CORRECTNESS

The receiver can recover the plaintext as:

$$(\eta, ID_s, m)$$
$$= \mathcal{C} \oplus \mathcal{h}_2((\mathcal{Pk}_s + \mathcal{Cer}_s)\Upsilon).$$
$$= \mathcal{C} \oplus \mathcal{h}_2((\alpha_s + \delta_s + \mathscr{b}\mathcal{h}_0(ID_s, FP\beta_s))\Upsilon).$$

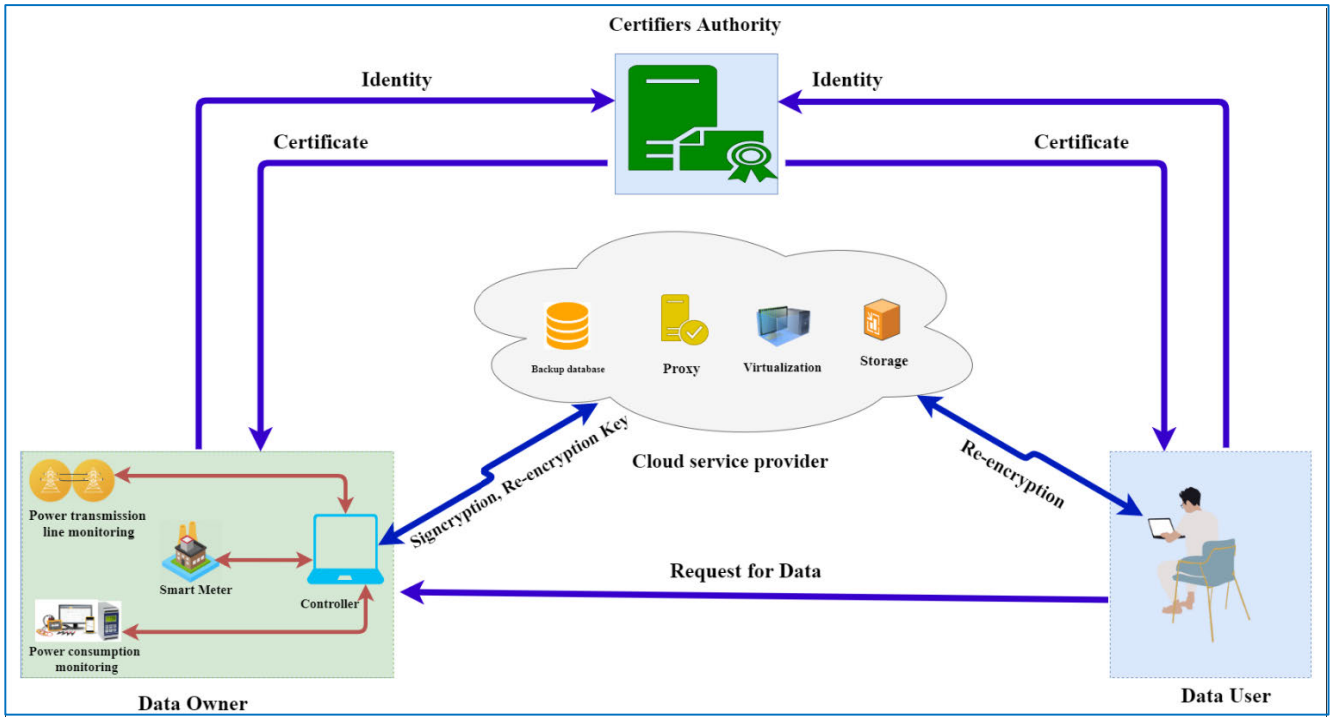


FIGURE 3. Network model of the proposed scheme.

$$= \mathcal{C} \oplus \hbar_2\left(\left(\alpha_s + \delta_s + \wp\hbar_0(ID_s, \mathcal{FP}\beta_s)\right)\dagger.D\right).$$
$$= \mathcal{C} \oplus \hbar_2\left(\left(\mathcal{P}u\hbar_{sI} + \mathcal{P}u\hbar_{sII} + \hbar_0(ID_s, \mathcal{FP}\beta_s)\mathcal{R}\right)\dagger\right).$$
$$= (\eta, ID_s, FNs, m) \oplus \hbar_2(\P.\mathcal{Q}_s) \oplus \hbar_2(\dagger.\mathcal{Q}_s) = (\eta, ID_s, m)$$

It can also verify the signature as: $\Upsilon \stackrel{?}{=} .\mathcal{D} + \mathcal{G}.\mathcal{PP}\beta_s$
$\stackrel{?}{=} (\dagger - \mathcal{G}.\mathcal{P}\hbar_s).\ \mathcal{D} + \mathcal{G}.\mathcal{PP}\beta_s$
$\stackrel{?}{=} (\dagger.\mathcal{D} - \mathcal{G}.\mathcal{P}\hbar_s.\mathcal{D}) + \mathcal{G}.\mathcal{PP}\beta_s$
$\stackrel{?}{=} \dagger.\mathcal{D} - \mathcal{G}.\mathcal{PP}\beta_s + \mathcal{G}.\mathcal{PP}\beta_s \stackrel{?}{=} \mathcal{G}\dagger.\mathcal{D} = \Upsilon$

IV. SECURITY ANALYSIS

In the threat model, we explain the basic security properties that need efficient and secure communication between cloud and smart grid-based IoT devices. Moreover, we prove that the CBSRE scheme is fully secured and infeasible against malicious attackers while satisfying the basic security properties.

To certify the security of the CBSRE scheme we are checking the following security features of CBSRE against the attacker, i.e. type one $\mathcal{A}_I$ and type two $\mathcal{A}_{II}$.

A. THEOREM (CONFIDENTIALITY)

Confidentiality means that the plaintext message (m) should be hidden from the attacker. The CBSRE provides confidentiality property because of the attacker ($\mathcal{A}_I$ and $\mathcal{A}_{II}$) is infeasible to get access to the original contents of ciphertext in the following cases. We provide the following two Lemma's to prove this property.

Lemma 1: Suppose a probabilistic polynomial-time attacker called type one $\mathcal{A}_I$ having the advantage ς to break IND-CBSRE-CCA2-I, the security of designed approach with the time τ and carrying out utmost $\mathcal{Q}_{\hbar_i}$ hash queries $\hbar i\ (i = 0, 1, 2, 3, 4)$, $\mathcal{Q}_{cc}$ create contestant queries to the oracle $\theta^{createcont}$, $\mathcal{Q}_{corp}$ corrupt queries to the oracle $\theta^{corrupt}$, $\mathcal{Q}_{cert}$ certificate queries to the oracle $\theta^{\text{certificate}}$, $\mathcal{Q}_{signc}$ signcryption queries to the oracle $\theta^{signcrypt}$, $\mathcal{Q}_{renk}$ re-encryption key queries to the oracle $\theta^{\text{re-encrypt-key}}$, $\mathcal{Q}_{renc}$ re-encryption queries to the oracle $\theta^{\text{re-encryption}}$, and $\mathcal{Q}_{decr}$ decryption queries to the oracle $\theta^{\text{decryption}}$, then there exists an algorithm ξ which can solve *HCCDHP* problems for $\mathcal{A}_I$ with the following advantages:

$$\varsigma' = {}^{1}\!/_{\mathcal{Q}_2}\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^{\pi}} - \frac{\mathcal{Q}_{decr}}{2^{\pi}} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right)$$

Proof: Here we show that how the algorithm ξ can interact with $\mathcal{A}_I$ to solve *HCCDHP* from the given instance $(\mathcal{D}, ß.\mathcal{D}, \Lambda.\mathcal{D})$. So, the ξ can interact with $\mathcal{A}_I$ by utilizing the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly from $(1\ \partial \preceq \mathcal{Q}_{cc})$, select $ß \epsilon Z_n$ and compute $\mathcal{R} = ß.\ \mathcal{D}$ as a master public key. Compute $\mho = (\mathcal{HC}, \hbar_0, \hbar_1, \hbar_2, h_3, \hbar_4, n = 2^{80}, Z_n, \mathcal{R})$, provide $\mathcal{R}$ and to $\mathcal{A}_I$.

$\hbar_0$ Queries: If $\mathcal{A}_I$ submit a query with $(ID_i, \mathcal{FP}\beta_i)$ after reception this query ξ search in LH_0 list, and if the tuple $(ID_i, \mathcal{FP}\beta_i, h_0)$ exists, then ξ handover h_0 to $\mathcal{A}_I$. Otherwise, it picks h_0 from Z_n, store $(ID_i, \mathcal{FP}\beta_i, h_0)$ in LH_0, and returns h_0 to $\mathcal{A}_I$.

$\hbar_1$ Queries: An event that $\mathcal{A}_I$ submit a query with (η, ID_i, FNi, m) after reception this query ξ search in LH_1, and if the tuple $(\eta, ID_i, FNi, m, h_1)$ exists, then ξ handover h_1 to $\mathcal{A}_I$. Otherwise, it picks $h_1 Z_n$, store $(\eta, ID_i, FNi, m, h_1)$ in LH_1, and returns h_1 to $\mathcal{A}_I$.

h_2 Queries: When $\mathcal{A}_I$ submit a query with (δ), after reception this query ξ search in LH_2, and if the tuple (δ, h_2) exists, then ξ handover h_2 to A_I. Otherwise, it picks h_2Z_n, store (δ, h_2) in LH_2, and returns h_2 to $\mathcal{A}_I$.

h_3 Queries: An event that $\mathcal{A}_I$ submit a query with ($\mathcal{W}_i$, Υ_i, $\mathcal{C}_i$), after reception this query ξ search in LH_3, and if the tuple ($\mathcal{W}_i$, Υ_i, $\mathcal{C}_i$, h_3) exists, then ξ handover h_3 to $\mathcal{A}_I$. Otherwise, it picks h_3Z_n, store ($\mathcal{W}_i$, Υ_i, $\mathcal{C}_i$, h_3) in LH_3, and returns h_3 to $\mathcal{A}_I$.

h_4 Queries: When $\mathcal{A}_I$ submit a query with (ID_i, ID_j, $\mathcal{S}$), after reception this query ξ search in LH_4, and if the tuple (ID_i, ID_j, $\mathcal{S}$, h_4) exists, then ξ handover h_4 to $\mathcal{A}_I$. Otherwise, it picks h_4Z_n, store (ID_i, ID_j, $\mathcal{S}$, h_4) in LH_4, and returns h_4 to $\mathcal{A}_I$.

$\theta^{createcont}$ ***Queries***: If $\mathcal{A}_I$ send a query with identity ID_i for the tuple (ID_i, $\mathcal{FP}\beta_i$, $\mathcal{P}k_i$, δ_i, $\mathcal{C}er_i$), then ξ can do the following steps.

- At the event if ID_i is already available In the contestant list CON^{list}, then it returns $\mathcal{FP}\beta_i$ to $\mathcal{A}_I$.
- When the ID_i is the ∂ dissimilar identity which is asked by $\mathcal{A}_I$, then it uniformly picks $\delta_\partial, \alpha_\partial \epsilon Z_n$, sets $\mathcal{FP}\beta_\partial = (\delta_\partial.\mathcal{D}, \alpha_\partial.\mathcal{D})$ and set $\alpha_\partial = \mathcal{P}k_\partial$. After this process, it inserts a new tuple (ID_∂, $\mathcal{FP}\beta_\partial$, $\mathcal{P}k_\partial$, δ_∂, $\perp$) into CON^{list} and set $\mathcal{C}er_\partial = \delta_\partial + \Lambda h_0(ID_\partial, \mathcal{FP}\beta_\partial)$. Note that $\mathcal{C}er_\partial$ cannot be known to $\mathcal{A}_I$.
- If the above two steps were not happening, it uniformly selects $\alpha_i, \varkappa_i, \varphi_i \epsilon Z_n$, set $\mathcal{FP}\beta_i = (\mathcal{P}uk_{iI}, \mathcal{P}uk_{iII}) = (\alpha_i.\mathcal{D}, \varphi_i.\mathcal{D} - _i .\varkappa.\mathcal{R})$, set $\alpha_i = \mathcal{P}k_i$, *and* $\mathcal{C}er_i = \varphi_i$. After this process, it inserts a tuple (ID_i, $\mathcal{FP}\beta_i$, , $\varkappa_i$) into LH_0 and (ID_i, $\mathcal{FP}\beta_i$, $\mathcal{P}k_i$, $\perp$, $\mathcal{C}er_i$) into CON^{list}. It also handover $\mathcal{FP}\beta_i$ *to* $\mathcal{A}_I$.

$\theta^{corrupt}$ ***Queries***: Upon receiving the query for the corruption of the private key of ID_i, ξ can search for a tuple (ID_i, $\mathcal{FP}\beta_i$, $\mathcal{P}k_i$, $\mathcal{C}er_i$) in CON^{list} and send $\mathcal{P}k_i$ to $\mathcal{A}_I$.

$\theta^{certificate}$ **Queries**: Upon receiving the query for the certificate of ID_i, ξ can search for a tuple (ID_i, $\mathcal{FP}\beta_i$, $\mathcal{P}k_i$, $\mathcal{C}er_i$) in CON^{list} and send $\mathcal{C}er_i$ to $\mathcal{A}_I$.

$\theta^{signcrypt}$ ***Queries:*** When $\mathcal{A}_I$ send the query with ID_i, if $ID_i = ID_r^*$ or $ID_i = ID_s^*$, then ξ terminate the game, otherwise, it checks the entry for ID_i and ID_r in CON^{list} and if such entry is not available previously, then it calls $\theta^{createcont}$ ***Queries***. Hence, utilizing the obtained information, ξ produced the signcrypted text ψ.

$\theta^{re-encrypt-key}$ **Queries**: When A_I submit two distinct identities (ID_i, ID_j), ξ can check the equality $ID_i = ID_\partial$, if this equality holds, then ξ destroyed further processing. Further, if it is not held, then ξ produce the private key $\mathcal{P}k_i$ and certificate $\mathcal{C}er_i$ of the identity ID_i. It also produces the public key $\mathcal{FP}\beta_j$ of identity of ID_j and send the output of Re Encryption Key Generations ($\mho$, ID_i, $\mathcal{P}k_i$, $\mathcal{C}er_i$, ID_j,$\mathcal{FP}\beta_j$) to $\mathcal{A}_I$

$\theta^{re-encryption}$ **Queries**: When A_I submit two distinct identities (ID_i, ID_j) and $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$, ξ can check the equality $\Upsilon \stackrel{?}{=} \mathcal{Z}.\mathcal{D}+h_3.\mathcal{FP}\beta_i$, if this equality fails, then ξ destroyed further processing. Otherwise, it performs the following steps:

- If $ID_i = ID_\partial$, it combs for the tuple (η, ID_i, FNi, m, h_1) in a list LH_1 such that $\Upsilon = h_1.\mathcal{D}$, $\mathcal{C} = (\eta, ID_i, FNi, m) \oplus h_2(\dagger.\mathcal{Q}_i)$, where $\mathcal{Q}_i = \mathcal{P}uk_{iI} + \mathcal{P}uk_{iII} + h_0(ID_i, \mathcal{FP}\beta_i)$. $\mathcal{R}$, and $\mathcal{Z} = h_1 - h_3.\mathcal{P}k_i$. If the aforementioned parameters are not available in LH_1 and LH_3, then ξ cannot respond for the asked query. Otherwise, ξ sets $\Upsilon^/ = h_1.\mathcal{RK}_{i\longmapsto j}$, $\mathcal{C}^/ = \mathcal{C}$, and send a tuple $\psi^/ = (\mathcal{C}^/, \Upsilon^/, \mathcal{Z})$ as a re-encrypted text to $\mathcal{A}_I$.
- Otherwise, it asked for the oracle $\theta^{re-encrypt-key}$ with two different identities (ID_i, ID_j), for to get re-encryption key $\mathcal{RK}_{i\longmapsto j}$, then it produces the final re-encrypted text and handover to $\mathcal{A}_I$.

Not that the *HCCDHP* solver algorithm ξ cannot accept the valid encrypted text, during the simulation of an $\theta^{re-encryption}$ oracle, if the probability is lesser then $\frac{Q_{renc}}{2^\pi}$.

$\theta^{decryption}$ **Queries**: When $\mathcal{A}_I$ submit query (ID_i, ψ_i), then ξ performs the following steps.

- If $ID_i = ID_\partial$ and ψ_i is the first level signcrypted text ($\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z}$), then ξ can check the equality $\Upsilon \stackrel{?}{=} \mathcal{Z}.\mathcal{D}+h_3.\mathcal{FP}\beta_i$ if this equality fails, then ξ destroyed further processing. Otherwise, it searches for a tuple (η, ID_i, m, h_1) in a list LH_1 such that $\Upsilon = h_1.\mathcal{D}$, $\mathcal{C} = (\eta, ID_i, m) \oplus h_2(\dagger.\mathcal{Q}_i)$, where $\mathcal{Q}_i = \mathcal{P}uk_{iI} + \mathcal{P}uk_{iII} + h_0(ID_i, \mathcal{FP}\beta_i)$. $\mathcal{R}$, and $\mathcal{Z} = h_1 - h_3.\mathcal{P}k_i$ and (η, ID_i, m) as a result of $\mathcal{A}_I$.
- If $ID_i = ID_\partial$ and $\psi_i^/$ is the re-encryption text ($\mathcal{C}^/, \Upsilon^/, \mathcal{Z}, $), it send a query for $\theta^{re-encrypt-key}$ with (ID_j, ID_i) to get a re-encryption key $\mathcal{RK}_{j\longmapsto i}$ and calculate $\Upsilon = \frac{\Upsilon^/}{\mathcal{RK}_{j\longmapsto i}}$. ξ combs for the tuple (η, ID_j, m, h_1) in a list LH_1 such that $\Upsilon = h_1.\mathcal{D}$, $\mathcal{C}^/ = (\eta, ID_j, m) \oplus h_2(\dagger.\mathcal{Q}_j)$, where $\mathcal{Q}_j = \mathcal{P}uk_{jI} + \mathcal{P}uk_{jII} + h_0(ID_j, \mathcal{FP}\beta_j)$. $\mathcal{R}$, and $\mathcal{Z} = h_1 - h_3.\mathcal{P}k_j$. If the aforementioned parameters are available in LH_1, then it sends a tuple (η, ID_j, m) as a decryption result to $\mathcal{A}_I$.
- If the above two steps have not happened, it recovers the plain text from the encrypted text in a normal method because of the private key $\mathcal{P}k_i$ and certificate $\mathcal{C}er_i$ is already known to it.

Not that the *HCCDHP* solver algorithm ξ cannot accept the valid encrypted text, during the simulation of an $\theta^{decryption}$ oracle, if the probability is lesser then $\frac{Q_{decr}}{2^\pi}$.

Challenge: The attacker $\mathcal{A}_1$ submits an identity ID_{chl} and two equal length but distinct plaintexts ($\mathfrak{M}_x$, $\mathfrak{M}_y$). The algorithm ξ check if $ID_{chl} \neq ID_\partial$, then it aborts further processing. Otherwise, it uniformly picks $\mathcal{C}\epsilon\{0, 1\}$, $\mathcal{Z}_{chl}$, $w^*\epsilon Z_n$, $\mathcal{C}_{chl}\epsilon\{0, 1\}^\gamma$, set $\Upsilon_{chl} = \Lambda.\mathcal{D}, \mathcal{W}_{chl} = \mathcal{Z}_{chl}.\mathcal{D} - w^*(\Lambda.\mathcal{D})$, include a tuple ($\Upsilon_{chl}$, $\mathcal{C}_{chl}$, $\mathcal{W}_{chl}$, w^*) to LH_3, and send $\psi_{chl} = (\Upsilon_{chl}, \mathcal{Z}_{chl}, W_{chl}, \mathcal{C}_{chl})$ as challenge ciphertext to $\mathcal{A}_I$. It is not difficult for the challenger to verify it by utilizing the followed equation $\Upsilon_{chl} \stackrel{?}{=} \mathcal{Z}_{chl}..\mathcal{D}+w^*(\nu.\mathcal{D})$.

Note that, here the process for recovering of the challenge signcrypted text ψ_{chl} is $\mathcal{C}_{chl} \oplus h_2\left(\left(\mathcal{P}k_\partial + \mathcal{C}er_\partial\right)\Upsilon_{chl}\right) = \mathcal{C} \oplus h_2\left(\left(\alpha_\partial + \delta_\partial + ßh_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}\right)$ and $\Lambda = \left(\eta^*, ID_\partial, FN\partial, \mathfrak{M}_\mathcal{Z}\right)$ where $\eta^*\epsilon\{0, 1\}^\gamma$.

Hence, $\mathcal{A}_I$ cannot decide on ψ_{chl} that it is a genuine ciphertext of $\mathfrak{M}_{\mathcal{Z}}$, since it produced a query $\hbar_1\left(\eta^*, \mathrm{ID}_\partial, \mathfrak{M}_{\mathcal{Z}}\right)$ or $\hbar_2\left((\alpha_\partial + \delta_\partial + ß\hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)\right).\Lambda.\mathcal{D})$.

Guess: In the guessing phase, ξ disregarded the bit $\mathcal{Z}'$ which is guess by $\mathcal{A}_I$. So, to calculate $ß.\Lambda.\mathcal{D}$, the output of ξ from CON^{list} is α_∂ and δ_∂ with ID_∂. The algorithm uniformly picks $(\mathcal{I}, \mathrm{h}_2)$ from LH_2 and determine the solution for *HCCDHP* as $\phi = \hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)^{-1}(\mathcal{I} - \alpha_\partial.\Lambda.\mathcal{D} - \delta_\partial.\Lambda.\mathcal{D})$. So, it is not hard to assume that $\phi = ß.\Lambda.\mathcal{D}$ if $\mathcal{I} = \left(\alpha_\partial + \delta_\partial + ß\hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}$.

Analysis: We define the following events, in which the algorithm ξ can get the solution of *HCCDHP*.

a) $\mathcal{EV}_\mathrm{a}$: During the execution, the algorithm ξ stops the game.
b) $\mathcal{EV}_\mathrm{b}$: Error occurred during the execution of $\theta^{\mathrm{re-encryption}}$ oracle.
c) $\mathcal{EV}_\mathrm{c}$: Error occurred during the execution of $\theta^{\mathrm{decryption}}$ oracle.
d) $\mathcal{EV}_\mathrm{d}$: When $\mathcal{A}_I$ makes a query to $\hbar_1$ oracle on $\left(\eta^*, ID_\partial, \mathfrak{M}_{\mathcal{Z}}\right)$.
e) $\mathcal{EV}_\mathrm{e}$: When $\mathcal{A}_I$ makes a query to $\hbar_2$ oracle on $\left(\left(\alpha_\partial + \delta_\partial + ß\hbar_0\left(\mathrm{ID}_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}\right)$.

Suppose $\mathcal{EV} = (\mathcal{EV}_\mathrm{b} \vee \mathcal{EV}_\mathrm{c} \vee \mathcal{EV}_\mathrm{d} \vee \mathcal{EV}_\mathrm{e}) \mid \neg\mathcal{EV}_\mathrm{a}$. Note that, if $\mathcal{EV}$ does not occur during the aforementioned simulation, then $\mathcal{A}_I$ advantage's for winning is not exceeded from $\frac{1}{2}$. So, we can get $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{Z}' = \mathcal{Z} \mid \neg\mathcal{EV}] \preceq \frac{1}{2}$.

So, by excruciating the probability, we require $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{Z}' = \mathcal{Z}] = \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{Z}' = \mathcal{Z} \mid \neg\mathcal{EV}]\,\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}] + \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{Z}' = \mathcal{Z} \mid \mathcal{EV}]\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}]$

$\preceq \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\neg\mathcal{EV}]/2 + \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}] = \frac{1}{2} + \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}]/2$.

Hence, in game 1 of IND-CBSRE-CCA2-I, according to the definition regarding the advantages of $\mathcal{A}_I$, we have

$\preceq 2[\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{Z}' = \mathcal{Z}] - 1/2 \mid \preceq \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}]$

$\preceq \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[(\mathcal{EV}_b \vee \mathcal{EV}_c \vee \mathcal{EV}_d \vee \mathcal{EV}_e) \mid \neg\mathcal{EV}_a]$

$\preceq (P_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[EV_b] \vee \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_c] \vee \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_d] \vee \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_e])/\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\neg\mathcal{EV}_a]$.

We apparently have that $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\neg\mathcal{EV}_a] = 1/\mathcal{Q}_{cc}$, $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_b] \preceq \frac{\mathcal{Q}_{renc}}{2^\pi}$, $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_c] \preceq \frac{\mathcal{Q}_{decr}}{2^\pi}$, *and* $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_d] \preceq \frac{\mathcal{Q}_1}{2^{\gamma+1}}$. *Thus, we can get* $\mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_e] \succeq \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\neg\mathcal{EV}_a]\varsigma - \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_b] - \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_c] - \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_d]$

$\succeq \frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}$.

Here, the solution for *HCCDHP* that if $\mathcal{EV}_\mathrm{e}$ occurred, then the algorithm ξ choose the correct values from LH_2. Hence, the obtained advantages of the algorithm ξ for solving *HCCDHP* as

$$\varsigma' \succeq \mathcal{P}_{\mathcal{r}_{\mathcal{O}\mathcal{B}}}[\mathcal{EV}_e]/\mathcal{Q}_2 \succeq 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right).$$

Lemma 2: Let a probabilistic polynomial-time attacker known to be type two $\mathcal{A}_{II}$ having the advantage ς to break IND-CBPSE-CCA2-II, the security of the proposed approach with the time τ and performing utmost $\mathcal{Q}_{\hbar i}$ hash queries where $\hbar i\,(i = 0, 1, 2, 3, 4)$, $\mathcal{Q}_{cc}$ create contestant queries to the oracle $\theta^{createcont}$, $\mathcal{Q}_{corp}$ corrupt queries to the oracle $\theta^{\mathrm{corrupt}}$, $\mathcal{Q}_{cert}$ certificate queries to the oracle $\theta^{\mathrm{certificate}}$, $\mathcal{Q}_{signc}$ signcryption queries to the oracle $\theta^{signcrypt}$, $\mathcal{Q}_{renk}$ re-encryption key queries to the oracle $\theta^{\mathrm{re-encrypt-key}}$, $\mathcal{Q}_{renc}$ re-encryption queries to the oracle $\theta^{\mathrm{re-encryption}}$, and $\mathcal{Q}_{decr}$ decryption queries to the oracle $\theta^{\mathrm{decryption}}$, then there exists an algorithm ξ which may able to solve *HCCDHP* problems for $\mathcal{A}_{II}$ with the following mentioned advantages:

$$\varsigma' = 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right)$$

Proof: Here we show that how the algorithm ξ will interact with $\mathcal{A}_{II}$ to solve *HCCDHP* from the given instance $(\mathcal{D}, ß.\mathcal{D}, \Lambda.\mathcal{D})$. So, ξ can interact with $\mathcal{A}_{II}$ by applying the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly from $(1 \preceq \partial \preceq \mathcal{Q}_{cc})$, Select $\mathscr{b} \epsilon \mathrm{Z_n}$ and compute $\mathcal{R} = \mathscr{b}.\mathcal{D}$ as a master public key. Compute $\mho = (\mathcal{HC}, \hbar_0, \hbar_1, \hbar_2, \hbar_3, \hbar_4, \mathrm{n} = 2^{80}, \mathrm{Z_n}, \mathcal{R})$ and published it to the network and provide $\mathscr{b}$ to $\mathcal{A}_{II}$.

The queries which can be used in this game are the same as in theorem 1, except the following.

$\theta^{\mathrm{createcont}}$ **Queries**: If $\mathcal{A}_{II}$ send a query with identity $\mathrm{ID_i}$ for the tuple $(\mathrm{ID_i}, \mathcal{FP}\beta_\mathrm{i}, \mathcal{P}\hbar_\mathrm{i}, \delta_\mathrm{i}, \mathcal{C}er_\mathrm{i})$, then ξ can do the following steps.

- At the event if ID_i is already available In the contestant list CON^{list}, then it returns $\mathcal{FP}\beta_\mathrm{i}$ to $\mathcal{A}_{II}$.
- When the $\mathrm{ID_i}$ is the ∂ dissimilar identity which is asked by $\mathcal{A}_{II}$, then it uniformly picks $\delta_\partial, h_\partial \epsilon Z_n$, sets $\mathcal{FP}\beta_\partial = (\delta_\partial.\mathcal{D}, ß.\mathcal{D})$ and $\mathcal{C}er_\partial = \delta_\partial + \mathscr{b}\mathrm{h}_\partial$ After this process, it inserts a new tuple $(\mathrm{ID}_\partial, \mathcal{FP}\beta_\partial, \delta_\partial, \mathcal{C}er_\partial, \perp)$ into CON^{list} and $(\mathrm{ID}_\partial, \mathcal{FP}\beta_\partial, \mathrm{h}_\partial)$ into LH_0. Note that $\mathcal{P}\hbar_\partial = ß$ and $\mathcal{A}_{II}$ will not know about ß.
- If the above two steps were not happening, it uniformly selects $\alpha_i, \delta_i, h_i \epsilon Z_n$, set $\mathcal{FP}\beta_\mathrm{i} = (\mathcal{P}u\hbar_{iI}, \mathcal{P}u\hbar_{iII}) = (\alpha_i.\mathcal{D}, \delta_i.\mathcal{D})$, set $\alpha_\mathrm{i} = \mathcal{P}\hbar_\mathrm{i}$, and $\mathcal{C}er_\mathrm{i} = \delta_i + \mathscr{b}\mathrm{h_i}$. After this process, it inserts a tuple $(ID_i, \mathcal{FP}\beta_i, , h_i)$ into LH_0 and $(ID_i, \mathcal{FP}\beta_i, \mathcal{P}\hbar_i, \delta_i, \mathcal{C}er_i)$ into CON^{list}. It also handover $\mathcal{FP}\beta_i$ *to* $\mathcal{A}_{II}$.

$\boldsymbol{\theta^{\mathrm{corrupt}}}$ **Queries**: Upon receiving the query for the corruption of the private key of ID_i, ξ can check the equality $ID_i = ID_\partial$, if this equality holds, then ξ destroyed further processing. Otherwise, it can search for a tuple $(ID_i, \mathcal{FP}\beta_i, \mathcal{P}\hbar_i, \mathcal{C}er_i)$ in CON^{list} and send $\mathcal{P}\hbar_i$ to $\mathcal{A}_{II}$.

Challenge: The attacker $\mathcal{A}_\mathrm{I}$ submits an identity ID_{chl} and two equal length but distinct plaintexts $(\mathfrak{M}_\mathrm{x}, \mathfrak{M}_\mathrm{y})$. The algorithm ξ check if $ID_{chl} \neq ID_\partial$, then it aborts further processing. Otherwise, it uniformly picks $\mathcal{Z} \epsilon \{0, 1\}$, $\mathcal{Z}_{chl}$, $\mathcal{w}^* \epsilon Z_n$, $\mathcal{C}_{chl} \epsilon \{0, 1\}^\gamma$, set $\Upsilon_\mathrm{chl} = \Lambda.\mathcal{D}$, $\mathcal{W}_{chl} = \mathcal{Z}_{chl}.\mathcal{D} - \mathcal{w}^*(\Lambda.\mathcal{D})$, include a tuple $(\Upsilon_\mathrm{chl}, \mathcal{C}_\mathrm{chl}, \mathcal{W}_\mathrm{chl}, \mathcal{w}^*)$ to $\mathrm{LH_3}$, and send $\psi_\mathrm{chl} = (\Upsilon_{chl}, \mathcal{Z}_{chl}, \mathcal{W}_{chl}, \mathcal{C}_{chl})$ as challenge ciphertext to $\mathcal{A}_\mathrm{I}$. It is not difficult for the challenger to verify it by utilizing the followed equation $\Upsilon_{chl} \stackrel{?}{=} \mathcal{Z}_{chl}..\mathcal{D} + \mathcal{w}^*(\nu.\mathcal{D})$.

Note that, here the process for recovering of the challenge signcrypted text ψ_{chl} is $\mathcal{C}_{chl} \oplus \hbar_2\left(\left(\mathcal{P}\hbar_\partial + \mathcal{C}er_\partial\right)\Upsilon_{chl}\right) = \mathcal{C} \oplus \hbar_2\left(\left(ß + \delta_\partial + \mathscr{b}\hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}\right)$ and $\Lambda = \left(\eta^*, ID_\partial, FN\partial, \mathfrak{M}_{\mathcal{Z}}\right)$ where $\eta^* \epsilon \{0, 1\}^\gamma$.

Hence, $\mathcal{A}_{II}$ cannot decide on ψ_{chl} that it is a genuine ciphertext of $\mathfrak{M}_{\mathcal{Q}}$, since it produced a query $\hbar_1\left(\eta^*, ID_\partial, FN\partial, \mathfrak{M}_{\mathcal{Q}}\right)$ or $\hbar_2((ß + \delta_\partial + \mathscr{b}\hbar_0\,(ID_\partial, \mathcal{FP}\beta_\partial))\,\Lambda.\mathcal{D})$.

Guess: In the guessing phase, ξ disregarded the bit $\mathcal{Q}'$ which is guess by $\mathcal{A}_{II}$. So, to calculate $ß.\Lambda.\mathcal{D}$, the output of ξ from CON^{list} is α_∂ and δ_∂ with ID_∂. The algorithm uniformly picks $(\mathcal{I}, \mathrm{h}_2)$ from LH_2 and determine the solution for *HCCDHP* as $\phi = \hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right)^{-1}(\mathcal{I} - \delta_\partial.\Lambda.\mathcal{D} - \mathscr{b}\hbar_0\left(ID_\partial, \mathcal{FP}\beta_\partial\right).\Lambda.\mathcal{D})$.

So, it is not hard to assume that $\phi = ß.\Lambda.\mathcal{D}$ if $\mathcal{I} = (ß + \delta_\partial + \mathscr{b}\hbar_0\,(ID_\partial, \mathcal{FP}\beta_\partial))\,\Lambda.\mathcal{D}$.

Analysis: We define the following events, in which the algorithm ξ can get the solution of *HCCDHP*.

f) $\mathcal{EV}_{\mathrm{a}}$: During the execution, the algorithm ξ stops the game.
g) $\mathcal{EV}_{\mathrm{b}}$: Error occurred during the execution of $\theta^{\mathrm{re-encryption}}$ oracle.
h) $\mathcal{EV}_{\mathrm{c}}$: Error occurred during the execution of $\theta^{\mathrm{decryption}}$ oracle.
i) $\mathcal{EV}_{\mathrm{d}}$: When $\mathcal{A}_{II}$ makes a query to $\hbar_1$ oracle on $\left(\eta^*, ID_\partial, \mathfrak{M}_{\mathcal{Q}}\right)$.
j) $\mathcal{EV}_{\mathrm{e}}$: When $\mathcal{A}_{II}$ makes a query to $\hbar_2$ oracle on $((ß + \delta_\partial + \mathscr{b}\hbar_0\,(ID_\partial, \mathcal{FP}\beta_\partial))\,\Lambda.\mathcal{D})$.

Suppose $\mathcal{EV} = (\mathcal{EV}_b \vee \mathcal{EV}_c \vee \mathcal{EV}_d \vee \mathcal{EV}_e) \mid \neg\mathcal{EV}_a$. Note that, if $\mathcal{EV}$ does not occur during the aforementioned simulation, then $\mathcal{A}_{II}$ advantage's for winning is not exceeded from $\frac{1}{2}$. So, we can get $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{Q}' = \mathcal{Q} \mid \neg\mathcal{EV}] \preceq \frac{1}{2}$.

So, by excruciating the probability, we require $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{Q}' = \mathcal{Q}] = \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{Q}' = \mathcal{Q} \mid \neg\mathcal{EV}]\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}] + \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{Q}' = \mathcal{Q} \mid \mathcal{EV}]\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}]$

$\preceq \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\neg\mathcal{EV}]/2 + \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}] = \frac{1}{2} + \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}]/2$.

Hence, in game 1 of IND-CBSRE-CCA2-II, according to the definition regarding the advantages of $\mathcal{A}_{II}$, we have

$$\begin{aligned}
&\preceq 2[\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{Q}' = \mathcal{Q}] - 1/2 \mid \preceq \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}] \\
&\preceq \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[(\mathcal{EV}_{\mathrm{b}} \vee \mathcal{EV}_{\mathrm{c}} \vee \mathcal{EV}_{\mathrm{d}} \vee \mathcal{EV}_{\mathrm{e}}) \mid \neg\mathcal{EV}_{\mathrm{a}}] \\
&\preceq (\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_{\mathrm{b}}] \vee \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_{\mathrm{c}}] \vee \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_{\mathrm{d}}] \\
&\quad \vee \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_{\mathrm{e}}])/\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\neg\mathcal{EV}_{\mathrm{a}}].
\end{aligned}$$

We apparently have that $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\neg\mathcal{EV}_a] = 1/\mathcal{Q}_{cc}$, $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_b] \preceq \frac{\mathcal{Q}_{renc}}{2^\pi}$, $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_c] \preceq \frac{\mathcal{Q}_{decr}}{2^\pi}$, *and* $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_d] \preceq \frac{\mathcal{Q}_1}{2^{\gamma+1}}$. *Thus, we can get* $\mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_e] \succeq \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\neg\mathcal{EV}_a]\varsigma - \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_b] - \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_c] - \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_d] \succeq \frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}$.

Here, the solution for *HCCDHP* that if $\mathcal{EV}_{\mathrm{e}}$ occurred, then the algorithm ξ choose the correct values from LH_2. Hence, the obtained advantages of the algorithm ξ for solving *HCCDHP* as

$$\varsigma' \succeq \mathcal{P}_{\mathcal{r}\mathscr{o}\mathscr{b}}[\mathcal{EV}_{\mathrm{e}}]/\mathcal{Q}_2 \succeq 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right).$$

Note that, the encryption is done through $\hbar_2(\dagger.\mathcal{Q}_{\mathrm{s}})$, this further needs the calculation of $\dagger$ from $\dagger = \hbar_1(\eta, ID_s, m)$. Here, computing both $\dagger$ needs η, which is infeasible for the adversary. So, from the above discussion, it is clear that our proposed scheme provides the following Corollary.

Corollary: if the adversary somehow obtains the private key of the sender in the proposed scheme, even still the confidentiality of the messages will be maintained which is called forward secrecy.

B. THEOREM UNFORGEABILITY

Unforgeability means that the forger (f_I and f_{II}) is infeasible to forge the original signature. We provide the following two Lemma's i.e., Lemma-III and Lemma-IV to prove this property.

Lemma 3: Let a probabilistic polynomial-time attacker known as type one f_I having the advantage ς to break the EUF-CBSRE-CMA-I, the security of the proposed technique with the time τ and performing utmost $\mathcal{Q}_{\hbar i}$ hash queries $\hbar i\,(i = 0, 1, 2, 3, 4)$, $\mathcal{Q}_{cc}$ create contestant queries to the oracle $\theta^{createcont}$, $\mathcal{Q}_{corp}$ corrupt queries to the oracle $\theta^{\mathrm{corrupt}}$, $\mathcal{Q}_{cert}$ certificate queries to the oracle $\theta^{\mathrm{certificate}}$, $\mathcal{Q}_{signc}$ signcryption queries to the oracle $\theta^{signcrypt}$, $\mathcal{Q}_{renk}$ re-encryption key queries to the oracle $\theta^{\mathrm{re-encrypt-key}}$, $\mathcal{Q}_{renc}$ re-encryption queries to the oracle $\theta^{\mathrm{re-encryption}}$, and $\mathcal{Q}_{decr}$ decryption queries to the oracle $\theta^{\mathrm{decryption}}$, then there exists an algorithm ξ which can solve the *HCCDHP* problems for f_I with the mentioned advantages below:

$$\varsigma' = 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right)$$

Proof: Here we are going to show that, how the algorithm ξ can interact with f_I to solve *HCCDHP* from the given instance $(\mathcal{D}, ß.\mathcal{D}, \Lambda.\mathcal{D})$. So, the ξ can interact with f_I by utilizing the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly from $(1 \preceq \partial \preceq \mathcal{Q}_{cc})$, Select $ß \epsilon \mathrm{Z_n}$ and compute $\mathcal{R} = ß.\mathcal{D}$ as a master public key. Compute $\mho = (\mathcal{HC}, \hbar_0, \hbar_1, \hbar_2, \hbar_3, \hbar_4, \mathrm{n} = 2^{80}, \mathrm{Z_n}, \mathcal{R})$, provide $\mathcal{R}$ and to f_I.

Training Phase: In this game, the same steps are performed for different queries oracles are the same as in theorem 1 of game IND-CBSRE-CCA2-I among f_I and ξ.

Forgery: At the end of the above process, f_I can make a signcrypted text $\psi = (\mathcal{C}, \Upsilon, \mathcal{W}, \mathcal{Z})$. Here, note that when f_I have the capacity to produce a valid signcrypted, then we can conclude that, ξ will also have the capacity of solving *HCCDHP* problems. Hence, by utilizing a forking lemma [], ξ will produce another signcrypted text $\psi^f = (\mathcal{C}, \Upsilon^f, \mathcal{W}^f, \mathcal{Z}^f)$. So, it leads us to the followed calculations.

$\mathcal{Z}.\mathcal{D} + = \mathcal{Z}^f.\mathcal{D} + \mathcal{G}^f.\,\mathcal{PP}\beta_{\mathrm{s}}^*$
$\mathcal{Z}.\mathcal{D} - \mathcal{Z}^f.\mathcal{D} = \mathcal{G}^f.\,\mathcal{PP}\beta_{\mathrm{s}}^* - \mathcal{G}.\mathcal{PP}\beta_{\mathrm{s}}^*$
$(\mathcal{Z} - \mathcal{Z}^f).\mathcal{D} = G^f.\,\mathcal{PP}\beta_{\mathrm{s}}^* - \mathcal{G}.\mathcal{PP}\beta_{\mathrm{s}}^*$
$(\mathcal{Z} - \mathcal{Z}^f).\mathcal{D} = (\mathcal{G}^f - \mathcal{G}).\mathcal{PP}\beta_{\mathrm{s}}^*$
$(\mathcal{Z} - \mathcal{Z}^f).\mathcal{D} = (\mathcal{G}^f - \mathcal{G}).\mathcal{P}\hbar_{\mathrm{s}}.\mathcal{D}^*$
$(\mathcal{Z} - \mathcal{Z}^f) = (\mathcal{G}^f - \mathcal{G}).\mathcal{P}\hbar_{\mathrm{s}}^*$

$\mathcal{P}\hbar_{\mathrm{s}}^* = \frac{\mathcal{Z} - \mathcal{Z}^f)}{(\mathcal{G}^f - \mathcal{G})} = ß.\Lambda.\mathcal{G} = \frac{(\mathcal{Z} - \mathcal{Z}^f)}{(\mathcal{G}^f - \mathcal{G})}$ is the solution for *HCCDHP*.

Analysis: We define the following events, in which the algorithm ξ can get the solution of *HCCDHP*.

a) $\mathcal{EV}_a$: During the execution, the algorithm ξ stops the game.
b) $\mathcal{EV}_b$: Error occurred during the execution of $\theta^{re-encryption}$ oracle.
c) $\mathcal{EV}_c$: Error occurred during the execution of $\theta^{decryption}$ oracle.
d) $\mathcal{EV}_d$: When f_I makes a query to $\hbar_1$ oracle on $\left(\eta^*, ID_\partial, \mathfrak{M}_\mathcal{Z}\right)$.
e) $\mathcal{EV}_e$: When f_I makes a query to $\hbar_2$ oracle on $\left(\left(\alpha_\partial + \delta_\partial + ß\hbar_0\left(\mathrm{ID}_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}\right)$.

Suppose $\mathcal{EV} = (\mathcal{EV}_b \vee \mathcal{EV}_c \vee \mathcal{EV}_d \vee \mathcal{EV}_e) \mid \neg\mathcal{EV}_a$. Note that, if $\mathcal{EV}$ does not occur during the aforementioned simulation, then f_I advantage's for winning is not exceeded from $\frac{1}{2}$.

We actually have that $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\neg\mathcal{EV}_a] = 1/\mathcal{Q}_{cc}$, $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_b] \preceq \frac{\mathcal{Q}_{renc}}{2^\pi}$, $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_c] \preceq \frac{\mathcal{Q}_{decr}}{2^\pi}$, and $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_d] \preceq \frac{\mathcal{Q}_1}{2^{\gamma+1}}$. Thus, we can get $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_e] \succeq \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\neg\mathcal{EV}_a]\varsigma - \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_b] - \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_c] - \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_d] \succeq \frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}$.

Here, the solution for *HCCDHP* that if $\mathcal{EV}_b$, $\mathcal{EV}_c$, $\mathcal{EV}_d$, and $\mathcal{EV}_e$ occurred, without errors. Hence, the obtained advantages of the algorithm ξ for solving *HCCDHP* as

$$\varsigma' \succeq \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_e]/\mathcal{Q}_2 \succeq 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right).$$

Lemma 4: Suppose a probabilistic polynomial-time attacker called type one f_{II} having the advantage ς to break EUF- CBSRE-CMA-I, the security of the proposed method with the time τ and carrying out utmost $\mathcal{Q}_{hi}$ hash queries $\hbar i\,(i = 0, 1, 2, 3, 4)$, $\mathcal{Q}_{cc}$ create contestant queries to the oracle $\theta^{createcont}$, $\mathcal{Q}_{corp}$ corrupt queries to the oracle θ^{corrupt}, $\mathcal{Q}_{cert}$ certificate queries to the oracle $\theta^{\text{certificate}}$, $\mathcal{Q}_{signc}$ signcryption queries to the oracle $\boldsymbol{\theta^{signcrypt}}$, $\mathcal{Q}_{renk}$ re-encryption key queries to the oracle $\theta^{\text{re-encrypt-key}}$, $\mathcal{Q}_{renc}$ re-encryption queries to the oracle $\theta^{\text{re-encryption}}$, and $\mathcal{Q}_{decr}$ decryption queries to the oracle $\theta^{\text{decryption}}$, then there exists an algorithm ξ which can solve the *HCCDHP* problems for f_{II} with the given advantages:

$$\varsigma' = 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right)$$

Proof: Here we are showing how the algorithm ξ can interact with f_{II} to solve *HCCDHP* from the given instance $(\mathcal{D}, ß.\mathcal{D}, \Lambda.\mathcal{D})$. So, the ξ can interact with f_{II} by utilizing the followed steps.

Setup: In this phase, ξ choose an index ∂ uniformly from $(1 \preceq \partial \preceq \mathcal{Q}_{cc}$ Select $\mathscr{b} \epsilon Z_n$ and compute $\mathcal{R} = \mathscr{b}.\mathcal{D}$ as a master public key. Compute $\mho$ and published it to the network and provide $\mathscr{b}$ to f_{II}.

Training Phase: in this game, the same steps are performed for different queries oracles are the same as in theorem 2 of game IND-CBSRE-CCA2-II among f_{II} and ξ.

Forgery: At the end of the above process, f_{II} can make a signcrypted text $\psi^f = (\mathcal{C}, \Upsilon^f, \mathcal{W}^f, \mathcal{Z}^f)$.Here, note that when f_{II} have the capacity to produce a valid signcrypted, then we can conclude that, ξ will also have the capacity of solving *HCCDHP* problems. Hence, by utilizing a forking lemma [], ξ will produce another signcrypted text $\psi^{ff} = (\mathcal{C}, \Upsilon^{ff}, \mathcal{W}^{ff}, \mathcal{Z}^{ff})$. So, it leads us to the followed calculations.

$\mathcal{Z}.\mathcal{D} + = \mathcal{Z}^{ff}.\mathcal{D} + \mathcal{G}^{ff}.\mathcal{PP}\beta_s^*$
$\mathcal{Z}.\mathcal{D} - \mathcal{Z}^{ff}.\mathcal{D} = \mathcal{G}^{ff}.\mathcal{PP}\beta_s^* - \mathcal{G}.\mathcal{PP}\beta_s^*$
$(\mathcal{Z} - \mathcal{Z}^{ff}).\mathcal{D} = \mathcal{G}^{ff}.\mathcal{PP}\beta_s^* - \mathcal{G}.\mathcal{PP}\beta_s^*$
$(\mathcal{Z} - \mathcal{Z}^{ff}).\mathcal{D} = (\mathcal{G}^{ff} - \mathcal{G}).\mathcal{PP}\beta_s^*$
$(\mathcal{Z} - \mathcal{Z}^{ff}).\mathcal{D} = (\mathcal{G}^{ff} - \mathcal{G}).\mathcal{P}\mathscr{k}_s.\mathcal{D}^*$
$(\mathcal{Z} - \mathcal{Z}^{ff}) = (\mathcal{G}^{ff} - \mathcal{G}).\mathcal{P}\mathscr{k}_s^*$
$ß.\Lambda.\mathcal{D} = \frac{(\mathcal{Z} - \mathcal{Z}^{ff})}{(\mathcal{G}^{ff} - \mathcal{G})}$ is the solution for *HCCDHP*.

Analysis: We define the following events, in which the algorithm ξ can get the solution of *HCCDHP*.

a) $\mathcal{EV}_a$: During the execution, the algorithm ξ stops the game.
b) $\mathcal{EV}_b$: Error occurred during the execution of $\theta^{\text{re-encryption}}$ oracle.
c) $\mathcal{EV}_c$: Error occurred during the execution of $\theta^{\text{decryption}}$ oracle.
d) $\mathcal{EV}_d$: When f_{II} makes a query to h_1 oracle on $\left(\eta^*, ID_\partial, \mathfrak{M}_\mathcal{Z}\right)$.
e) $\mathcal{EV}_e$: When f_{II} makes a query to $\hbar_2$ oracle on $\left(\left(ß + \delta_\partial + \mathscr{b}\hbar_0\left(\mathrm{ID}_\partial, \mathcal{FP}\beta_\partial\right)\right)\Lambda.\mathcal{D}\right)$.

Suppose $\mathcal{EV} = (\mathcal{EV}_b \vee \mathcal{EV}_c \vee \mathcal{EV}_d \vee \mathcal{EV}_e) \mid \neg\mathcal{EV}_a$. Note that, if $\mathcal{EV}$ does not occur during the aforementioned simulation, then f_{II} advantage's for winning is not exceeded from $\frac{1}{2}$.

We apparently have that $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\neg\mathcal{EV}_a] = 1/\mathcal{Q}_{cc}$, $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_b] \preceq \frac{\mathcal{Q}_{renc}}{2^\pi}$, $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_c] \preceq \frac{\mathcal{Q}_{decr}}{2^\pi}$, and $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_d] \preceq \frac{\mathcal{Q}_1}{2^{\gamma+1}}$. Thus, we can get $\mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_e] \succeq \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\neg\mathcal{EV}_a]\varsigma - \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_b] - \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_c] - \mathrm{P}_{\mathcal{R}\mathcal{O}ß}[\mathrm{EV}_d] \succeq \frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}$.

Here, the solution for *HCCDHP* that if $\mathcal{EV}_b$, $\mathcal{EV}_c$, $\mathcal{EV}_d$, and $\mathcal{EV}_e$ occurred, without errors. Hence, the obtained advantages of the algorithm ξ for solving *HCCDHP* as

$$\varsigma' \preceq \mathcal{P}_{\mathcal{R}\mathcal{O}ß}[\mathcal{EV}_e]/\mathcal{Q}_2 \succeq 1/\mathcal{Q}_2\left(\frac{\varsigma}{\mathcal{Q}_{cc}} - \frac{\mathcal{Q}_{renc}}{2^\pi} - \frac{\mathcal{Q}_{decr}}{2^\pi} - \frac{\mathcal{Q}_1}{2^{\gamma+1}}\right).$$

V. COMPARISON

A. COMPUTATIONAL COST

It is very important to find out the computational cost for the sender and receiver in terms of major operations used. Normally, the computational cost includes an expensive mathematical operation like elliptic curve point multiplication ($\mathfrak{E}\mathfrak{p}_\mathfrak{M}$), pairing operations ($\mathfrak{p}$), pairing-based point multiplication ($\mathfrak{p}_\mathfrak{M}\mathfrak{p}$), and hyperelliptic curve divisor multiplication ($\mathrm{h}\mathfrak{E}\mathrm{d}_\mathfrak{M}$) while designing a cryptographic algorithm. So, we compare our CBSRE scheme with Ahene *et al.* [56],

TABLE 3. Computational cost of major operations.

$\mathfrak{p}_\mathfrak{M}\mathfrak{p}$	$\mathfrak{E}\mathfrak{p}_\mathfrak{M}$	$\mathfrak{p}$	$\mathrm{h}\mathfrak{E}\mathrm{d}_\mathfrak{M}$
4.31ms	0.97ms	14.90ms	0.48ms

TABLE 4. Computational cost comparison on the basis of major operations.

Schemes	Signcryption	Proxy key generation	Re-encryption	Un-signcryption	Decryption	Total
Ahene et al. [56]	4 $\mathcal{E}p_M$	6 $\mathcal{E}p_M$		4 $\mathcal{E}p_M$	4$\mathcal{E}p_M$	18$\mathcal{E}p_M$
Ahene et al. [55]	1p+3 $p_M p$	2p+3 $p_M p$		1p+2 $p_M p$	1p+2 $p_M p$	5p+10 $p_M p$
Manzoor et al. [36]	3 $\mathcal{E}p_M$	1 $\mathcal{E}p_M$		2 $\mathcal{E}p_M$	3 $\mathcal{E}p_M$	9 $\mathcal{E}p_M$
Braeken et al. [19]-section b security mechanism	2 $\mathcal{E}p_M$	3 $\mathcal{E}p_M$	3 $\mathcal{E}p_M$	3 $\mathcal{E}p_M$	1$\mathcal{E}p_M$	12 $\mathcal{E}p_M$
Proposed	3 h$\mathcal{E}d_M$	2 h$\mathcal{E}d_M$		2 h$\mathcal{E}d_M$	3 h$\mathcal{E}d_M$	10 h$\mathcal{E}d_M$

TABLE 5. Computational cost comparison in ms.

Schemes	Signcryption	Proxy key generation	Re-encryption	Un-signcryption	Decryption	Total
Ahene et al. [56]	3.88	5.82		3.88	3.88	17.46
Ahene et al. [55]	27.83	42.73		23.52	23.52	117.6
Manzoor et al. [36]	2.91	0.97		1.94	2.91	8.73
Braeken et al. [19]	1.94	2.91	2.91	2.91	0.97	11.64
Proposed	1.44	0.96		0.96	1.44	4.8

Ahene *et al.* [55], Manzoor *et al.* [36], and Braeken *et al.* [19] based on the aforementioned major operations, which is shown in the following Table 3. Here we neglect the operations which require minimal time such division, subtraction, encryption, decryption, addition, and hashing. Further, in the following Table 5, we also provide a comparison in milliseconds (ms) by utilizing these aforementioned major operations. By observing the experiments performed in [31], [35], and [57]–[60] with the given system specifications.

- The hardware consisted Intel Core i74510UCPU
- 2.0 GHz processor with 8 GB of memory
- Operating system used Windows 7 Home Basic 64-bit
- Multi-precision Integer and Rational Arithmetic C Library (MIRACL) used for runtime basic operation.

According to [31], [35], and [58]–[60], a single pairing-based point multiplication ($p_M p$) will consume 4.31 milliseconds, pairing operations (p) will consume 14.90 milliseconds, single scaler point multiplication will take 0.97 ms and a hyperelliptic curve divisor multiplication (h$\mathcal{E}d_M$) will consume 0.48 as shown in Table 4. Thus, from Table 5, it is clear that the proposed CBSRE scheme requires minimal computational powers as compared to the existing. Furthermore, in Figure 4, a clear computational cost reduction is shown.

Note: Elliptic curve point multiplication ($\mathcal{E}p_M$) means the point multiplication in elliptic curve based schemes and pairing-based point multiplication ($p_M p$) means, the multiplication used in pairing-based schemes [31], [35], and [58]–[60].

Computation Cost Reduction of CBSRE From the Existing Scheme

The computational cost reduction can be calculated by using the following formula [58].

$$\left(\frac{Cost\ of\ existing\ scheme - Cost\ of\ \text{CBSRE}}{Cost\ of\ existing}\right) * 100$$

The computational cost reduction of the proposed CBSRE scheme from the existing schemes is followed.

- Reduction from Ahene *et al.* [56] is:

$$\left(\frac{18\mathcal{E}p_M - 10h\mathcal{E}d_M}{18\mathcal{E}p_M}\right) * 100 = \left(\frac{17.46 - 4.8}{17.46}\right) * 100 = 72.50\%$$

- Reduction from Ahene *et al.* [55] is:

$$\left(\frac{5p + 10p_M p - 10h\mathcal{E}d_M}{5p + 10p_M p}\right) * 100 = \left(\frac{117.64.8}{117.6}\right) * 100 = 95.91\%$$

- Reduction from Manzoor *et al.* [36] is:

$$\left(\frac{9\mathcal{E}p_M - 10\ h\mathcal{E}d_M}{9\mathcal{E}p_M}\right) * 100 = \left(\frac{8.734.8}{8.73}\right) * 100 = 45.01\%$$

- Reduction from Braeken *et al.* [19] is:

$$\left(\frac{12\mathcal{E}p_M - 10h\mathcal{E}d_M}{12\mathcal{E}p_M}\right) * 100 = \left(\frac{11.644.8}{11.64}\right) * 100 = 58.76\%$$

B. COMMUNICATION COST

For communication costs, we compare CBSRE with existence schemes, i.e., Ahene *et al.* [56], Ahene *et al.* [55], Manzoor *et al.* [36], and Braeken *et al.* [19]. For this

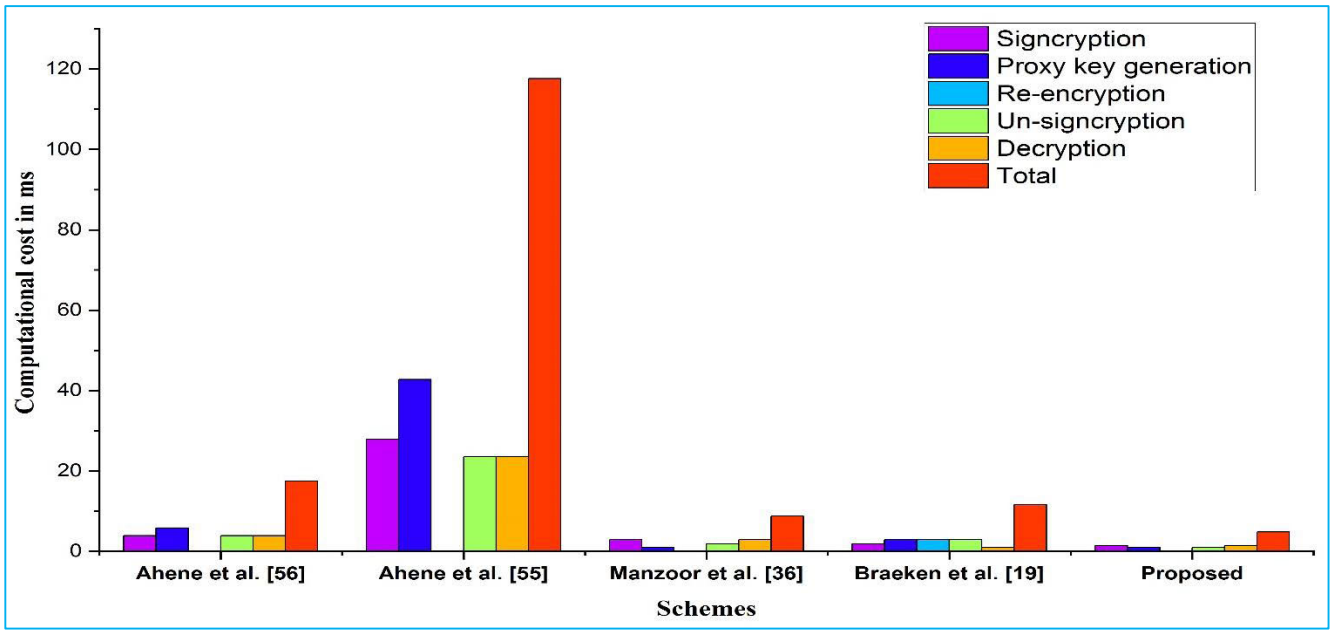


FIGURE 4. Computation cost comparison in millisecond.

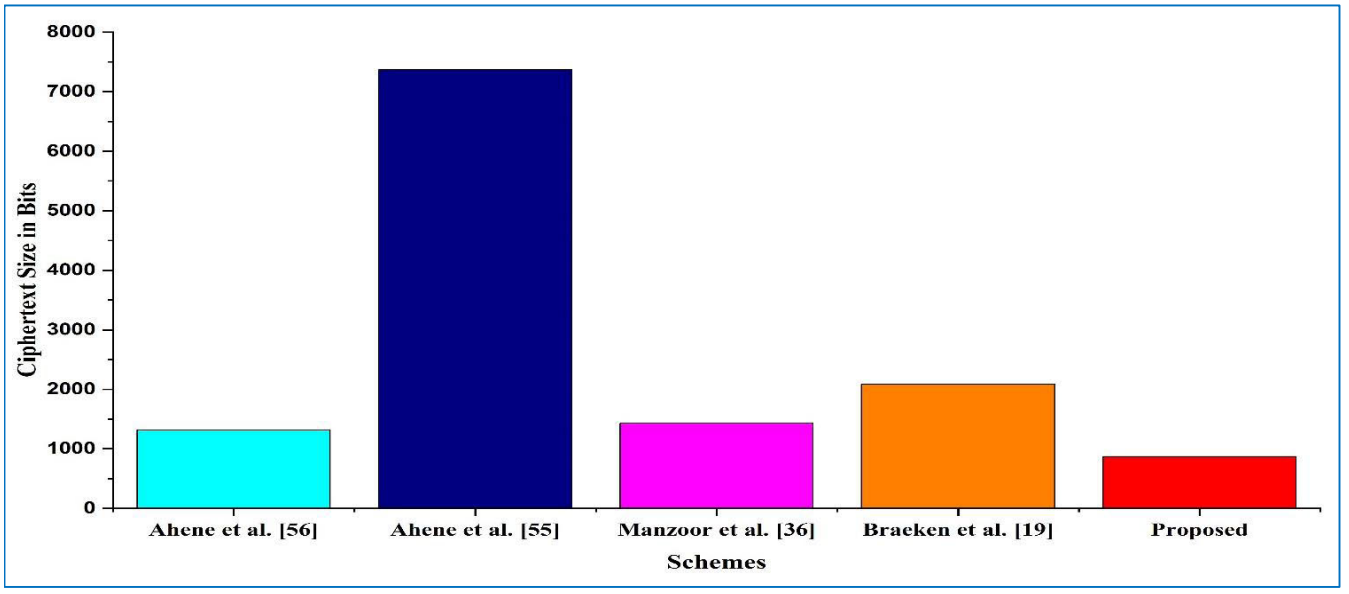


FIGURE 5. Communication cost comparison.

purpose, we suppose the length of elements in $|G1| = |G2| = |G| = 1024$ bits for BP, for ECC $|ϙ| = 160$ bits, HECC $= |\eta| = 80$ bits, $|m| = 100$ bits, $|H| = 256$ bits, and $|ID| = 80$ bits. Now according to our supposition, the communication cost for Ahene *et al.* [56] is $2|m| + 7|ϙ|$, for Ahene *et al.* [55] is $2|m| + 7|G|$, for Manzoor *et al.* [36] is $2|m| + 2|H| + 1|ID| + 4|ϙ|$, for Braeken *et al.* [19] is $2|m| + 3|H| + 6|ϙ| + 2|ID|$, and for the CBSRE is $2|m| + 2|H| + |\eta|$. From Table 6, it is clear that the proposed scheme is better in communicational cost than the previous ones that are Ahene *et al.* [56], Ahene *et al.* [55], Manzoor *et al.* [36], and Braeken *et al.* [19]. Furthermore, in Figure 5, the communicational cost reduction is also shown.

Communication Cost Reduction of CBSRE From the Existing Schemes:

The computational cost reduction of the proposed CBSRE scheme from the existing schemes is followed.

- Reduction from Ahene *et al.* [56]:

$$\left(\frac{7368-872}{7368}\right) * 100 = 88.16\%$$

TABLE 6. Communicational cost comparison in terms of ciphertext size.

Schemes	Computational cost	Size of Ciphertext
Ahene et al. [56]	$2\|m\|+7\|\varrho\|$	1320 bits
Ahene et al. [55]	$2\|m\|+7\|G\|$	7368 bits
Manzoor et al. [36]	$2\|m\|+2\|H\|+1\|ID\|+4\|\varrho\|$	1432 bits
Braeken et al. [19]	$2\|m\|+3\|H\|+6\|\varrho\|+2\|ID\|$	2088 bits
Proposed CBSRE	$2\|m\|+2\|H\|+\|\eta\|$	872 bits

- Reduction from Ahene *et al.* [55]:

$$\left(\frac{1320-872}{1320}\right)*100=33.93\%$$

- Reduction from Manzoor *et al.* [36] ais:

$$\left(\frac{1432-872}{1432}\right)*100=39.10\%$$

- Reduction from Braeken *et al.* [19] is:

$$\left(\frac{2088-872}{2088}\right)*100=58.23\%$$

VI. CONCLUSION

In this paper, we contribute a lightweight and formally secured certificate-based signcryption with proxy re-encryption (CBSRE) for the internet of things (IoT) enabled smart grid (SG) systems. The proposed scheme provides the security requirements of confidentiality (IND-CBSRE-CCA2-I and IND-CBSRE-CCA2-II), unforgeability (EUF-CBSRE-CMA-I and EUF-CBSRE-CMA-II) and forward secrecy. The comparison regarding computation and communication cost shows that the total computation cost of the proposed CBSRE scheme is 4.8 millisecond which reduced the computation cost from 72.50% of [56], 95.91% of [55], 45.01% of [36] and 58.76% of [19], while the total communication cost of the proposed CBSRE scheme is 872 bits which reduced the communication cost from 88.16% of [56], 33.93% of [55], 39.10% of [36] and 58.23% of [19] respectively. Thus, we can say that our scheme will be the best choice for the resource-hungry devices of the smart grid.

REFERENCES

[1] J. Corbett, K. Wardle, and C. Chen, "Toward a sustainable modern electricity grid: The effects of smart metering and program investments on demand-side management performance in the US electricity sector 2009-2012," *IEEE Trans. Eng. Manag.*, vol. 65, no. 2, pp. 252–263, May 2018.
[2] S. Ahmed, T. Muzaffar Gondal, M. Adil, S. Ahmad Malik, and R. Qureshi, "A survey on communication technologies in smart grid," in *Proc. IEEE PES GTD Grand Int. Conf. Expo. Asia (GTD Asia)*, Mar. 2019, pp. 7–12.
[3] C. Jiang and Y. Lu, "Research on IoT application and security risk analysis for smart grid," in *Proc. 5th IEEE Int. Conf. Cloud Comput. Intell. Syst. (CCIS)*, Nov. 2018, pp. 1003–1007.
[4] D. S. Terzi, B. Arslan, and S. Sagiroglu, "Smart grid security evaluation with a big data use case," in *Proc. IEEE 12th Int. Conf. Compat., Power Electron. Power Eng. (CPE-POWERENG)*, Apr. 2018, pp. 1–6.
[5] K. Ahuja and A. Khosla, "Data Analytics of IoT enabled smart energy meter in smart cities," in *Cloud Computing for Geospatial Big Data Analytics*, Springer, 2019, pp. 155–175.
[6] S. S. Reka and T. Dragicevic, "Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid," *Renew. Sustain. Energy Rev.*, vol. 91, pp. 90–108, Aug. 2018.
[7] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," in *Proc. Living Internet Things, Cybersecur. IoT*, 2018, p. 6
[8] S. Zahoor, N. Javaid, A. Khan, B. Ruqia, F. J. Muhammad, and M. Zahid, "A Cloud-Fog-Based smart grid model for efficient resource utilization," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 1154–1160.
[9] A. Waheed, J. Iqbal, N. Din, S. Ul, A. Iqbal, and N. Ul, "Improved cryptanalysis of provable certificateless generalized signcryption," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, pp. 1–7.
[10] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Gener. Comput. Syst.*, vol. 91, pp. 563–573, Feb. 2019.
[11] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu, and X. Du, "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1934–1944, Dec. 2017.
[12] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons, F. Ponci, and A. Monti, "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustain. Energy, Grids Netw.*, vol. 15, pp. 14–25, Sep. 2018.
[13] M. Kumar, H. K. Verma, and G. Sikka, "A secure lightweight signature based authentication for Cloud–IoT crowdsensing environments," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 4, p. e3292, Apr. 2019.
[14] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.
[15] 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.
[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1998, pp. 127–144.
[17] G. Ateniese and S. Hohenberger, "Proxy re-signatures: New definitions, algorithms, and applications," in *Proc. 12th ACM Conf. Comput. Commun. Secur. CS*, 2005, pp. 310–319.
[18] S. Chandrasekar, K. Ambika, and C. P. Rangan, "Signcryption with proxy re-encryption," *IACR Cryptol. ePrint Arch.*, vol. 2008, p. 276, 2008.
[19] 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.
[20] H. Yu and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *Comput. J.*, vol. 60, no. 8, pp. 1187–1196, Aug. 2017.
[21] Y. Lu and J. Li, "Provably secure certificate-based signcryption scheme without pairings," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 7, pp. 2554–2571, 2014.
[22] Y. Lu and J. Li, "A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds," *Future Gener. Comput. Syst.*, vol. 62, pp. 140–147, Sep. 2016.

[23] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2003, pp. 272–293.
[24] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, no. 8, p. 352, 2018.
[25] M. Yu, J. Zhang, J. Wang, J. Gao, T. Xu, R. Deng, Y. Zhang, and R. Yu, "Internet of Tings security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 12, Dec. 2018, Art. no. 155014771881584.
[26] 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.
[27] A. U. Rahman, I. Ullah, M. Naeem, R. Anwar, N.-U.-A., 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, pp. 160–167, 2018.
[28] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *Int. J. Adv. Stud. Sci. Res.*, vol. 3, no. 8, 2018.
[29] T. Wollinger, J. Pelzl, and C. Paar, "Cantor versus harley: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems," *IEEE Trans. Comput.*, vol. 54, no. 7, pp. 861–872, Jul. 2005.
[30] T. Wollinger, J. Pelzl, V. Wittelsberger, C. Paar, G. Saldamli, and Ç. K. Koç, "Elliptic and hyperelliptic curves on embedded," *ACM Trans. Embedded Comput. Syst.*, vol. 3, no. 3, pp. 509–533, Aug. 2004.
[31] 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, 2019.
[32] X. Fan, T. Wollinger, and G. Gong, "Efficient explicit formulae for genus 3 hyperelliptic curve cryptosystems over binary fields," *IET Inf. Secur.*, vol. 1, no. 2, p. 65, 2007.
[33] (2019). *Hyperelliptic Curve*. [Online]. Available: https://en.wikipedia.org/wiki/Hyperelliptic_curve
[34] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar, "Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Sep. 2003, pp. 351–365.
[35] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. U. Khanzada, and N. U. Amin, "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[36] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based proxy re-encryption scheme for secure IoT data sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 99–103.
[37] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[38] C. Sur, Y. Park, S. U. Shin, K. H. Rhee, and C. Seo, "Certificate-based proxy re-encryption for public cloud storage," in *Proc. 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2013, pp. 159–166.
[39] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proc. 14th ACM Conf. Comput. Commun. Secur. CCS*, 2007, pp. 185–194.
[40] H. K.-H. So, S. H. M. Kwok, E. Y. Lam, and K.-S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 321–326.
[41] J. Chen and Y. Y. Zhang, "The scheme of identity-based aggregation signcryption in smart grid," *Adv. Mater. Res.*, vols. 960–961, pp. 832–835, Jun. 2014.
[42] S. Alishahi, S. M. Seyyedi, M. H. Yaghmaee, and M. Alishahi, "Preserving integrity and privacy of data in smart grid communications," in *Proc. CIRED Workshop-Rome*, 2004, pp. 11–12.
[43] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attribute-based signcryption scheme to secure attribute-defined multicast communications," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.*, 2015, pp. 418–437.
[44] A. I. N. Umar and N. U. Amin, "A novel secure multicast communication in smart grid based on signcryption," *J. Appl. Env. Biol. Sci.*, vol. 6, no. 3S, pp. 127–133, 2016.
[45] J. Chen and X. Ren, "A privacy protection scheme based on certificateless aggregate signcryption and masking random number in smart grid," in *Proc. 4th Int. Conf. Mech. Mater. Manuf. Eng.*, 2016.
[46] C. Hu, J. Yu, X. Cheng, Z. Tian, and L. Sun, "CP_ABSC: An attribute-based signcryption scheme to secure multicast communications in smart grids," *Math. Found. Comput. Sci.*, vol. 1, no. 1, pp. 1–24, 2018.
[47] S. M. Sedaghat, M. H. Ameri, M. Delavar, J. Mohajeri, and M. R. Aref, "An efficient and secure attribute-based signcryp-tion scheme for smart grid applications," Cryptology ePrint Archive, Tech. Rep. 2018/263, 2018.
[48] C. Jin, G. Chen, C. Yu, J. Shan, J. Zhao, and Y. Jin, "An efficient heterogeneous signcryption for smart grid," *PLoS ONE*, vol. 13, no. 12, 2018, Art. no. e0208311.
[49] C. Wan, V. V. Phoha, B. Pei, and C. Chen, "Securing dynamic microgrid partition in the smart grid," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 5, May 2017, Art. no. 155014771771113.
[50] W. Baoyi, L. Li, Z. Shaomin, and H. Jing, "Research on privacy protection scheme based on certificateless aggregation signcryption in AMI," *Internet Things Eng. Appl.*, vol. 4, no. 1, pp. 7–12, 2019.
[51] W. Huige, W. Caifen, and C. Hao, "ID-based proxy re-signcryption scheme," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng.*, Jun. 2011, pp. 317–321.
[52] F. Li, B. Liu, and J. Hong, "An efficient signcryption for data access control in cloud computing," *Computing*, vol. 99, no. 5, pp. 465–479, May 2017.
[53] S. S. Rawat and G. K. Shrivastava, "Improved ID-based proxy re-signcryption scheme," in *Proc. 4th Int. Conf. Comput. Intell. Commun. Netw.*, Nov. 2012, pp. 730–733.
[54] Y. H. Wang and J. Y. Ye, "Research on ID-based proxy re-signcryption scheme," *Appl. Mech. Mater.*, vol. 685, pp. 663–666, Oct. 2014.
[55] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9722–9737, Dec. 2019.
[56] E. Ahene, J. Dai, H. Feng, and F. Li, "A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid," *Telecommun. Syst.*, vol. 70, no. 4, pp. 491–510, Apr. 2019.
[57] 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, Aug. 2017.
[58] I. Ullah, N. Amin, J. Khan, M. Rehan, M. Naeem, H. Khattak, S. Khattak, and H. Ali, "A novel provable secured signcryption scheme ????: A hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, 2019.
[59] I. Ullah, A. Alomari, N. Ul 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, 2019.
[60] 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, 2020.

SADDAM HUSSAIN received the bachelor's degree from Islamia College University, Peshawar, Pakistan, in 2017. He is currently pursuing the M.S. degree from Hazara University Mansehra, Pakistan. His major research domains are cryptography, network security, information centric networking (ICN), named data networking (NDN), smart grid, the Internet of Things (IoT), the Industrial Internet of Things (IIoT), and cloud computing.

INSAF ULLAH received the M.S. degree in computer sciences from the Department of Information Technology, Hazara University Manshera, Pakistan, where he is currently pursuing the Ph.D. degree in computer sciences. He is also serving as a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interest includes network security. He has published 23 articles in different journals and conferences.

HIZBULLAH KHATTAK received the Ph.D. degree from Hazara University Mansehra, Pakistan, in 2018. His major research domains are information-centric networking, networks security, mobile adhoc networks, the Internet of Things (IoT), IIoT, wireless sensor networks (WSN), wireless body area networks (WBAN), and cryptography.

MUHAMMAD ADNAN received the B.S. degree from the University of Peshawar, Peshawar, Pakistan, in 2006, the M.S. degree from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, in 2008, and the Ph.D. degree from Dongguk University, Seoul, South Korea, in 2016. He worked as a Lecturer in different public sector universities of Pakistan, from 2008 to 2012 and from 2016 to 2018. He held a post-doctoral position at the College of Information Technology, United Arab Emirates (UAE) University, United Arab Emirates. He is currently a Faculty Member at the Higher Colleges of Technology, Al Ain Men's College, United Arab Emirates. His research interests include wireless networks, resource management, energy efficiency, and the IoT for health care.

SARU KUMARI received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor with the Department of Mathematics, Chaudhary Charan Singh University, Meerut. She has published more than 160 research articles in reputed international journals and conferences, including 140 publications in SCI-Indexed Journals. Her current research interests include information security and applied cryptography. She is on the editorial board of more than a dozen of international journals, of high repute, under Elsevier, Springer, Wiley, and others including SCI journals, such as the *AEÜ—International Journal of Electronics and Communications* (SCI) (Elsevier), the *International Journal of Communication Systems* (SCI-E) (Wiley), *Telecommunication Systems* (SCI) (Springer), *Human-Centric Computing and Information Sciences* (SCI-E) (Springer), *Transactions on Emerging Telecommunications Technologies* (SCI-E) (Wiley), Information Technology and Control, Kaunas University of Technology, Lithuania (SCI-E), *KSII Transactions on Internet and Information Systems* (SCI-E), *Information Security Journal: A Global Perspective* (ESCI, Scopus) (Taylor & Francis), the International Journal of Wireless Information Networks (ESCI, Scopus) (Springer), and the *Journal of Reliable Intelligent Environments* (ESCI, Scopus) (Springer). She served as a lead/guest editor of four special issues in SCI journals of Elsevier, Springer, and Wiley. She is a technical program committee member for more than a dozen of international conferences. She is also serving as a reviewer of dozens of reputed journals, including SCI-Indexed of the IEEE, Elsevier, Springer, Wiley, and Taylor & Francis.

SYED SAJID ULLAH received the M.C.S. degree from Hazara University Mansehra, Pakistan, in 2017, where he is currently pursuing the M.S. degree. His major research domains are cryptography, network security, information centric networking (ICN), named data networking (NDN), and the IoT.

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 also serving as a Lecturer with the Department of Electrical Engineering, Hamdard University, Islamabad. His research interests include UAVs/drones with a focus on networks, platforms, security, as well as applications and services. He is a reviewer of various journals published by the IEEE, Elsevier, MDPI, and EURASIP.

SHAH JAHAN KHATTAK received the B.E. degree in electronics engineering from UET NED, Karachi, the M.S. degree in telecom engineering from UET Peshawar, and the Ph.D. degree in engineering management from Gomal University, Dera Ismail Khan. He has 26 years of experience in administration, planning, teaching, research, and operation. His research interests include network security, information centric networking (ICN), named data networking (NDN), the IoT, IIoT, and wireless sensor networks (WSN).