IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 4, 2021, accepted July 12, 2021, date of publication July 19, 2021, date of current version July 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3097403

An Anonymous Certificateless Signcryption Scheme for Internet of Health Things

INSAF ULLAH[1], ALI ALKHALIFAH[2], SAJJAD UR REHMAN[3], (Member, IEEE), NEERAJ KUMAR[4,5,6], (Senior Member, IEEE), AND MUHAMMAD ASGHAR KHAN[1]

[1]HIET, Hamdard University, Islamabad 44000, Pakistan
[2]Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia
[3]Department of Electrical Engineering, Namal Institute, Mainwali 42250, Pakistan
[4]Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala 147004, India
[5]Department of Computer Science and Information Engineering, Asia University, Taichung 413, Taiwan
[6]School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand 248007, India

Corresponding author: Muhammad Asghar Khan (khayyam2302@gmail.com)

This work was supported by the Deanship of Scientific Research, Qassim University.

ABSTRACT Internet of Health Things (IoHT) is a hot topic of research presently, which provides a reliable and intelligent healthcare system for monitoring the physical conditions of the patients over the Internet from anywhere and anytime. The ease of time-independent interaction from geographically remote areas is a core advantage of the IoHT system, which offers preventive or proactive healthcare facilities at a lower cost. IoHT communication, on the other hand, is usually carried out with a range of low-power biomedical sensors, rendering them vulnerable to cyber-attacks and incompatible with traditional cryptographic techniques. The most critical security concern in IoHT is ensuring the authenticity of patients' health-related messages sent over the internet. Other key concerns include receiver anonymity and forward security, which means that only the sender knows the identities of the recipients. As a result, even if the private key of senders compromised, the adversary will be unable to decrypt the ciphertext. Existing signcryption schemes that employ certificateless cryptography for the healthcare system failed to guarantee both receiver anonymity and forward security simultaneously. Therefore, in this article, we propose an anonymous certificateless signcryption scheme for IoHT applications, which is based on the notion of the Hyperelliptic Curve (HEC) cryptosystem to satisfy these security requirements. The proposed scheme guarantees formal security analysis for confidentiality, unforgeability, and receiver anonymity using the Random Oracle Model (ROM). The results authenticate that the proposed scheme improves security while lowering computation and communication costs.

INDEX TERMS Internet of things, IoHT, security, signcryption, hyperelliptic curve cryptosystem, random oracle model.

I. INTRODUCTION

The Internet of Health Things (IoHT) refers to the remote exchange of patient health-related information over the Internet, such as patient monitoring, treatment progress, observation, and consultation [1]. The health-related information of patients can be obtained using biomedical sensors and analyzed using user terminal devices like laptops, smartphones, smartwatches, or even a special embedded device in the IoHT framework [2]. It includes breathing rate, blood pressure, chest vibration, body temperature, respiratory rate, electrocardiogram (ECG), patient posture (accelerometer), and others [3]–[7]. IoHT can also be used to track environmental factors such as patient care venues, room status, laboratory shift times, treatment times, and staff-to-patient ratios in addition to medical applications [8]. As a result, this dynamic environment requires a stable yet adaptable connectivity, networking, and computing technology base. Short-range wireless technologies such as Bluetooth low energy (BLE), Wi-Fi, and Zigbee, among others, are used to link user terminal devices to a gateway node in the IoHT architecture. The BLE, on the other hand, makes use of good features including a modest data rate, low power consumption, and an unlicensed band, making it the best choice for linking wearable sensor nodes [9]. For high storage and intensive data processing, the gateway node can be linked to a (clinical)

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Khurram Khan.

server or cloud infrastructure through a Fifth-Generation (5G) wireless connection. Medical record can be stored as electronic health documents in a health information system and made accessible to medical providers when the patient leaves the hospital. Since the IoHT framework involves regular and continuous communications between biomedical sensors and mobile devices over an open wireless network, it poses a range of issues, the most serious of which is the security and privacy of patients' health-related information [10]. Furthermore, as data is transmitted more often via numerous biomedical devices and sensors, the risk of cyber-attacks is comparatively higher.

The primary security issue in delivering safe access in an IoHT environment is ensuring the validity of patient-transmitted health-related communications sent over an open wireless platform on the Internet. And then there is the issue of receiver anonymity, which means that only the sender knows about the identity of the recipients. Fortunately, such an impediment may be overcome by using a compound scheme known as anonymous signcryption [11]. By integrating encryption and authentication in one step, anonymous signcryption protects against malicious user attacks. To avoid the key escrow problem in the proposed compound scheme, a certificateless cryptosystem with anonymous signcryption may be used. In a certificateless cryptosystem, the Key Generation Center (KGC) has no prior knowledge of the participant's secret value, which is one of the key features to avoid the key escrow problem [12].

Conventional cryptographic techniques, such as Rivest-Shamir-Adleman (RSA), bilinear pairing, and elliptic curve cryptography, are commonly used to achieve security and efficiency in the security scheme [13]. However, these techniques come at a high cost in terms of computation and communication. The RSA cryptography, for example, employs a massive factorization with a key size of up to 1024 bits. Due to enormous pairing and map-to-point function computation, bilinear pairing is weaker than RSA. On the other hand, the elliptic curve can be used to overcome contradictions in RSA and bilinear pairing, which is a bit modern cryptography technique. With a key size of up to 160 bits, the ECC is used to provide security and performance. However, elliptic curve cryptography (ECC) is still incompatible in a resource-constrained environment, so a more advanced variant called hyperelliptic curve (HEC) can be used [14]. The use of an 80-bit key size is a positive aspect of HEC, as it guarantees the security features of elliptic curve, bilinear pairing, and RSA at the same time. As a result, the HEC is presented as a much superior option for IoHT. In order to adapt an anonymous certificateless signcryption scheme for use in the IoHT, the proposed scheme must meet the security requirements of confidentiality, unforgeability, and anonymity.

A. AUTHOR'S MOTIVATIONS AND CONTRIBUTIONS

This article is inspired by the above discussion and proposes a new scheme that is certificateless and built on the principle of HEC cryptography to address the issue of ensuring the authenticity of the transmitted message and receiver anonymity. The following excellent characteristics differentiate the major achievements of the undertaken research work:

- For an IoHT environment, an efficient cryptographic scheme, namely an anonymous certificateless signcryption scheme, has been provided.
- Through using the certificateless cryptography mechanism, the proposed scheme avoids the key escrow problem. In addition, for encryption and signature verification, the proposed scheme employs HEC cryptography.
- The proposed scheme guarantees confidentiality, unforgeability, and receiver anonymity on open wireless links under the Random Oracle Model (ROM) analysis.
- Finally, a comparison of the proposed scheme with related state-of-the-art schemes reveals that it is efficient, especially in terms of computational and communication costs.

B. STRUCTURE OF THE PAPER

The article is structured as follows. Related work is discussed in Section II. Preliminaries are explained in section III. System models are given in section IV. The proposed scheme can be seen in Section V. Formal security analysis using ROM is carried out in section V. Section VII presents performance comparison with existing schemes. Finally, section VIII contains the concluding remarks.

II. RELATED WORK

The scientific literature does not properly discuss the security and privacy problems solved by using the anonymous certificateless signcryption schemes in the IoHT. Therefore, it must be carefully investigated. Regardless of the devilish technique used, a well-designed security scheme will significantly reduce the risk of data being compromised. Li and Hong [15] proposed an efficient certificateless signcryption mechanism in 2016, which they then used to create a WBAN access control scheme. The scheme achieves confidentiality, integrity, authentication, non-repudiation, public verifiability, and ciphertext authenticity. The proposed scheme, on the other hand, is based on bilinear pairing, which comes at a high cost in terms of computation and communication. Li *et al.* [16] proposed a novel certificateless signcryption scheme in 2018, and then used the novel signcryption to design a cost-effective and anonymous access control scheme for WBANs. Anonymity, confidentiality, authentication, integrity, and nonrepudiation are all achieved by the proposed access control scheme. Since the proposed scheme depends on bilinear pairing once again, it is unsuitable for implementation over IoHT. In 2019, Gao *et al.* [17] suggested an efficient access control scheme for WBAN that included certificateless signcryption. The schemes' accuracy is shown by mathematical calculations. On the basis of the hardness of the Computational Diffie-Hellman (CDH) and Discrete Logarithm (DL) problems, the proposed scheme proved to provide anonymity and

unforgeability in the random oracle model. However, owing to the point multiplication operation, the scheme was not computationally efficient. In 2020, Gao *et al.* [17] suggested a certificateless signcryption scheme for wireless body area networks that was both efficient and practical. The scheme does not use bilinear pairing and is built solely on the widely used RSA cryptosystem. Since RSA, like bilinear pairing, is computationally expensive, it is not appropriate for IoHT. Finally, Liu *et al.* [18] introduced a secure pairing-free certificateless signcryption scheme for use in ubiquitous healthcare systems in 2021. The authors contrasted the proposed scheme's performance to that of other similar signcryption schemes. In a random oracle model, a formal security proof for indistinguishability against adaptive chosen ciphertext attack and unforgeability against adaptive chosen message attack is proposed for the scheme.

Security and privacy are the critical concern for the resource constrained devices [19]–[26]. The healthcare systems are generally equipped with the limited computational resources [27]–[29]. However, all of the above schemes rely on complex cryptographic methods, such as elliptic curves and bilinear pairing, and hence have high computation and communication costs. Therefore, these schemes are incompatible with IoHT systems, which typically have limited computational resources. The use of the state-of-the-art anonymous certificateless signcryption scheme is important for developing an efficient IoHT cryptographic scheme that needs less computing power. HEC cryptography, a more advanced variant of the elliptic curve, is the foundation of our proposed scheme. As compared to an elliptical curve, bilinear pairing, and modular exponential, it offers the same level of security with a smaller key dimension.

III. PRELIMINARIES

The hyper elliptic curve (HEC) is the generalized/ short key range form of ECC. As all know, in the elliptic curve, points are plagiaristic from a certain group. In HEC, from the divisor the additive Abelian group will calculate, which causes low parameter and key size compared to EC. So in this regard, compared to RSA and EC, the HEC can be a more suited technique for resource-poor environment. Let $\mathbb{f}id*$ is the algebraic closure $\mathbb{f}id$ which is the ultimate field. Suppose HEC of genus $\mathfrak{S} \geq 1$ over $\mathbb{f}id$ is shown as followed:

$$(\text{HEC}) : o^2 + (p)o = f(p) \text{ where } (\alpha, 0)\epsilon \mathbb{f}id \times \mathbb{f}id. \quad (1)$$

Further, a polynomial f(p) $\in (p)$ with degree $\mathfrak{S}$ and a monic one as f(p) $= \mathbb{f}id(p)$ with a degree $2\mathfrak{S} + 1$.

HECDP Problem: Suppose $\in \{1, 2, 3 \ldots, -1\}$ and $\delta, \mathcal{D}$ is the divisor from HEC. Let the $\mathcal{V} = \delta.$, and finding from this equation is called the HEC discrete logarithm problem (HECDP).

HCDH Problem: Suppose, $\mathcal{w} \in \{1, 2, 3, , -1\}$ and $\mathcal{D}$ is the divisor from HEC. Let the $\mathcal{N} = \delta.\mathcal{w}.\mathcal{D}$, and finding, from this equation is called the HEC computational defi-helman problem (HCDH).

The symbols used in the scheme are illustrated in Tab 1.

TABLE 1. Symbols used.

S.NO	Symbol	Descriptions
1	ξ	Input security parameter having size 80 bit
2	KGC	Key generation center
3	EUF-CMA	existential unforgeability against adaptive chosen-message attack
4	IND- CCA2	selected message adaptive chosen-ciphertext attack
5	ANON- CCA2	anonymous indistinguishability against selected identity adaptive chosen-ciphertext attack
6	Φ	freely identified set of parameters
7	HEC	Hyper elliptic curve
8	$\hbar_1, \hbar_2, \hbar_3, \hbar_4$	One-way Hash functions
9	$\mathcal{G}$	Genus of Hyper elliptic curve having degree $\mathcal{G} \geq 2$
10	$\mathcal{U}_p$	A finite field of order $p \geq 2^{80}$
11	η	Represents the master secret key of KGC
12	$\mathcal{Q}$	Represents the master public key of KGC
13	$\mathcal{D}$	Represents the of Hyper elliptic curve
14	$\mho$	A user with $\text{ID}_{\mho}$
15	ID_s, ID_r	Identity of sender and receiver
16	$\Upsilon_{\mho}$	secret number for a user with $\text{ID}_{\mho}$
17	$\mathcal{P}_{\mho}$	Partial private key for a user with $\text{ID}_{\mho}$
18	$\mathcal{PBK}_s, \mathcal{PBK}_r$	Sender and receiver public key
19	$\mathcal{PK}_s, \mathcal{PK}_r$	Sender and receiver private key
20	$\mathcal{M}$ and $\mathcal{C}$	Represents plaintext and Ciphertext
21	Ψ	Represents signcryption text
22	$\perp$	Null

IV. SYSTEM MODEL

A. NETWORK MODEL

As shown in Fig. 1, IoHT can be used in a variety of settings, depending on the requirements. Depending on the patient's illness, the necessary gadgets are generally included in the medical sensors. The sensors can be linked to the gateway router using short-range radio transceivers (i.e., BLE). The BLE operates on the 2.4 GHz frequency band. There are good reasons to choose this technology standard. They operate in the unlicensed spectrum, for example, and have decent data rates while using relatively minimal power. The out-of-clinic patients will use a smartphone or smartwatch, which is equipped with software programs (apps) and peripheral hardware. These apps allow for the automatic collection and storage of patient information in personalized

profiles. These devices provide the data in a variety of visual ways, such as graphs that show patterns over time and frequently contain explanations of optimal ranges for a particular health measure. The aggregated data from the patient tracking sensors may be too large for the local server to accommodate. It necessitates a high level of storage and computational capability. Fortunately, the new fifth-generation (5G) mobile networking infrastructure has a multiaccess edge computing (MEC) facility. As MEC is implemented into an IoHT system, it has high capacity and intensive processing capabilities.

B. THREAT MODEL

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

We also supposed to divides the role of adversary into two ways that are $\mathcal{A}_1$ and $\mathcal{A}_2$, which can be harmfull for our scheme during communication regarding to destroyed the security of confidentiality, unforgeability, receiver anonymity, and forward security, respectively. here, we represent $\mathcal{A}_1$ is an outsider attacker which has not the ability to get access to the master secret key of KGC without replacing the user public key and still struggling to break the security of confidentiality, unforgeability and receiver anonymity. Here, $\mathcal{A}_2$ is an insider attacker which has the ability to get access to the master secret key of KGC and still struggling to break the security of confidentiality, unforgeability and receiver anonymity. The specific security models under different adversaries as same as: such that confidentiality regarding selected message adaptive chosen-ciphertext attack (IND- CCA2-game). This game can be split into two parts e.g. (1) $\mathcal{A}_1$ try to break the confidentiality of a message (IND-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$ (2)$\mathcal{A}_2$ try to break the confidentiality of a message (IND-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$ without replacing the user public key.

Unforgeability regarding existential unforgeability against adaptive chosen-message attack (EUF-CMA-game), this game can be split into two parts e.g. (1) $\mathcal{A}_1$ can try to forge signature and communicate for this purpose with the challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$ (2)$\mathcal{A}_2$ try to forge signature and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$ without replacing the user public key.

Anonymity regarding anonymous indistinguishability against selected identity adaptive chosen-ciphertext attack (ANON- CCA2-game), this game can be split into two parts e.g. (1) $\mathcal{A}_1$ try to break the anonymity and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$ (2) $\mathcal{A}_2$ try to break the anonymity and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$ without replacing the user public key.

Forward security can be achieved, when the private key is accessed by $\mathcal{A}_1$ or $\mathcal{A}_2$ but the confidentiality is still exist.

V. PROPOSED SCHEME

A. DEFINITION OF THE PROPOSED SCHEME

i. *Setup:* Considering a security input ξ, KGC creates freely identified set of parameters (Φ) and a master secret key (η).
ii. *Partial Private Key Generation (PPG):* Given η, Φ, $\text{ID}_{\mho}$, and $\mathcal{T}_{\mho}$, KGC results $\mathcal{P}_{\mho}$ as a partial private key for $\mho$ with $\text{ID}_{\mho}$.
iii. *Secret Number Generation (SNG):* Considering Φ and $\text{ID}_{\mho}$ as an input, a user ($\mho$) with $\text{ID}_{\mho}$ picks his secret number $\Omega_{\mho}$ and saves it privately.
iv. *Private Key Generation (PKG):* It takes a secret number $\Omega_{\mho}$, and $\mathcal{P}_{\mho}$ as input, and produced a private key $\mathcal{PK}_{\mho}$.
v. *Public Key Generation (PUBKG):* It takes a secret number $\Omega_{\mho}$, freely identified set of parameters (Φ), a user private key $\mathcal{PK}_{\mho}$ as an input and produced a public key $\mathcal{PBK}_{\mho}$.
vi. *Certificateless Signcryption Generation (CSG):* It takes a plaintext $\mathscr{M}$, Φ, $\mathcal{PBK}_{\text{s}}$, $\mathcal{PBK}_{\text{r}}$, and $\mathcal{PK}_{\text{s}}$ as an input and returns Ψ as a certificateless signcryption text.
vii. *Certificateless Un-Signcryption (CUNS):* It takes Ψ, Φ, $\mathcal{PK}_{\text{r}}$, $\mathcal{PBK}_{\text{s}}$, and $\mathcal{PBK}_{\text{r}}$ as an input, it checks the correctness of Ψ, if it is genuine then it outputs $\mathscr{M}$; otherwise $\perp$.

B. PROPOSED ALGORITHM

In this phase, we explain the new scheme construction steps:

Setup: Considering a security input ξ, KGC creates freely identified set of parameters $\Phi = \{\hbar_1, \hbar_2, \hbar_3, \hbar_4\, \mathbb{hEc}, \mathcal{G} \succeq 2, \mathcal{G}_p, \mathcal{D}, \mathcal{Q} = \eta.\mathcal{D}\}$, where $\hbar$ is an irreversible hash function, $\mathbb{hEc}$ is the genus 2 hyper elliptic curve, $\mathcal{G} \succeq 2$ is the genus of $\mathbb{hEc}$, $\mathcal{U}_p$ is a finite field of order $p \succeq 2^{80}$, $\mathcal{D}$ is the divisor of $\mathbb{hEc}$, $\mathcal{Q} = \eta.\mathcal{D}$ is the master public key, and

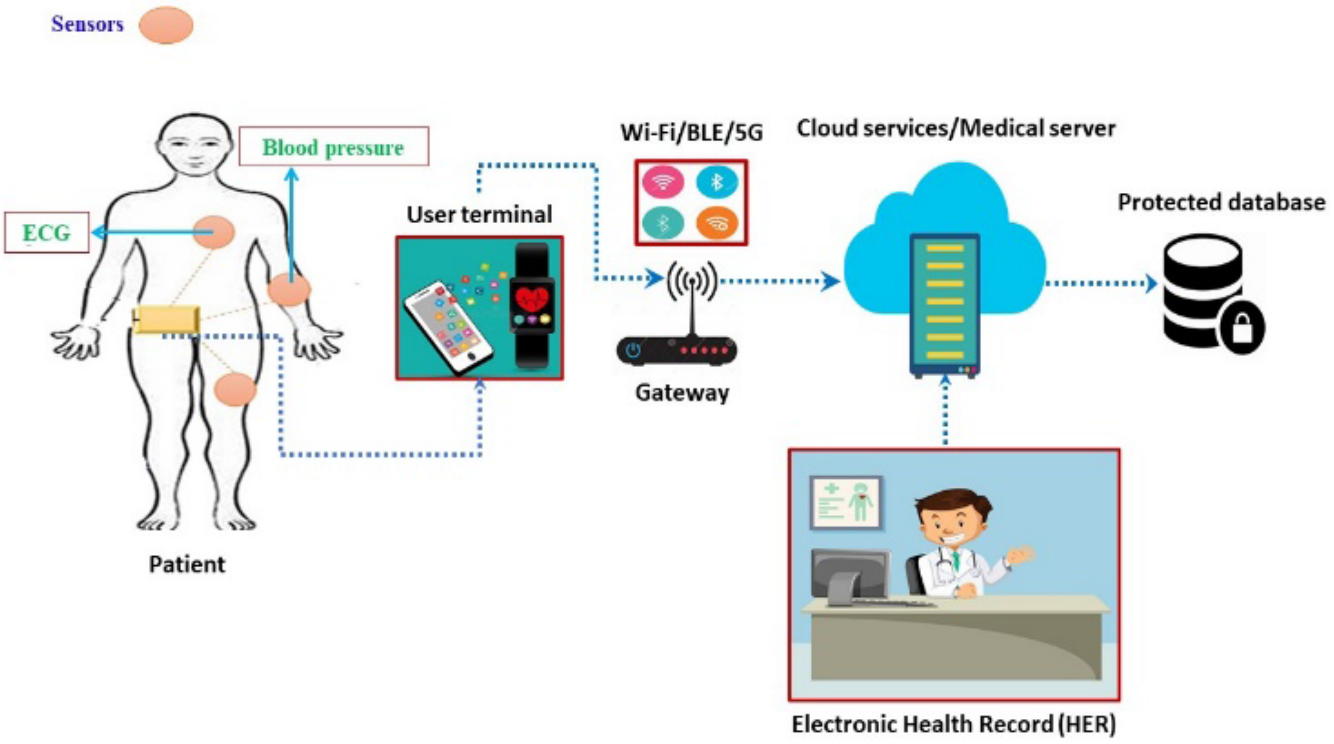


FIGURE 1. Proposed network model.

$\eta \in \{1, 2, \ldots\ldots, p-1\}$ is the master secret key, respectively. Then, KGC keep private η and get freely available the set of parameters Φ in a network.

Secret Number Generation (SNG): A user ($\mho$) with $\mathrm{ID}_{\mho}$, figures a public value $\mathrm{T}_{\mho}$ utilizing Φ as followed:

- It selects a secret number $\Upsilon_{\mho} \in \{1, 2, \ldots\ldots, p-1\}$ and compute $\mathcal{T}_{\mho} = \Upsilon_{\mho}\mathcal{D}$
- And sends a tuple $(\mathrm{ID}_{\mho}, \mathcal{T}_{\mho})$ to KGC, as a request for partial private key.

Partial Private Key Generation (PPG): Given η, Φ, $\mathrm{ID}_{\mho}$, and $\mathcal{T}_{\mho}$, KGC results $\mathcal{P}_{\mho}$ as a partial private key for $\mho$ with $\mathrm{ID}_{\mho}$ and the process as followed:

- Selects $\gamma_{\mho} \in \{1, 2, \ldots\ldots, p-1\}$ and Computes $\beta_{\mho} = \gamma_{\mho}\mathcal{D}$
- Compute $\mathrm{X}_{\mho} = \hbar_1(\mathrm{ID}_{\mho}, \beta_{\mho}, \mathcal{T}_{\mho})$ and $\mathcal{PBK}_{\mho} = \mathrm{X}_{\mho}.\mathcal{T}_{\mho} + \beta_{\mho}$
- Calculate $\varphi_{\mho} = \hbar_2(\mathrm{ID}_{\mho}, \mathcal{PBK}_{\mho})$ and $\mathcal{P}_{\mho} = \gamma_{\mho} + \varphi_{\mho}.\eta$
- Send the tuple $(\beta_{\mho}, \mathcal{P}_{\mho})$ to the user ($\mho$) with $\mathrm{ID}_{\mho}$ using secure channel

User Key Generation (UKG): Upon receiving $((\beta_{\mho}, \mathcal{P}_{\mho}))$, it takes a secret number $\Upsilon_{\mho}$, freely identified set of parameters (Φ), a user identity $\mathrm{ID}_{\mho}$ as an input and produced a public key $\mathcal{PBK}_{\mho}$ and private key $\mathcal{PK}_{\mho}$ by using the following steps:

- Verify the tuple $(\beta_{\mho}, \mathcal{P}_{\mho})$ as $\mathcal{P}_{\mho}.\mathcal{D} = \beta_{\mho} + \hbar_2(\mathrm{ID}_{\mho}, \mathcal{PBK}_{\mho}).\ \mathcal{Q}$
- Compute $\mathrm{X}_{\mho} = \hbar_1(\mathrm{ID}_{\mho}, \beta_{\mho}, \mathcal{T}_{\mho})$ and $\mathcal{PBK}_{\mho} = \mathrm{X}_{\mho}.\mathcal{T}_{\mho} + \beta_{\mho}$
- Calculate $\mathcal{PK}_{\mho} = \mathrm{X}_{\mho}.\Upsilon_{\mho} + \mathcal{P}_{\mho}$
- Set $\mathcal{PK}_{\mho}$ as a private key and send $\mathcal{PBK}_{\mho}$ as a public key for publishing

Certificateless Signcryption Generation (CSG): It takes a plaintext $\mathcal{M}$, Φ, $\mathcal{PBK}_{\mathrm{s}}$, $\mathcal{PBK}_{\mathrm{r}}$, and $\mathcal{PK}_{\mathrm{s}}$ as an input and returns Ψ as a certificateless signcryption text utilizing the below process.

- Selects $a \in \{1, 2, \ldots\ldots, p-1\}$ and Computes $\mathcal{U} = a.\mathcal{D}$
- Calculate $\varphi_{\mathrm{r}} = \hbar_2(\mathrm{ID}_{\mathrm{r}}, \mathcal{PBK}_{\mathrm{r}})$ and $\delta_{\mathrm{r}} = a.(\mathcal{PBK}_{\mathrm{r}} + \varphi_{\mathrm{r}}.\mathrm{Q})$
- Compute $\mathcal{K}_{\mathrm{r}} = \hbar_3(\mathrm{ID}_{\mathrm{r}}, \delta_{\mathrm{r}}, \mathcal{U})$ and $\mathcal{C} = \mathcal{E}_{\mathcal{K}_{\mathrm{r}}}(\mathcal{M}, \mathcal{U})$
- Compute $r = \hbar_4(\mathrm{ID}_{\mathrm{s}}, \mathcal{C}, \mathcal{U})$ and $\mathcal{W} = a - r.\mathcal{PK}_{\mathrm{s}}$
- Set $\Psi = (\mathcal{C}, r, \mathcal{W})$ and return it to the receiver

Certificateless Un-Signcryption (CUNS): It takes Ψ, Φ, $\mathcal{PK}_{\mathrm{r}}$, $\mathcal{PBK}_{\mathrm{s}}$, and $\mathcal{PBK}_{\mathrm{r}}$ as an input, it checks the correctness of Ψ, if it is genuine then it outputs $\mathcal{M}$; otherwise $\perp$. The process is followed:

- Calculate $\varphi_{\mathrm{s}} = \hbar_2(\mathrm{ID}_{\mathrm{s}}, \mathcal{PBK}_{\mathrm{s}})$ and $\mathcal{U} = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_{\mathrm{s}} + \varphi_{\mathrm{s}}.\mathcal{Q})$
- Calculate $r^{/} = \hbar_4(\mathrm{ID}_{\mathrm{s}}, \mathcal{C}, \mathcal{U})$ and compare if $r^{/} = r$, then accept Ψ otherwise returns $\perp$
- Compute $\delta_{\mathrm{r}} = \mathcal{PK}_{\mathrm{r}}.\mathcal{U}$ and $\mathcal{K}_{\mathrm{r}} = \hbar_3(\mathrm{ID}_{\mathrm{r}}, \delta_{\mathrm{r}}, \mathcal{U})$
- Finally, recovered the plaintext as $(\mathcal{M}, \mathcal{U}) = \mathcal{D}_{\mathcal{K}_{\mathrm{r}}}(\mathcal{C})$

C. CORRECTNESS

Evidently, for each user ($\mho$) with $\mathrm{ID}_{\mho}$, it has $\mathcal{PK}_{\mho}.\mathcal{D} = \mathcal{PBK}_{\mho} + \varphi_{\mho}.\mathcal{Q}$.

So, $\mathcal{U} = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_{\mathrm{s}} + \varphi_{\mathrm{s}}.\mathcal{Q} = (a - r.\mathcal{PK}_{\mathrm{s}}).\ \mathcal{D} + r.\mathcal{PK}_{\mathrm{s}}.\mathcal{D})$

$$= a.\mathcal{D} - r.\mathcal{PK}_s.\mathcal{D} + r.\mathcal{PK}_s.\mathcal{D} = a.\mathcal{D} = \mathcal{U},$$

$$\delta_r = a.(\mathcal{PBK}_r + \varphi_r.\mathcal{Q}) = a.(\mathcal{PK}_r.\mathcal{D}) = a.\mathcal{D}\,(\mathcal{PK}_r)$$
$$= \mathcal{U}.\mathcal{PK}_r = \delta_r$$

VI. SECURITY ANALYSIS

Here, we provide the security proofs for our scheme on the basis of random oracle model. It includes the six games, which are explained in the following theorems.

Theorem 1: In this theorem, $\mathcal{A}_1$ try to break the confidentiality of a message (IND-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{HCDH}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{HCDH}$ is to calculate the HCDH problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$.

Proof: Suppose a triple $\{\mathcal{D}, X\mathcal{D}, \Upsilon\mathcal{D}\}$ is the given instance of HCDH problem, then in the following steps we provide that how the challenger $\mathcal{C}_{HCDH}$ interacts with $\mathcal{A}_1$ for getting the solution of HCDH problem.

Setup: Here, $\mathcal{C}_{HCDH}$ sets the master secret $\eta = \perp$ and master public key as $\mathcal{Q} = \eta.\mathcal{D}$, then it handovers the freely identified set of parameters Φ to $\mathcal{A}_1$.

Phase A: In this phase, $\mathcal{A}_1$ creates four lists (list$^{i=1,2,3,4}$), which are initially empty, then it selects the sender and receiver target identity ($ID_s{}^t$, $ID_r{}^t$) and sends them $\mathcal{C}_{HCDH}$. So, the hash queries can be performing in the following manner.

$\hbar_i$ *Query:* When $\mathcal{A}_1$ submits hash queries ($\hbar_{i=1,2,3,4}$), then $\mathcal{C}_{HCDH}$ check the values in list$^{i=1,2,3,4}$ for these queries, if it is found then handovers to $\mathcal{A}_1$, otherwise it selects the values e.g., $r_{\mathcal{A}}$, r_b, $r_{\mathcal{C}}$, and r_d and returns it to $\mathcal{A}_1$. $\mathcal{C}_{HCDH}$ also updates the lists list$^{i=1,2,3,4}$ with $r_{\mathcal{A}}$, r_b, $r_{\mathcal{C}}$, and r_d, respectively.

Phase B: In this phase, $\mathcal{A}_1$ made some query with $\mathcal{C}_{HCDH}$. Here, $\mathcal{C}_{HCDH}$ create a list (list$^{\mho}$), so the queries can be performing in the following manner.

Public Key Extract Query(**Q_{pkeq}**) : On input $ID_\mho$, $\mathcal{C}_{HCDH}$ combs for a tuple ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho, \mathcal{PBK}_\mho$), if it is existing in list$^{\mho}$, then it sends $\mathcal{PBK}_\mho$ to $\mathcal{A}_1$. Otherwise, $\mathcal{C}_{HCDH}$ perform the below steps:

- If $ID_\mho = ID_r{}^t$, $\mathcal{C}_{HCDH}$ picks $\gamma_\mho, \propto_\mho, X_\mho, \varphi_\mho \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_\mho = \gamma_\mho.\mathcal{D}, \mathcal{T}_\mho = X_\mho{}^{-1}(\Upsilon + \propto_\mho \mathcal{D} - \beta_\mho - \varphi_\mho.\mathcal{Q})$, $\mathcal{PBK}_\mho = X_\mho.\mathcal{T}_\mho + \beta_\mho$, and sets $\mathcal{PK}_\mho = \perp$.
- If $ID_\mho = ID_s{}^t$, $\mathcal{C}_{HCDH}$ picks $\gamma_\mho, \propto_\mho, X_\mho, \varphi_\mho \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_\mho = \gamma_\mho.\mathcal{D}, \mathcal{T}_\mho = \Upsilon_\mho.\mathcal{D}$, $\mathcal{PBK}_\mho = X_\mho.\mathcal{T}_\mho + \beta_\mho$, and sets $\mathcal{PK}_\mho = \perp$ and $\propto_\mho = \Upsilon_\mho$.
- Otherwise, $\mathcal{C}_{HCDH}$ picks $\gamma_\mho, \propto_\mho, X_\mho, \varphi_\mho \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_\mho = \gamma_\mho.\mathcal{D} - \Upsilon_\mho.\varphi_\mho.\mathcal{D}, \mathcal{T}_\mho = \Upsilon_\mho.\mathcal{D}$, $\mathcal{PBK}_\mho = X_\mho.\mathcal{T}_\mho + \beta_\mho$, and sets $\mathcal{PK}_\mho = X_\mho.\Upsilon_\mho + \gamma_\mho$ and $\propto_\mho = \Upsilon_\mho$.

So, after the above process, $\mathcal{C}_{HCDH}$ updates ($ID_\mho, \beta_\mho, \mathcal{T}_\mho, X_\mho$) and ($ID_\mho, \varphi_\mho \mathcal{PBK}_\mho$), in list^1 and list^2. Further, $\mathcal{C}_{HCDH}$ stores ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho, \mathcal{PBK}_\mho$) in the list$^{\mho}$ and returns $\mathcal{PBK}_\mho$ to $\mathcal{A}_1$.

Secret Number Generation Query (**Q_{sngq}**) : On input $ID_\mho$, $\mathcal{C}_{HCDH}$ combs for a tuple ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho, \mathcal{PBK}_\mho$), if it is not existing in list$^{\mho}$, then $\mathcal{C}_{HCDH}$ perform **Q_{pkeq} with** $ID_\mho$. If $ID_\mho = ID_r{}^t$, $\mathcal{C}_{HCDH}$ returns $\perp$, otherwise it outputs ($\propto_\mho, \mathcal{T}_\mho$).

Partial Private Key Generation Query (**Q_{ppkgq}**) : On input $ID_\mho$, $\mathcal{C}_{HCDH}$ combs for a tuple ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho$, $\mathcal{PBK}_\mho$), if it is not existing in list$^{\mho}$, then $\mathcal{C}_{HCDH}$ perform **Q_{pkeq} with** $ID_\mho$. Then $\mathcal{C}_{HCDH}$ outputs ($\gamma_\mho + \varphi_\mho.\eta, \beta_\mho$).

User Key Generation Query (**Q_{ukgq}**) : On input $ID_\mho$, $\mathcal{C}_{HCDH}$ combs for a tuple ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho, \mathcal{PBK}_\mho$), if it is not existing in list$^{\mho}$, then $\mathcal{C}_{HCDH}$ perform **Q_{pkeq} with** $ID_\mho$. If $ID_\mho = ID_s{}^t$, it outputs ($\mathcal{PK}_\mho, \mathcal{PBK}_\mho$), otherwise $\mathcal{C}_{HCDH}$ returns $\perp$.

Public Key Replace Query(**Q_{pkrq}**) : On input ($ID_\mho$, $\mathcal{PBK}_\mho{}^{/}$)$\mathcal{C}_{HCDH}$ combs for a tuple ($\gamma_\mho, \beta_\mho, \propto_\mho, \mathcal{T}_\mho, \mathcal{PK}_\mho$, $\mathcal{PBK}_\mho$), if it is not existing in list$^{\mho}$, then $\mathcal{C}_{HCDH}$ perform **Q_{pkeq}** with $ID_\mho$. Then, $\mathcal{C}_{HCDH}$replaced$\mathcal{PBK}_\mho$ with $\mathcal{PBK}_\mho{}^{/}$.

Certificateless Signcryption Generation Query (**Q_{csgq}**) : $\mathcal{C}_{HCDH}$ responses to this query in the following manner:

- If $\mathcal{PK}_\mho = \perp$, then $\mathcal{C}_{HCDH}$ randomly choose $\mathcal{K}_r, r, \mathcal{W}\{\in 1, 2, \ldots\ldots, p-1\}$
- Compute $U = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_s + \varphi_s.\mathcal{Q})$ and $\mathcal{C} = \mathcal{E}_{\mathcal{K}_r}(\mathcal{M}, \mathcal{U})$

After this process, it stores ($ID_r, \perp, \mathcal{K}_r, \mathcal{U}$) in list^3 and ($ID_s, \mathcal{C}, \mathcal{W}, r$) in list^4, otherwise, it performs the signcryption algorithm in a normal way and at the same time updates list^3 and list^4. Finally, $\mathcal{C}_{HCDH}$ set $\Psi = (\mathcal{C}, r, \mathcal{W})$ and return it to $\mathcal{A}_1$.

Certificateless Un-Signcryption Query (Q_{cusq}): $\mathcal{C}_{HCDH}$ responses to this query in the following manner:

- It computes $U = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_s + \varphi_s.\mathcal{Q})$ and get access to ($ID_r, \delta_r, \mathcal{U}, \mathcal{K}_r$)
- Then, it computes $(\mathcal{M}, \mathcal{U}) = \mathcal{D}_{\mathcal{K}_r}(\mathcal{C})$ and sends it to $\mathcal{A}_1$.

Challenge: In this phase, first of all $\mathcal{A}_1$ choose two same but different nature messages ($\mathcal{M}_1, \mathcal{M}_2$) and sends the tuple ($ID_r, \mathcal{M}_1, \mathcal{M}_2$) to $\mathcal{C}_{HCDH}$. Then, $\mathcal{C}_{HCDH}$ pick $\mathbb{f}\{\in 0, 1\}$ and produces the challenge signcrypted text Ψ^* by using the following steps.

- $\mathcal{C}_{HCDH}$ randomly choose $\mathcal{K}_r, r, \mathcal{W} \in \{1, 2, \ldots\ldots, p-1\}$ and compute $\mathcal{U} = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_s + \varphi_s.\mathcal{Q})$, and renewed ($ID_s, \mathcal{C}, r, \mathcal{U}$) in list^4.
- Compute $\mathcal{C} = \mathcal{E}_{\mathcal{K}_r}(\mathcal{M}, \mathcal{U})$ and stores ($ID_r, \perp, \mathcal{K}_r, \mathcal{U}$) in list^3
- Set $\Psi^* = (\mathcal{C}, r, \mathcal{W})$ and return it to $\mathcal{A}_1$.

Phase C: In this phase, $\mathcal{A}_1$ made same query with $\mathcal{C}_{HCDH}$ aforementioned, ignoring Q_{cusq} with $ID_s{}^t$, $ID_r{}^t$, Ψ^*, respectively.

Guess: $\mathcal{A}_1$ made the bits $\mathbb{f}^*\{\in 0, 1\}$ and get advantages for wining in this game if $\mathbb{f}^* = \mathbb{f}$. It is obvious that, if $\mathcal{A}_1$ succeeded then it has the genuine $\mathcal{K}_r$, for this it get the access to the tuple ($ID_r, \delta_r, \mathcal{U}$) such that: $\delta_r = a.(\mathcal{PBK}_r + \varphi_r.\mathcal{Q}) = \mathcal{W} + r.(X_s.\Upsilon_s + \gamma_s + \varphi_s.X)(\Upsilon.\mathcal{D} + \propto_\mho .\mathcal{D})$. finally, the $\mathcal{C}_{HCDH}$ getting access to δ_r in list^3 and find the HCDH solution as: $X\Upsilon.\mathcal{D} = (r\varphi_s)^{-1}(\delta_r - (\mathcal{W} + (rX_s.\Upsilon_s + r\gamma_s)(\Upsilon.\mathcal{D} + \propto_\mho .\mathcal{D}))) - \propto_\mho .X.\mathcal{D}$ with adversary $\phi^{/}$.

Theorem 2: In this theorem, $\mathcal{A}_2$ try to break the confidentiality of a message (IND-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$.

Proof: Suppose a triple $\{\mathcal{D}, X\mathcal{D}, \Upsilon\mathcal{D}\}$ is the given instance of HCDH problem, then in the following steps we provide that how the challenger $\mathcal{C}_{\text{HCDH}}$ interacts with $\mathcal{A}_2$ for getting the solution of HCDH problem.

Setup: Here, $\mathcal{C}_{\text{HCDH}}$ sets the master secret as η and master public key as $\mathcal{Q} = \eta.\mathcal{D}$, then it handovers the freely identified set of parameters Φ and η to $\mathcal{A}_2$.

*Phase B:*In this phase, $\mathcal{A}_2$ cannot made Q_{pkrq} and $\mathcal{C}_{\text{HCDH}}$ answers to Q_{pkeq} as followed: $\mathcal{C}_{\text{HCDH}}$ picks $\gamma_{\text{s}}, \propto_{\text{s}}, \text{X}_{\text{s}}, \varphi_{\text{s}} \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_{\text{s}} = \gamma_{\text{s}}.\mathcal{D}, \mathcal{T}_{\mho} = \text{X}_{\text{s}}^{-1}(\Upsilon\mathcal{D} + \propto_{\text{s}} \mathcal{D} - \beta_{\text{s}} - \varphi_{\text{s}}.\mathcal{Q}), \mathcal{PBK}_{\text{s}} = \text{X}_{\text{s}}.\mathcal{T}_{\text{s}} + \beta_{\text{s}}$, and sets $\mathcal{PK}_{\text{s}} = \perp$. Then, renewed list$^{\mho}$, *list*^{1}, and list^2, respectively and sends $\mathcal{PBK}_{\text{s}}$ to $\mathcal{A}_2$.

Guess: $\mathcal{A}_2$ made the bits $\mathbb{f}^* \in 0, 1\}$ and get advantages for wining in this game if $\mathbb{f}^* = \mathbb{f}$. It is obvious that, if $\mathcal{A}_2$ succeeded then it has the genuine $\mathcal{K}_{\text{r}}$, for this it gets the access to the tuple $(\text{ID}_{\text{r}}, \delta_{\text{r}}, \mathcal{U})$ such that: $\delta_{\text{r}} = a.(\mathcal{PBK}_{\text{r}} + \varphi_{\text{r}}.\mathcal{Q}) = \mathcal{W} + r.(\text{X} + \propto_{\text{s}})(\mathcal{PBK}_{\text{s}} + \varphi_{\text{s}}.\mathcal{D}) = (\mathcal{W} + r.(\text{X} + \propto_{\text{s}})(\Upsilon + \propto_{\text{s}})\mathcal{D})$. Finally, the $\mathcal{C}_{\text{HCDH}}$ getting access to δ_{r} in list^3 and find the HCDH solution as: $X\Upsilon\mathcal{D} = r^{-1}(\delta_{\text{r}} - (\mathcal{W} + r.\propto_{\text{s}})(\Upsilon.\mathcal{D} + \propto_{\mho}.\mathcal{D}) - \propto_{\mho}.\text{X}.\mathcal{D}$ with adversary $\phi^{/} = \phi$.

Theorem 3: In this theorem, $\mathcal{A}_1$ try to break the confidentiality of a message (EUF-CMA-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HECDP}}$ is to calculate the HECDP problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$.

Proof: For forging the signature, we suppose a public key $\mathcal{V}$, then in the following steps we provide that how the challenger $\mathcal{C}_{\text{HECDP}}$ interacts with $\mathcal{A}_1$ for getting the solution of HECDP problem.

Setup: Here, $\mathcal{C}_{\text{HECDP}}$ sets the master secret $\eta = \perp$ and master public key as $\mathcal{Q} = \eta.\mathcal{D}$, then it handovers the freely identified set of parameters Φ to $\mathcal{A}_1$.

Query: In this phase, $\mathcal{A}_1$ made the same query like in Phase A,B of Theorem 1, excepting the following two queries:

1. $\mathbf{Q_{pkeq}}$: On input $\text{ID}_{\mho}$, $\mathcal{C}_{\text{HECDP}}$ combs for a tuple $(\gamma_{\mho}, \beta_{\mho}, \propto_{\mho}, \mathcal{T}_{\mho}, \mathcal{PK}_{\mho}, \mathcal{PBK}_{\mho})$, if it is existing in list$^{\mho}$, then it sends $\mathcal{PBK}_{\mho}$ to $\mathcal{A}_1$. Otherwise, it picks $\gamma_{\mho}, \propto_{\mho}, \text{X}_{\mho}, \varphi_{\mho} \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_{\mho} = \gamma_{\mho}.\mathcal{D}, \mathcal{T}_{\mho} = \text{X}_{\mho}^{-1}(\mathcal{V} + \propto_{\mho} \mathcal{D} - \beta_{\mho} - \varphi_{\mho}.\mathcal{Q}), \mathcal{PBK}_{\mho} = \text{X}_{\mho}.\mathcal{T}_{\mho} + \beta_{\mho}$, and sets $\mathcal{PK}_{\mho} = \perp$ and and $\propto_{\mho} = \Upsilon_{\mho}$. Then, renewed list$^{\mho}$, list^1, and list^2, respectively and sends $(\mathcal{PBK}_{\mho}, \mathcal{PK}_{\mho})$ to $\mathcal{A}_1$.
2. $\mathbf{Q_{ukgq}}$: On input $\text{ID}_{\mho}$, $\mathcal{C}_{\text{HECDP}}$ combs for a tuple $(\gamma_{\mho}, \beta_{\mho}, \propto_{\mho}, \mathcal{T}_{\mho}, \mathcal{PK}_{\mho}, \mathcal{PBK}_{\mho})$, if it is exist in list$^{\mho}$ and $\mathcal{PK}_{\mho} \neq \perp$, then $\mathcal{C}_{\text{HECDP}}$ returns $(\mathcal{PBK}_{\mho}, \mathcal{PK}_{\mho})$ to $\mathcal{A}_1$. Otherwise, $\mathcal{C}_{\text{HECDP}}$ picks $\text{P}_{\mho}, \propto_{\mho}, \text{X}_{\mho}, \varphi_{\mho} \in \{1, 2, \ldots\ldots, p-1\}$ and compute $\mathcal{T}_{\mho} = \propto_{\mho}.\mathcal{D}, \beta_{\mho} = \mathcal{P}_{\mho}.\mathcal{D} - \varphi_{\mho}.\mathcal{Q}, \mathcal{PK}_{\mho} = \text{X}_{\mho}.\Upsilon_{\mho} + \mathcal{P}_{\mho}$, and $\mathcal{PBK}_{\mho} = \text{X}_{\mho}.\mathcal{T}_{\mho} + \beta_{\mho}$, Then, renewed list$^{\mho}$, list^1, and list^2, respectively and sends $(\text{PBK}_{\mho}, \mathcal{PK}_{\mho})$ to $\mathcal{A}_1$.

Forgery: $\mathcal{A}_1$ returns a forge signature $\Psi^{\text{f}} = (\mathcal{C}^{\text{f}}, r^{\text{f}}, \mathcal{W}^{\text{f}})$ for $\text{ID}_{\text{r}}^{\text{t}}$ which has not asked for $\mathbf{Q_{ukgq}}$. So, $\mathcal{A}_1$ succeeded easily if the followed equation is hold: $\mathcal{U} = \mathcal{W}^{\text{f}}.\mathcal{D} + r^{\text{f}}.(\mathcal{PBK}_{\text{s}} + \varphi_{\text{s}}.\mathcal{Q}) = \mathcal{W}^{\text{f}} + r^{\text{f}}.(\mathcal{V} + \propto_{\mho}.\mathcal{D}) = (\mathcal{W}^{\text{f}} + r^{\text{f}} \propto_{\mho}).\mathcal{D} + r.\mathcal{V}$, then $\mathcal{C}_{\text{HECDP}}$ forge a signature $(r^{\text{f}} \propto_{\mho}, r^{\text{f}}, \mathcal{W}^{\text{f}})$ with adversary $\phi^{/} = \phi$.

Theorem 4: In this theorem, $\mathcal{A}_2$ try to break the confidentiality of a message (EUF-CMA-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HECDP}}$ is to calculate the HECDP problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$.

Proof: For forging the signature, we suppose a public key $\mathcal{V}$, then in the following steps we provide that how the challenger $\mathcal{C}_{\text{HECDP}}$ interacts with $\mathcal{A}_2$ for getting the solution of HECDP problem.

Setup: Here, $\mathcal{C}_{\text{HECDP}}$ sets the master secret as η and master public key as $\mathcal{Q} = \eta.\mathcal{D}$, then it handovers the freely identified set of parameters Φ and η to $\mathcal{A}_2$.

Query: In this phase , $\mathcal{A}_2$ cannot made $\mathcal{Q}_{\text{pkrq}}$ and $\mathcal{C}_{\text{HCDH}}$ answers to Q_{pkeq} and Q_{pkeq} working as like Theorem 3.

Forgery: $\mathcal{A}_2$ returns a forge signature $\Psi^{\text{f}} = (\mathcal{C}^{\text{f}}, r^{\text{f}}, \mathcal{W}^{\text{f}})$ for $\text{ID}_{\text{r}}^{\text{t}}$. So, $\mathcal{A}_2$ succeeded easily, then $\mathcal{C}_{\text{HECDP}}$ forge a signature $(r^{\text{f}} \propto_{\mho}, r^{\text{f}}, \mathcal{W}^{\text{f}})$ with adversary $\phi^{/} = \phi$.

Theorem 5: In this theorem, $\mathcal{A}_1$ try to break the confidentiality of a message (ANON-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_1$ with the utilized advantage $\phi^{/}$.

Proof: Suppose a triple $\{\mathcal{D}, X\mathcal{D}, \Upsilon\mathcal{D}\}$ is the given instance of HCDH problem, then in the following steps we provide that how the challenger $\mathcal{C}_{\text{HCDH}}$ interacts with $\mathcal{A}_1$ for getting the solution of HCDH problem.

Setup: Here, $\mathcal{C}_{\text{HCDH}}$ sets the master secret $\eta = \perp$ and master public key as $\mathcal{Q} = \eta.\mathcal{D}$, then it handovers the freely identified set of parameters Φ to $\mathcal{A}_1$.

Phase A: In this phase, $\mathcal{A}_1$ selects two identity $(\text{ID}_1{}^1, \text{ID}_2{}^2)$ and sends them to $\mathcal{C}_{\text{HCDH}}$. So, it performs the same hash queries.

Phase B: $\mathcal{C}_{\text{HCDH}}$ answered to $\mathbf{Q_{pkeq}}$ in the following manner: $\mathcal{C}_{\text{HCDH}}$ picks $\gamma_{\mho}, \propto_{\mho}, \text{X}_{\mho}, \varphi_{\mho} \in \{1, 2, \ldots\ldots, p-1\}$, calculates $\beta_{\mho} = \gamma_{\mho}.\mathcal{D}, \mathcal{T}_{\mho} = \text{X}_{\mho}{}^{-1}(X\mathcal{D} + \propto_{\mho} - \beta_{\mho} - \varphi_{\mho}.\mathcal{Q}), \mathcal{PBK}_{\mho} = \text{X}_{\mho}.\mathcal{T}_{\mho} + \beta_{\mho}$, and sets $\mathcal{PK}_{\mho} = \perp$. Then, renewed list$^{\mho}$, list^1, and list^2, respectively and sends $\mathcal{PBK}_{\text{s}}$ to $\mathcal{A}_1$.

Challenge: In this phase, first of all $\mathcal{A}_1$ choose a message $\mathcal{M}$ and sends the tuple $(\text{ID}_{\text{r}}, \mathcal{M}, \text{ID}_{\text{s}})$ to $\mathcal{C}_{\text{HCDH}}$. Then, it produces the challenge signcrypted text Ψ^* by using the following steps.

- $\mathcal{C}_{\text{HCDH}}$ randomly choose $\mathcal{K}_{\text{r}}, r, \mathcal{W} \in \{1, 2, \ldots\ldots, p-1\}$ and compute $\mathcal{U} = \mathcal{W}.\mathcal{D} + r.(\mathcal{PBK}_{\text{s}} + \varphi_{\text{s}}.\mathcal{Q})$, and renewed $(\text{ID}_{\text{s}}, \mathcal{C}, r, \mathcal{U})$ in list^4.
- Compute $\mathcal{C} = \mathcal{E}_{\mathcal{K}_{\text{r}}}(\mathcal{M}, \mathcal{U})$ and stores $(\text{ID}_{\text{r}}, \perp, \mathcal{K}_{\text{r}}, \mathcal{U})$ in list^3
- Set $\Psi^* = (\mathcal{C}, r, \mathcal{W})$ and return it to $\mathcal{A}_1$.

Finally, the $\mathcal{C}_{\text{HCDH}}$ getting access to δ_{r} in list^3 and find the HCDH solution with adversary $\phi^{/} = \phi$.

TABLE 2. Computational cost comparison.

Schemes	Signcryption	Unsigncryption	Total	Total (ms)
Li et al.[16]	ξ	2 $\beta\rho$	2 $\beta\rho$+ ξ	2(14.90)+1.25=31.05
Cao et al. [17]	7 $\xi\rho m$	5 $\xi\rho m$	12 $\xi\rho m$	12(0.97)=11.64
Liu et al. [18]	5ξ	6ξ	11 ξ	11(1.25)=13.75
Proposed	4 $\hbar\xi dm$	4 $\hbar\xi dm$	8 $\hbar\xi dm$	8(0.48)= 3.84

TABLE 3. Computational cost comparison.

Schemes	Communication Cost	Communication Cost (bits)
Li et al. [16]	|m|+ 2|g|	3072
Cao et al. [17]	|m|+ 2|Q|	1344
Liu et al. [18]	|m|+ |P|+2|H|	2557
Proposed	|m|+ 2|N|	1184

TABLE 4. Variable values.

Variable	Value
|m|	1024 bits
|P|	1024
|H|	256
|Q|	160 bits
|N|	80 bits
|g|	1024 bits

Theorem 6: In this theorem, $\mathcal{A}_2$ try to break the confidentiality of a message (ANON-CCA2-Game) and communicate for this purpose with a challenger $\mathcal{C}_{\text{HCDH}}$ with the privilege ϕ. Here, the duty of $\mathcal{C}_{\text{HCDH}}$ is to calculate the HCDH problem for $\mathcal{A}_2$ with the utilized advantage $\phi^{/}$.

Proof: Suppose a triple $\{\mathcal{D}, X\mathcal{D}, \Upsilon\mathcal{D}\}$ is the given instance of HCDH problem, then in the following steps we provide that how the challenger $\mathcal{C}_{\text{HCDH}}$ interacts with $\mathcal{A}_2$ for getting the solution of HCDH problem. So, $\mathcal{A}_2$ make the same series query which is performed in theorem 2, accepts that the Phase A, Phase B and Challenge are the alike as Theorem 5. Finally, the $\mathcal{C}_{\text{HCDH}}$ getting access to δ_{r} in list^3 and find the HCDH solution with adversary $\phi^{/} = \phi$.

Theorem 7: This theorem proves that the proposed scheme is forwardly secure from $\mathcal{A}_1$ and $\mathcal{A}_2$. In our scheme we used the secret key for encryption and decryption, so if the $\mathcal{A}_1$ and $\mathcal{A}_2$ get access to sender private key but they still failed to unscrambled the Ciphertext.

VII. PERFORMANCE COMPARISON

A. COMPUTATIONAL COST

Here, we compare our afresh assembled technique with those of Li *et al.* [16], Cao *et al.* [17], and Liu *et al.* [18], with respect to major operations such bilinear pairing ($\beta\rho$), exponentiations (ξ), elliptic curve multiplications ($\xi\rho m$), and hyper elliptic curve devisor multiplications ($\hbar\xi dm$), which is illustrated in Table 2. Then, we make the comparisons in Table 2, with the help of milli seconds on the basis of results used in [30], which includes the running time for is 14.90 ms; for ξ is 1.25 ms; for $\hbar\xi dm$ is 0.97 ms and for $\hbar\xi dm$ is 0.48 ms [31], [32]. To estimate the performance of the proposed approach, the Multi precision Integer and Rational Arithmetic C Library (MIRACL) is used to test the runtime of the basic cryptographic operations up to 1000 times. The following are the details of resources used for testing the running time of the basic cryptographic operations up to 1000 times:

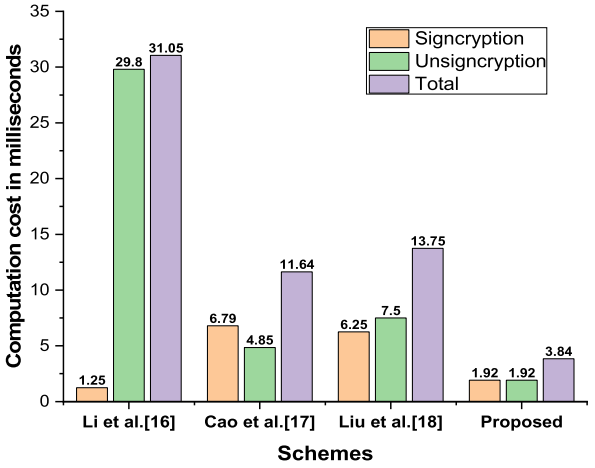


FIGURE 2. Computation cost comparison (in ms).

- Intel Core i74510U$\mathcal{CPU}$
- 2.0$\mathcal{G}$Hz processor
- 8 GB RAM
- C++ with MIRACL
- window 7

It is obvious that the scheme of Li *et al.* [16], Cao *et al.* [17], and Liu *et al.* [18], are inferior in term of computational efficiency from our scheme which is presented in Tab. 2 and Fig. 2.

B. COMMUNICATION COST

Here, we compare our afresh assembled technique with those of Li *et al.* [16], Cao *et al.* [17], and Liu *et al.* [18], with respect to bits as exemplified in Table 3. In Table 4, we provide the supposed values for bilinear pairing (g), RSA (P), elliptic curve (Q), hash (H), and hyper elliptic curve (N). It is obvious that the scheme of Li *et al.* [16], Cao *et al.* [17], and Liu *et al.* [18], are inferior in term of communications efficiency from our scheme which is presented in Tab. 3 and Fig. 3.

TABLE 5. Security properties comparisons.

Schemes	Confidentiality	Unforgeability	Anonymity	Forward Security
Li et al.[16]	YES	YES	YES	NO
Cao et al. [17]	YES	YES	NO	NO
Liu et al. [18]	YES	YES	NO	NO
Proposed	YES	YES	YES	YES

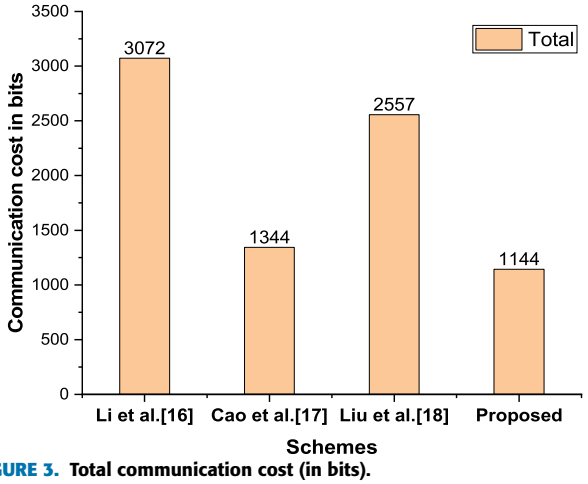


FIGURE 3. Total communication cost (in bits).

C. SECURITY PROPERTIES COMPARISONS

In Table 5, we present the security properties comparisons of the proposed scheme with the schemes presented by Li *et al.* [16], Cao *et al.* [17], and Liu *et al.* [18]. As shown in table 5 that the proposed scheme ensures confidentiality, unforgeability, anonymity, and forward security, whiles the Cao *et al.* [17], and Liu *et al.* [18], only ensures confidentiality and unforgeability. Moreover, the scheme proposed by Li *et al.* [16], ensures confidentiality, unforgeability, and anonymity.

VIII. CONCLUSION

Internet of Health Things (IoHT) is a combination of the Internet of Things (IoT) and Wireless Body Area Networks (WBAN) that allows healthcare services to be delivered over the Internet at any time and from any place. However, in the absence of protective measures, IoHT ecosystems may be risky. It allows large-scale malicious attackers to alter, capture, erase, or even inject fake information into patients' health-related information. To address these issues, we introduced an anonymous certificateless signcryption scheme for the IoHT environment based on the HEC concept. The HEC approach is efficient at generating small keys, making it suitable for use in an IoHT system. Furthermore, the proposed scheme eliminates the key escrow issue due to the certificateless cryptography mechanism. In an open wireless channel, the scheme, therefore, guarantees receiver anonymity, message confidentiality, and unforgeability of digital signature. The computational and communication cost analysis shows that the proposed scheme is proficient from existing counterparts.

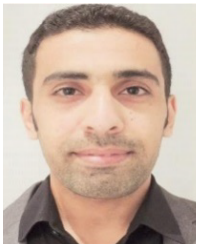
In the future, we are intended to design a certificateless signcryption scheme with the presence of public verifiability in multi-cast communication settings.

REFERENCES

[1] J. J. P. C. Rodrigues, D. B. De Rezende Segundo, and H. A. Junqueira, "Enabling technologies for the Internet of health things," *IEEE Access*, vol. 6, pp. 13129–13141, 2018.
[2] S. M. Riazul Islam, D. Daehan Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kyung-Sup Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.
[3] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, and M. L. Stefanizzi, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.
[4] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The Internet of things in healthcare: An overview," *J. Ind. Inf. Integr.*, vol. 1, pp. 3–13, Mar. 2016.
[5] M. Woo, J. Lee, and K. Park, "A reliable IoT system for personal healthcare devices," *Future Gener. Comput. Syst.*, vol. 78, pp. 626–640, Jan. 2018.
[6] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generat. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.
[7] F. Firouzi, A. M. Rahmani, K. Mankodiya, M. Badaroglu, G. V. Merrett, P. Wong, and B. Farahani, "Internet-of-Things and big data for smarter healthcare: From device to architecture, applications and analytics," *Future Gener. Comput. Syst.*, vol. 78, pp. 583–586, Jan. 2018.
[8] M. A. Khan, S. U. Rehman, M. I. Uddin, S. Nisar, F. Noor, A. Alzahrani, and I. Ullah, "An online-offline certificateless signature scheme for Internet of health things," *J. Healthcare Eng.*, vol. 2020, Dec. 2020, Art. no. 6654063.
[9] M. A. Khan, I. M. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)," *Drones*, vol. 3, no. 1, p. 16, Feb. 2019.
[10] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.
[11] L. Zhang, L. Zhang, Z. Xv, and C. Guo, "An anonymous signcryption scheme based on one-off public key," in *Proc. Int. Conf. Cyberspace Technol. (CCT)*, Beijing, China, 2013, pp. 81–86.
[12] M. A. Khan, I. Ullah, S. Nisar, F. Noor, and I. M. Qureshi, "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[13] M. Suárez-Albela, P. Fraga-Lamas, and T. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, Nov. 2018.
[14] 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, 2018, Art. no. e03763.
[15] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors J.*, vol. 16, no. 13, pp. 5389–5396, Jul. 2016.
[16] F. Li, Y. Han, and C. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 747–758, Mar. 2018.
[17] G. Gao, X. Peng, and L. Jin, "Efficient access control scheme with certificateless signcryption for wireless body area networks," *Int. J. Netw. Secur.*, vol. 21, no. 3, pp. 428–437, May 2019.
[18] X. Liu, Z. Wang, Y. Ye, and F. Li, "An efficient and practical certificateless signcryption scheme for wireless body area networks," *Comput. Commun.*, vol. 162, pp. 169–178, Oct. 2020.
[19] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010.

[20] S.-J. Horng, S. F. Tzeng, Y. Pan, and P. Fan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013, doi: 10.1109/TIFS.2013.2277471.
[21] V. Odelu, A. K. Das, M. K. Khan, K. R. Choo, and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," *IEEE Access*, vol. 5, pp. 3273–3283, 2017, doi: 10.1109/ACCESS.2017.2669940.
[22] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017, doi: 10.1109/TVT.2015.2406877.
[23] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Commun.*, vol. 10, no. 14, pp. 1795–1802, Sep. 2016.
[24] M. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world," *IETE Tech. Rev.*, vol. 26, no. 3, pp. 191–195, 2009.
[25] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, M. S. Hossain, and M. Atiquzzaman, "A reliable Internet of Things based architecture for oil and gas industry," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2017, pp. 705–710, doi: 10.23919/ICACT.2017.7890184.
[26] M. K. Khan and J. Zhang, "An efficient and practical fingerprint-based remote user authentication scheme with smart cards," in *Information Security Practice and Experience*. Berlin, Germany: Springer, 2006, pp. 260–268.
[27] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Aug. 2019, pp. 1–5.
[28] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K.-F. Hsiao, "Ensuring privacy and security in E- health records," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2018, pp. 1–5.
[29] M. E. Mukhtar Mahmoud, J. P. C. Joel Rodrigues, K. Saleem, J. Al-Muhtadi, N. Kumar, and V. Korotaev, "Towards energy-aware fog-enabled cloud of things for healthcare," *Comput. Elect. Eng.*, vol. 67, pp. 58–69, Apr. 2018.
[30] I. Ullah, N. U. Amin, M. Zareei, A. Zeb, H. Khattak, A. Khan, and S. Goudarzi, "A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications," *Symmetry*, vol. 11, no. 11, p. 1386, 2019.
[31] M. A. Khan, I. Ullah, N. Kumar, and O. S. Oubbati, "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol 70, no. 5, pp. 4839–4851, May 2021, doi: 10.1109/TVT.2021.3055895.
[32] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. Khanzada, H. Khattak, and M. A. Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Inf. Syst.*, vol. 2020, Jul. 2020, Art. no. 8861947.

INSAF ULLAH received the master'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 working as a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interest includes network security.



ALI ALKHALIFAH received the B.S. degree in computer science from Qassim University, in 2007, the master's degree (Hons.) in IT from the University of Newcastle, in 2010, and the Ph.D. degree in information systems from the University of New South Wales, Australia, in 2013. He is currently an Associate Professor with the IT Department, College of Computer, Qassim University. He has been involved in several program committees and is being a reviewer in different international conferences and journals. His research interests include IT adoption, information security, identity management systems, and evaluation of the World Wide Web.

SAJJAD UR REHMAN (Member, IEEE) received the B.Sc. degree in electronics engineering from Iqra University, Karachi, Pakistan, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2018. From 2007 to 2008, he worked as a Lecturer with the Department of Electronics Engineering, Iqra University (Peshawar Campus). From 2008 to 2019, he worked as a Researcher with the Electrical Engineering Department, King Saud University. From May 2019 to October 2019, he worked as an Associate Professor with the Qurtuba University of Science and IT, Dera Ismail Khan, Pakistan. He is currently an Associate Professor with the Namal Institute, Mianwali, Pakistan. His research interests include the Internet of Things (IoT), advanced technologies in wireless communications, reconfigurable antennas and filter designing, and MIMO antennas. His awards and honors include the Kind Saud University College of Engineering Excellent Research Award, in 2012, 2015, and 2017. He was awarded the General Prize by the Deanship of Graduate Studies, King Saud University, for his outstanding research performance, in 2013.

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He is also working with the Department of Computer Science and Information Engineering, Asia University, Taiwan, and the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India. He has more than 300 technical research articles in leading journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TWPS, the IEEE SYSTEMS JOURNAL, the *IEEE Communications Magazine*, the *IEEE Wireless Communications Magazine*, the *IEEE Network Magazine*, and conferences. His research is supported from DST, TCS, and UGC. He has guided many students leading to M.E. and Ph.D. His research interests include mobile computing, parallel/distributed computing, multi-agent systems, service-oriented computing, routing and security issues in mobile *ad hoc*, and sensor and mesh networks. He was a recipient of best papers award from IEEE SYSTEMS JOURNAL (2018) and IEEE ICC (2018). He is a TPC member/technical committee member of various conferences and organized various workshops in ICC, and Globocom conferences.

MUHAMMAD ASGHAR KHAN received the Ph.D. degree in electronic engineering from the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He is currently working as the Director-ORIC of the Department of Electrical Engineering, Hamdard University, Islamabad. He has more than 40 technical research articles in leading journals, such as the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Future Generation Computer Systems*, the IEEE INTERNET OF THINGS JOURNAL, and conferences. His main research interests include drones/UAVs, the IoT, e-health with a focus on networks, platforms, security, as well as applications and services. He is a reviewer for various journals published by IEEE, Elsevier, MDPI, and EURASIP. He has served as a guest editor for a number of international journals.