Hindawi
Journal of Healthcare Engineering
Volume 2020, Article ID 6654063, 10 pages
https://doi.org/10.1155/2020/6654063

Research Article

An Online-Offline Certificateless Signature Scheme for Internet of Health Things

Muhammad Asghar Khan,[1] **Sajjad Ur Rehman**,[2] **M. Irfan Uddin**,[3] **Shibli Nisar**,[4] **Fazal Noor**,[5] **Ali Alzahrani**,[5] **and Insaf Ullah**[1]

[1]*Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan*
[2]*Department of Electrical Engineering, Namal Institute, Mianwali, Pakistan*
[3]*Institute of Computing, Kohat University of Science and Technology, Kohat 26000, Pakistan*
[4]*Department of Electrical Engineering, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan*
[5]*Department of Computer Science and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia*

Correspondence should be addressed to Insaf Ullah; insafktk@gmail.com

Received 17 November 2020; Revised 11 December 2020; Accepted 21 December 2020; Published 31 December 2020

Academic Editor: Shah Nazir

The Internet of Health Things (IoHT) is an extended breed of the Internet of Things (IoT), which plays an important role in the remote sharing of data from various physical processes such as patient monitoring, treatment progress, observation, and consultation. The key benefit of the IoHT platform is the ease of time-independent interaction from geographically distant locations by offering preventive or proactive healthcare services at a lower cost. The communication, integration, computation, and interoperability in IoHT are provided by various low-power biomedical sensors equipped with limited computational capabilities. Therefore, conventional cryptographic solutions are not feasible for the majority of IoHT applications. In addition, executing computing-intensive tasks will lead to a slow response time that can deteriorate the performance of IoHT. We strive to resolve such a deficiency, and thus a new scheme has been proposed in this article, called an online-offline signature scheme in certificateless settings. The scheme divides the signing part into two phases, i.e., online and offline. In the absence of a message, the offline phase performs computationally intensive tasks, while lighter computations are executed in the online phase when there is a message. Security analyses and comparisons with the respective existing schemes are carried out to show the feasibility of the proposed scheme. The results obtained authenticate that the proposed scheme offers enhanced security with lower computational and communication costs.

1. Introduction

IoHT is an IoT submarket, capable of grouping all medical devices and applications for gathering, analyzing, and exchanging physiological data of patients over the Internet [1]. Patient data can be collected through biomedical sensors and processed via user terminal devices such as computers, smart phones, smart watches, or even a specific embedded device [2]. Patient data may include breathing rate, blood pressure, chest sound, body temperature, respiratory rate, electrocardiogram (ECG), patient position (accelerometer), etc. [3–7]. In addition to medical applications, IoHT can also be used to monitor environmental conditions such as patient-care venues, room status, laboratory shift times, treatment times, and staff-to-patient ratios. The user terminal devices are linked to a gateway via short-range wireless technologies such as Bluetooth Low Energy (BLE), Wi-Fi, and Zigbee. The BLE, however, uses strong features such as moderate data rate, low-power consumption, and unlicensed band, making them the most preferable options for connecting wearable sensor nodes. The gateway may be further connected to a (clinical) server or cloud services via fifth-generation (5G) wireless link for high storage and intensive data processing. In a health information system, patient details can be maintained as

electronic health records, which are available to the medical professionals when the patient visits the hospital.

Since a large scale of interactions between biomedical sensors and mobile devices is undertaken on an open wireless channel in IoHT environment, which poses a range of challenges, the most significant of which is the security and privacy of health-related information of patients [8]. To steal or fabricate patient health-related information, an intruder may capture the communication between the sensors and mobile devices. Likewise, with high probability, the attacker may gain access to the disease or health status of the patient. In addition, most devices involved in the IoHT platform have limited computing capabilities and, consequently, fail to perform conventional cryptographic calculations. For example, heavy computations are needed for most of the public key cryptosystems proposed in the literature; therefore, their implementation has not been considered acceptable for IoHT devices. An online-offline approach can be used to address heavy computation issues. When the IoHT devices have reported a message, the online phase is used to perform light computations only, while the offline computations or heavy computations are performed if no message has been recorded by the IoHT devices. Authentication is a major concern for securing IoHT devices. In general, the digital signature is used for authentication in cryptography. Therefore, the digital signature can be used with the online-offline approach for securing IoHT devices. The offline-computed signature value is generated in the offline phase, while the online phase operates with the same offline signature value.

The two basic methods used to validate the public keys are Identity-Based Cryptography (IBC) and Public Key Infrastructure (PKI) in public key cryptosystems. This includes a Certificate Authority (CA) signature, which provides a unique signature link [9]. The CA specifies the public keys with the certificates as defining a participant. However, shortcomings such as distribution, storage, and manufacturing difficulties are associated with PKI systems. Instead, IBC is suggested to decrease the cost of public-key management [10]. The trusted Private Key Generator (PKG) has first-hand data about the participants' private keys with the expense of private key escrow issues [11, 12]. Therefore, certificateless cryptosystem can be used with the signature scheme to accommodate the key escrow problem.

Some computationally hard problems, such as bilinear pairing, Rivest–Shamir–Adleman (RSA), and elliptic curve cryptosystems, usually measure the efficiency of signature schemes. The RSA cryptosystem [13, 14] uses a large key of 1024 bits [15]. Likewise, due to the massive pairing and map-to-point function computation, bilinear pairing is 14.31 times lower than RSA [16]. Similarly, in order to remove the shortcomings of RSA and bilinear pairing, the elliptic curve was introduced [17]. The security hardness and efficiency of elliptic curve cryptography are based on 160-bit keys compared to bilinear pairing and RSA [18]. Despite this, for resource-hungry devices, the 160-bit key is also undesirable and not affordable. Therefore, a new form, the generalization of the elliptic curve, called the hyperelliptic curve was thus suggested [19]. The hyperelliptic curve offers the same degree of protection as the elliptic curve, bilinear pairing, and RSA using 80-bit keys, identity, and certificate size [20, 21]. For energy-constrained IoHT devices, the hyperelliptic curve would be a better option. Therefore, the data generated by the anticipated massive number of biomedical sensors and IoT devices would need to be collected, processed, and analyzed efficiently in real-time to ensure safe and timely management of patient health [22].

Considering the above objectives, a new scheme, called the online-offline certificateless signature scheme, has been introduced for IoHT. The scheme uses the concept of the hyperelliptic curve and is characterized by the small key size. In comparison, it is uncompromisingly identical to the solutions introduced by the elliptical curve method with half key size.

The research study conducted has the following excellent characteristics:

(i) A lightweight security scheme, namely, online-offline certificateless signature, has been proposed for an IoHT platform.

(ii) The proposed scheme divides the certificateless signature scheme into two phases, i.e., online and offline. Lighter computations are performed when there is a message in the online phase, while the offline phase performs computing-intensive tasks in the absence of a message.

(iii) The scheme uses the hyperelliptic curve cryptography that tackles the limitations faced by IoHT devices such as limited energy and computing capabilities.

(iv) The proposed scheme has shown to be immune to numerous attacks through formal security analysis.

(v) Our approach offers better efficiency in terms of computational cost and communication overhead when compared to the existing equivalent schemes.

1.1. Structure of the Paper. The rest of the article is structured as follows. In Section 2, the relevant work is discussed. Section 3 includes preliminaries. The proposed online-offline certificateless signature system is introduced in Section 4. Security analysis can be found in Section 5. The cost analysis is provided in Section 6 with current solutions. Concluding remarks are available in Section 7.

2. Related Work

In scientific literature, the security and privacy concerns using the online-offline approach have not received ample consideration. Thus, the problems need to be thoroughly investigated. A well-designed security framework would greatly minimize the risk of the data being hacked, regardless of the devilish strategy involved. Some research studies are devoted to addressing IoHT platform data security problems.

The offline-online signature technique was first suggested by Even et al. [23], which is suitable for limited-storage devices. When the message to be signed is known, the execution of

their procedure enables the use of the offline mechanism to do moderate computations. After the message is understood to be authenticated, the second phase is carried out electronically. The protection of their method is dependent on the intractability of the large integer factoring mechanism. Their device is protected by chosen messages from attacks. However, their approach is not so successful in practice.

In 2001, to create an effective online-offline signature scheme, Shamir and Tauman [24] used chameleon hash functions based on an ordinary digital signature. In the proposed scheme, the key scale and signature sizes are reduced according to the original scheme. A new type of hash function, called the trapdoor hash function, has been introduced in their model to increase the system security. If the signer repeatedly uses the same hash value to get two signatures on two distinct messages, the recipient can gain a hash collision and use it to retrieve trapdoor information from the signer, which is the secret key of the signer. However, the proposed scheme uses many chameleon hash values for various messages. The main disclosure issue of chameleon hashing is known as this concern.

Yu and Tate [25] suggested an effective online-offline signature scheme that is known to be secure without a random oracle under the RSA assumption. They did not use the hash function at the trapdoor. Therefore, the second key pair did not need to be handled by their scheme and did not have to include in their signature the random commitment attribute. However, the proposed scheme is not affordable for resource-constrained IoHT devices due to the RSA cryptosystem, which is based on hard problems and incurs the high computational cost. Wu et al. [26], using bilinear pairing, suggested a successful online-offline signature scheme. The security of the model is connected to the theoretical Diffie–Hellman assumption in the random oracle model. Addobea et al. [27] also proposed an offline-online signature scheme called the MHCOOS for M-Health devices based on bilinear pairing. However, bilinear pairing involves high pairing and map-to-point function operations, which is not suitable for resource-constrained IoHT devices.

All of the above schemes are based on complex cryptographic techniques, i.e., elliptic curve and bilinear pairing, and thus suffer from high costs of computation and communication overhead. These schemes are thus not compatible with IoHT systems equipped with minimal computing capability. To create a viable IoHT cryptographic solution that needs less computation, there is a critical need to use the state-of-the-art online-offline certificateless signature technique. Our proposed scheme is based on hyperelliptic curve cryptography, which is an advanced version of the elliptic curve. It provides the same degree of protection with the smaller key size as compared to an elliptical curve, bilinear pairing, and modular exponential.

3. Preliminaries

*3.1. Hyperelliptic Curve Discrete Logarithm Problem (**HC DL P**).* Suppose a given instance of hyperelliptic curve $\delta = \varepsilon$. Then, the HCDLP is to determine ε from the given instance.

3.2. Threat Model. The security models of the proposed scheme include message c, unforgeability against the adversaries called Type 1 adversary (A_1), and Type 2 adversary (A_2), respectively. A_1 is a malicious adversary who has the ability to replace the user's public key besides the system master keys, while A_2 means an honest-but-curious KGC who knows the system master keys but is not allowed to replace the user's public key. The specific security models under different adversaries are as same as [28] such that unforgeability regarding EUF-CMA-A_1 and unforgeability regarding EUF-CMA-A_2.

4. Proposed Online-Offline Certificateless Signature Scheme

4.1. Network Model. An initiative to incorporate the proposed scheme must be preceded by careful consideration of the following assumptions:

(1) Patient data input can be obtained by sensors and analyzed by user terminal devices, such as laptops, tablets, smart watches, or even a particular embedded system

(2) Each of the medical sensors and the user terminal are connected through BLE

(3) The user terminal can be further linked with the cloud server using 5G, equipped with cloud computing services

(4) The medical server presumes the role of administrators

(5) The medical server is linked with the local computer in which electronic health records (HER) can be viewed by the medical personnel

(6) The HER is stored securely in the database server for future consultations

IoHT can be implemented in various settings, depending on the requirements as shown in Figure 1. The required gadgets are usually included in the medical sensors according to the patient's illness. Using short-range radio transceivers (i.e., BLE), the sensors can be connected with the gateway router. On a frequency band of 2.4 GHz, the BLE works. There are valid reasons for selecting this level of technology. They function, for example, in the unlicensed spectrum and provide fair data rates and consume very low power [29]. The aggregated data from the patient monitoring sensors may be too big to be handled by the local server. It demands a high ability for storage and computing. Fortunately, with its architecture, the emerging fifth-generation (5G) mobile networking introduces multiaccess edge computing (MEC) facility. MEC performs high storage and intensive processing facilities when integrated into an IoHT setting.

4.2. Construction of the Proposed Scheme. This section covers the construction of the proposed scheme. Notations used in the proposed scheme are illustrated in Table 1. The proposed

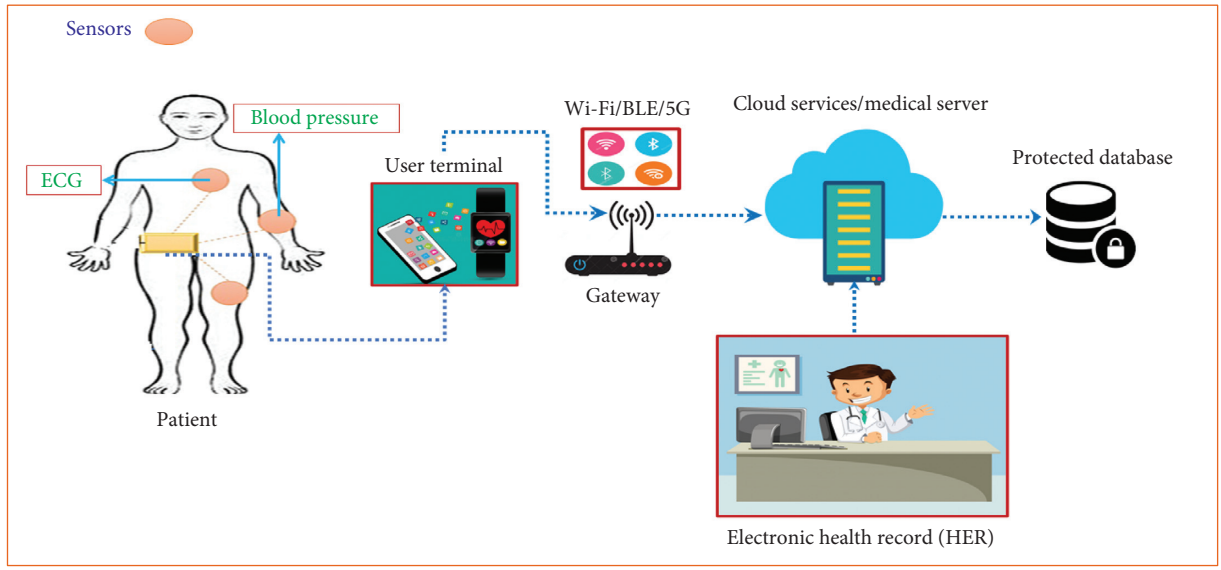

Figure 1: Sample network model of IoHT system.

Table 1: Notations used.

Notation	Description
η	It represents a security parameter
$\hbar c$	It represents a hyperelliptic curve
$f(n)$	It represents a finite field of n
n	It represents a large prime number belonging to hyperelliptic curve where the size of $n \geq 2^{80}$
$\mathscr{D}$	Divisor on the hyperelliptic curve ($\hbar c$)
$\mathscr{Q}$	Master private key of the system
$\mathscr{K}$	Master public key of the system
ψ	It represents a global parameter set that can be available publicly in a network
id_s, id_r	Identity of sender and receiver
Γ_s, Γ_r	They represent partial private key pair for sender and receiver
$\mathscr{N}_s$, $\mathscr{N}_r$	They represent private key pair for sender and receiver
$\mathscr{Z}_s$, $\mathscr{Z}_r$	They represent public key pair for sender and receiver
$\mathscr{S}$	Its represents signature
ϕ	It represents signature pair
h_x, h_y, h_z	Three irreversible and collision resistance hash functions
$\perp$	It represents null

scheme can be made from the following computational constructions [28]:

Setup: the following computations can be used for this phase:

(i) The security parameter η can choose by KGC

(ii) It selects a hyperelliptic curve ($\hbar c$) with field $f(n)$, where the size of $n \geq 2^{80}$

(iii) Select a $\mathscr{D}$ devisor from hyperelliptic curve ($\hbar c$)

(iv) Then, choose three irreversible and collision resistance hash functions h_x, h_y, and h_z

(v) KGC picks $\mathscr{Q} \in \{1, 2, \ldots, n-1\}$ as a master key and then computes the public key as $\mathscr{K} = \mathscr{Q} \cdot \mathscr{D}$

(vi) KGC produces $\psi = \{\mathscr{K}, h?, h?, h?, \mathscr{D}, \hbar c, (?), ? \geq 2^{80}$ as global parameter set and publishes it publicly

Secret value setting: the participating entity with identity id_i picks $l_i \in \{1, 2, \ldots, n-1\}$as a secret value and computes $\mathscr{V}_i = l_i \cdot \mathscr{D}$ as a public key

Partial private key setting: for a participating entity with identity id_i, the KGC picks $\vartheta_i \in \{1, 2, \ldots, n-1\}$, computes $\mu_i = \vartheta_i \cdot \mathscr{D}$, calculates $\omega_?, = \vartheta_i + \mathscr{Q} h_x(id_i, \mathscr{V}_i, \mu_i)$, and sends $\Gamma_i = (\omega_?, ?_?)$ to entity with id_i via secure network

Private key setting: the participating entity, with identity id_i, sets $\mathscr{N}_i = (\Gamma_i, l_i)$of its private key.

Public key setting: the participating entity, with identity id_i, set$_s$ $\mathscr{Z}_i = (\mathscr{V}_i, \mu_i)$ of its public key.

Certificateless online/offline signature: the sender computations can be divided into the following two substeps, e.g., Online and Offline.

Offline phase: this part will be run over the server that is equipped with high resources and the construction step is carried out as follows:

(i) It picks $\in\in\{1,2,\ldots,n-1\}$ and computes $t==d\cdot\mathscr{V}_s$

(ii)Compute $\mathscr{P}$=h? (???, ??, ?, t) and $\mathscr{X}$=h? (???, $\mathscr{V}$?, ?, t)

(iii) Then, it gives (d, t, $\mathscr{P}$, $\mathscr{X}$) to the sensor nodes

Online phase: this part will be run on the sensor nodes and the construction step consists as follows:

(i)Compute $\mathscr{S} = l_s\cdot d-(l_s\cdot\mathscr{X}+\mathscr{P}\cdot w?)$

(ii) Set $\phi=(t,S)$ as a signature and send it to the receiver

Certificateless online/offline signature verification: upon reception ϕ, a receiver can verify $\mathscr{S}$ as follows:

(i) Compute $P=h_y(id_s,\mu_s,m,t)$ and $\chi=h_z(id_s,\mathscr{V}_s,m,t)$

(ii) Then, it checks if $S\cdot D=t\cdot\chi\mathscr{V}_s-\mathscr{P}(\mu_s+h_x(id_s,\mathscr{V}_s,\mu_s)\mathscr{K})$ holds

4.3. Correctness. The verifier/receptionist can verify the signature if the following computation is successfully processed:

So, if $P=h_y(id_s,\mu_s,m,t)$ and $X=h_z(id_s,\mathscr{V}_s,m,t)$, we acquire

$$\begin{aligned}\mathscr{S}.\mathscr{D} &= (l_s\cdot d-(l_s\cdot\mathscr{X}+\mathscr{P}\cdot w_s))D\\ &= (l_s\cdot d\cdot\mathscr{D}-(l_s\cdot\mathscr{X}+\mathscr{P}\cdot w_s))D\\ &= (\mathscr{V}_s\cdot d-(l_s\cdot\mathscr{X}+\mathscr{P}\cdot w_s)D\\ &= (t-(l_s\cdot\mathscr{X})\mathscr{D}-(\mathscr{P}.w_s)\mathscr{D}\\ &= (t-(l_s\cdot\mathscr{X}\cdot\mathscr{D})-(\mathscr{P}\cdot w_s)\mathscr{D}\\ &= (t-(\mathscr{V}_s\cdot\mathscr{X})-(\mathscr{P}\cdot(\vartheta_s+\mathscr{Q}h_x(id_s,\mathscr{V}_s,\mu_s))\mathscr{D})\\ &= (t-(\mathscr{V}_s\cdot\mathscr{X})-(\mathscr{P}\cdot(\vartheta_s.\mathscr{D}+\mathscr{Q}\cdot\mathscr{D}h_x(id_s,\mathscr{V}_s,\mu_s)))\\ &= (t-(\mathscr{V}_s\cdot\mathscr{X})-(\mathscr{P}\cdot(\vartheta_s\cdot\mathscr{D}+\mathscr{Q}\cdot\mathscr{D}h_x(id_s,\mathscr{V}_s,\mu_s))\\ &= (t-(\mathscr{V}_s.\mathscr{X})-(\mathscr{P}\cdot(\mu_s+h_x(id_s,\mathscr{V}_s,\mu_s).\mathscr{K})\cdot\end{aligned}\tag{1}$$

This validates the correctness of the proposed scheme.

5. Security Analysis

The purpose of this section is to explain the usefulness of the suggested method in resisting attacks.

Theorem 1. *The proposed scheme resists against an adaptive chosen message attack, if an adversary A_1 would not be able to solve the hyperelliptic curve discrete logarithm problem (HECDLP).*

Proof . Suppose there is a challenger ζ which helps A_1 to extract ℓ from the given instance $f=\ell\cdot\mathscr{D}$ of HECDLP. Further, to figure out HECDLP, ζ can set the master key secret key as $\mathscr{Q}=\ell$ and master public key as $\mathscr{K}=\ell\cdot\mathscr{D}$. Then, ζ generates ψ as a global parameter set and four empty lists ($L_{h_x}, L_{h_y}, L_{h_z}, L_k$) for holding the value of h_x, h_y, h_z, and keys.

Create ($\mathbf{id_i}$): after reception, Create id_i query, ζ selects $\alpha_i,\beta_i,l_i\in\{1,2,\ldots.\ldots,n-1\}$ and sets $h_x(id_i,\mathscr{V}_i,\mu_i)=-\beta_i$, $\mathscr{V}_i=l_i.\mathscr{D}$, and $\mu_i=\beta_i.\mathscr{K}-\alpha_i.\mathscr{D}$. Then, ζ answers in the following two steps:

(i) If $id_i\neq id_s$, with the identity $\mathbf{id_i}$, ζ outputs will be $(\Gamma_i=\nu_i,\mu_i)$, $\mathscr{N}_i=(\perp,l_i)$, and $\mathscr{Z}_i=(\mathscr{V}_i,\mu_i)$, respectively.

(ii) If $id_i\neq id_s$, with the identity $\mathbf{id_i}$, ζ outputs will be $(\Gamma_i=\nu_i,\mu_i)$, $\mathscr{N}_i=(\Gamma_i,l_i)$, and $\mathscr{Z}_i=(\mathscr{V}_i,\mu_i)$, respectively.

Thus, ζ included $(id_i,\mathscr{V}_i,\mu_i,\beta_i)$ into L_{h_x} and $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ into L_k.

Hash queries (h_x,h_y,h_z): after reception, Hash queries (h_x,h_y,h_z), ζ searches for the values $\Omega_i,\mathscr{P}_i,\mathscr{X}_i$ in lists L_{h_x},L_{h_y},L_{h_z}; if it finds in these lists then retunes to A_1; otherwise, the values $\Omega_i,\mathscr{P}_i,\mathscr{X}_i$ for each Hash query will select by ζ in a random manner and send it to the A_1.

Secret value setting queries: after reception, this query, then, (ζ) answers in the following two steps:

(i) If $id_i=id_s$, ζ aborts the process.

(ii) If $id_i\neq id_s$, ζ will look for $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ in L_k; if such a tuple is found, then it results in l_i; otherwise, ζ calls Create id_i query and gets $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ and then sends l_i to A_1.

Partial private key setting queries: after reception, this query, then, (ζ) answers in the following two steps:

(i) If $id_i=id_s$, ζ aborts the process.

(ii) If $id_i\neq id_s$, ζ will look for $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ in L_k; if such a tuple is found, then it sends $\Gamma_i$to A_1.

Public key setting queries: after reception, this query, then, (ζ) answers in the following two steps:

(i) If $id_i=id_s$, ζ aborts the process.

(ii) If $id_i\neq id_s$, ζ will look for $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ in L_k; if such a tuple is found, then it results in $\mathscr{Z}_i=(\mathscr{V}_i,\mu_i)$; otherwise, ζ calls Create id_i query and gets $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ and then sends $\mathscr{Z}_i=(\mathscr{V}_i,\mu_i)$ to A_1.

Public key replacement queries: after reception, this query, then, (ζ) will look for $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i)$ in L_k and replace $\mathscr{Z}_i$ by $\mathscr{Z}_i{}^*$ and include $(id_i,\Gamma_i,\mathscr{N}_i,\mathscr{Z}_i{}^*)$ into L_k. So, ζ sets $w_i=\perp$ and $\mathscr{N}_i=|\perp$.

Certificateless online/offline signature queries: after reception, this query, then, (ζ) checks. If $id_i=id_s$, then it aborts the process; otherwise, it will perform the following steps:

(i) ζ first gets access to L_{h_y},L_{h_z}, and L_k.

Offline phase:

(ii) It picks $d_i \in \{1, 2, \ldots, n-1\}$ and computes $d_i = d_i \cdot V_s$.

Online phase:

(iii) Compute $\mathcal{S}_i = l_i.d_i - (l_i.\mathcal{X}_i + \mathcal{P}_i.w_i)$ and it results as a signature $\Phi = t_i, S_i$.

Certificateless online/offline signature verification query: after reception, this query, then, (ζ) checks. If $id_i = id_s$, then it aborts the process; otherwise, it will perform the certificateless online/offline signature verification algorithm for the verifications of signature.

Forgery: at the end, A_1 results a lawful signature $(\Phi = t_i, S_i)$. If $id_i = id_s$, ζ aborts the process; otherwise, ζ checks for a list L_{h_x}, and according to forking lemma [], it generates another signature $\Phi^* = (\mathcal{S}_i^*, t_i)$. So, we have $\mathcal{S} \cdot \mathcal{D} = t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s.(\mu_s + \Omega_s\mathcal{K})$ and $\mathcal{S}_s^* \cdot \mathcal{D} = t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s^*.(\mu_s + \Omega_s\mathcal{K})$. We suppose that $\mu_s = \beta_s \cdot \mathcal{K} + \alpha_s \cdot \mathcal{D}$ and $\mathcal{K} = \ell \cdot \mathcal{D}$. So, when the subtractions between these two equations are performed, then we can get the following computations:

$$
\begin{aligned}
\mathcal{S}_i^* - \mathcal{S} \cdot \mathcal{D} &= \left(t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s\mathcal{K})\right)\left(t_s - X \cdot - \mathcal{V}_s - \mathcal{P}_s \cdot (\mu_s + \Omega_s\mathcal{K})\right),\\
\mathcal{S}_i^* \cdot \mathcal{D} - \mathcal{S} \cdot \mathcal{D} &= t_s - X\mathcal{V}_s - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s\mathcal{K}) - t_s - X \cdot \mathcal{V}_s + \mathcal{P}_s \cdot (\mu_s + \Omega_s\mathcal{K}),\\
\mathcal{S}_i^* \cdot \mathcal{D} - \mathcal{S} \cdot \mathcal{D} &= \mathcal{P}_s \cdot (\mu_s + \Omega_s\mathcal{K}) - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s\mathcal{K}),\\
(\mathcal{S}_i^* - \mathcal{S}) \cdot \mathcal{D} - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s \cdot \mathcal{D} &= (\mathcal{P}_s - \mathcal{P}_s^*(\beta_s + \Omega_s)\ell \cdot \mathcal{D},\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s) \cdot \mathcal{D} &= (\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)\ell \cdot \mathcal{D},\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s) &= (\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)\ell,\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s)/(\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)) &= \ell.
\end{aligned}
\tag{2}
$$

So, A_1 can solve HECDLP as $\ell = ((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s)/(\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)$, with the help of challenger ζ. □

5.1. Probability Analysis. Here, we define the following probability events:

(i) The winning probability of Create query must be greater than $(1 - Q_{h_x}Q_{\text{create}}/n)$

(ii) The succeeded probability of h_y must be greater than $(1 - Q_{h_y}/n)$

(iii) The succeeded probability of h_z must be greater than $(1 - Q_{h_y}/n)$

(iv) The succeeded probability of certificateless online/offline signature queries must be greater than (Q_s/n)

(v) $id_i = id_s$ satisfies with probability $(1/Q_{\text{create}})$

Note that Q_{create}, Q_{h_x}, Q_{h_y}, Q_{h_z}, and Q_s represent Create queries and Hash queries to h_x, h_y, h_z, and certificateless online/offline signature queries, respectively.

So, overall advantage of A_1 is towards its success as $\xi^* \geq (1 - Q_{h_x}Q_{\text{create}}/n)(1 - Q_{h_y}/n)(1 - Q_{h_z}/n)$ $((1/Q_{\text{create}})(Q_s/n)$.

Theorem 2. *By using the random oracle model, the proposed scheme resists against an adaptive chosen message attack, if an adversary A_2would not be able to solve the hyperelliptic curve discrete logarithm problem (HECDLP).*

Proof . Suppose there is a challenger ζ which helps A_1 to extract ℓ from the given instance $f = \ell \cdot \mathcal{D}$of HECDLP. Further, to figure out HECDLP, ζ picks b and sets master public key as $\mathcal{K} = b \cdot \mathcal{D}$. Then, ζ generates ψ as a global parameter set, and similar to Theorem 1, it picks four empty lists $(L_{h_x}, L_{h_y}, L_{h_z}, L_k)$ for holding the value of h_x, h_y, h_z, and keys.

Create (id_i): after reception, Create id_i query, ζ answers in the following steps:

(i) If $id_i = id_s$, ζ selects $\alpha_i, \Omega_i \in \{1, 2, \ldots, n-1\}$ and sets $h_x(id_i, \mathcal{V}_i, \mu_i) = \Omega_i$, $\mathcal{V}_i = \ell \cdot \mathcal{D}$, $w_i = \alpha_i + b\Omega_i$, and $\mu_i = \alpha_i \cdot \mathcal{D}$. So, it produces $(\Gamma_i = w_i, u_i)$, $\mathcal{N}_i = (\Gamma_i, \perp)$, and $\mathcal{Z}_i = (\mathcal{V}_i, \mu_i)$, respectively.

(ii) If $??_? \neq ??_?$, ζ selects $\alpha_i, l_i, \Omega_i \in \{1, 2, \ldots, n-1\}$ and sets $h_x(id_i, \mathcal{V}_i, \mu_i) = \Omega_i$, $\mathcal{V}_i = l_i.\mathcal{D}$, $w_i = \alpha_i b\Omega_i$, and $\mu_i = \alpha_i.\mathcal{D}$.

Thus, ζ included $(id_i, \mathcal{V}_i, \mu_i, \Omega_i)$ into L_{h_x} and $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ into L_k.

Hash queries ($\mathbf{h_x}, \mathbf{h_y}, \mathbf{h_z}$): these are the same as performed in Theorem 1.

Secret value setting queries: after reception, this query, then, (ζ) answers in the following two steps.

(i) If $\mathbf{id_i} = \mathbf{id_s}$, ζ aborts the process.

(ii) If $??_? \neq ??_?$, ζ will look for $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ in L_k; if such a tuple is found, then it results in l_i; otherwise, ζ calls Create id_i query and gets $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ and then sends l_i to A_2.

Partial private key setting queries: after reception, this query, then, (ζ) answers in the following two steps:

(i) If $\mathbf{id_i} = \mathbf{id_s}$, ζ aborts the process.

(ii) If $??_? \neq ??_?$, ζ will look for $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ in L_k; if such a tuple is found, then it sends $\Gamma_i$to A_2.

Public key setting queries: after reception, this query, then, (ζ) answers in the following two steps:

(ii) If $\mathbf{id_i} = \mathbf{id_s}$, ζ aborts the process.

(iii) If $??_? \neq ??_?$, ζ will look for $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ in L_k; if such a tuple is found, then it results in $\mathcal{Z}_i = (\mathcal{V}_i, \mu_i)$; otherwise, ζ calls Create id_i query and gets $(id_i, \Gamma_i, \mathcal{N}_i, \mathcal{Z}_i)$ and then sends $\mathcal{Z}_i = (\mathcal{V}_i, \mu_i)$ to A_2.

Certificateless online/offline signature queries: after reception, this query, then, (ζ) checks. If $\mathbf{id_i} = \mathbf{id_s}$, then it aborts the process; otherwise, it will perform the following steps:

(i) ζ first gets access to L_{h_y}, L_{h_z}, and L_k.

Offline phase:

(i) It picks $d_i \in \{1, 2, \ldots, n-1\}$ and computes $t_i = d_i \cdot \mathcal{V}_s$.

Online phase:

(ii) Compute $\mathcal{S}_i = l_i \cdot d_i - (l_i \cdot X_i + \mathcal{P}_{i\cdot} \cdot w_i)$ and it results as a signature $? = (t_?, \mathcal{S}_?)$.

Certificateless online/offline signature verification query: after reception, this query, then, (ζ) checks. If $id_i = id_s$, then it aborts the process; otherwise, it will perform the certificateless online/offline signature verification algorithm for the verifications of signature.

Forgery: at the end, A_1 results in a lawful signature $\phi = (t_?, \mathcal{S}_i)$. If $id_i = id_s$, ζ aborts the process; otherwise, ζ checks for a list L_{h_x}, and according to forking lemma [], it generates another signature $\Phi^* = (\mathcal{S}_i^*, t_i)$. So, we have $\mathcal{S} \cdot \mathcal{D} = t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s \cdot (\mu_s + \Omega_s \mathcal{K})$ and $\mathcal{S}_i^* \cdot \mathcal{D} = t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s \mathcal{K})$. We suppose that $\mu_s = \beta_s \cdot \mathcal{K} + \alpha_s \cdot \mathcal{D}$ and $\mathcal{K} = \ell \cdot \mathcal{D}$. So, when the subtractions between these two equations are performed, then we can get the following computations:

$$
\begin{aligned}
\mathcal{S}_i^* - \mathcal{S} \cdot \mathcal{D} &= \left(t_s - X \cdot \mathcal{V}_s - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s \mathcal{K})\right)\left(t_s - X \cdot - \mathcal{V}_s - \mathcal{P}_s \cdot (\mu_s + \Omega_s \mathcal{K})\right),\\
\mathcal{S}_i^* \cdot \mathcal{D} - \mathcal{S} \cdot \mathcal{D} &= t_s - X\mathcal{V}_s - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s \mathcal{K}) - t_s - X \cdot \mathcal{V}_s + \mathcal{P}_s \cdot (\mu_s + \Omega_s \mathcal{K}),\\
\mathcal{S}_i^* \cdot \mathcal{D} - \mathcal{S} \cdot \mathcal{D} &= \mathcal{P}_s \cdot (\mu_s + \Omega_s \mathcal{K}) - \mathcal{P}_s^* \cdot (\mu_s + \Omega_s \mathcal{K}),\\
(\mathcal{S}_i^* - \mathcal{S}) \cdot \mathcal{D} - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s \cdot \mathcal{D} &= (\mathcal{P}_s - \mathcal{P}_s^* (\beta_s + \Omega_s)\ell \cdot \mathcal{D},\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s) \cdot \mathcal{D} &= (\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)\ell \cdot \mathcal{D},\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s) &= (\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)\ell,\\
((\mathcal{S}_i^* - \mathcal{S}) - (\mathcal{P}_s - \mathcal{P}_s^*)\alpha_s)/(\mathcal{P}_s - \mathcal{P}_s^*)(\beta_s + \Omega_s)) &= \ell.
\end{aligned}
\tag{3}
$$

So, $\ell = (\mathcal{S}_i^* - \mathcal{S})/(\mathcal{X}^* - \mathcal{X})$ as the solution of HECDLP.

The probability analysis is same as Theorem 1 and as follows:

The utilized advantages of A_2 towards its success are as follows:

$\xi^* \geq (1 - Q_{h_x} Q_{\text{create}}/n)(1 - Q_{h_y}/n)(1 - Q_{h_z}/n)($ $(1/Q_{create})(Q_s/n)$. □

6. Cost Analysis

This section contrasts the efficiency of the proposed scheme with the existing equivalents suggested by the schemes of Yu and Tate [25], scheme 1, Yu and Tate [25], scheme 2, Wu et al. [26], and Addobea et al. [27].

6.1. Computational Cost. Table 2 displays the key results derived from the analysis. Elliptic curve scalar multiplication and bilinear pairings are used in the existing schemes, all of which are more expensive alternatives. Therefore, we add the multiplication of the hyperelliptic divider. Observations have shown that the time it takes for a single scalar multiplication to be processed differs considerably: elliptic curve point multiplication (ECPM), 0.97 milliseconds; bilinear pairing (P), 14.90 ms; pairing-based point multiplications (BPM), 4.31 ms; and modular exponentiation (E), 1.25 ms [16]. The Multiprecision Integer and Rational Arithmetic C Library (MIRACL) [30] is used to calculate the performance of the proposed system. It checks roughly 1000 times the runtime of specific cryptographic operations. A workstation with the following requirements is used for evaluating simulation results: Intel Core i7-4510U Processor @ 2.0 GHz, 8 GB RAM, and Windows 7 Home Standard 64-bit Operating System [29]. The hyperelliptic curve divisor multiplication (HM) is believed to be 0.48 milliseconds in length due to a smaller key size of 80 bits [31–34]. It is apparent from the results in Tables 2 and 3 that our solution is much more effective in terms of the computational cost as shown in Figure 2.

6.2. Communication Cost. This subsection is aimed at discussing the comparison results from the perspective of communication costs. The proposed approach is compared with the existing schemes presented by Yu and Tate [25] scheme 1, Yu and Tate [25] scheme 2, Wu et al. [26], and

Table 2: Computational cost.

Schemes	Signing	Verifying	Total
Yu and Tate [25] scheme 1	$1E + 3BPM$	$3E + 4BPM$	$4E + 7BPM$
Yu and Tate [25] scheme 2	$2E + 3BPM$	$3E + 3BPM$	$5E + 6BPM$
Wu et al. [26]	3BPM	2P + 2BPM	2P + 5BPM
Addobea et al. [27]	3 BPM	3P + 4BPM	3P + 7BPM
Proposed	4HM	3HM	7HM

Table 3: Computational cost in milliseconds.

Schemes	Signing	Verifying	Total (ms)
Yu and Tate [25] scheme 1	14.18	20.99	35.17
Yu and Tate [25] scheme 2	15.43	16.68	32.11
Wu et al. [26]	12.99	38.42	51.41
Addobea et al. [27]	12.99	61.94	74.93
Proposed	1.92	1.44	3.36

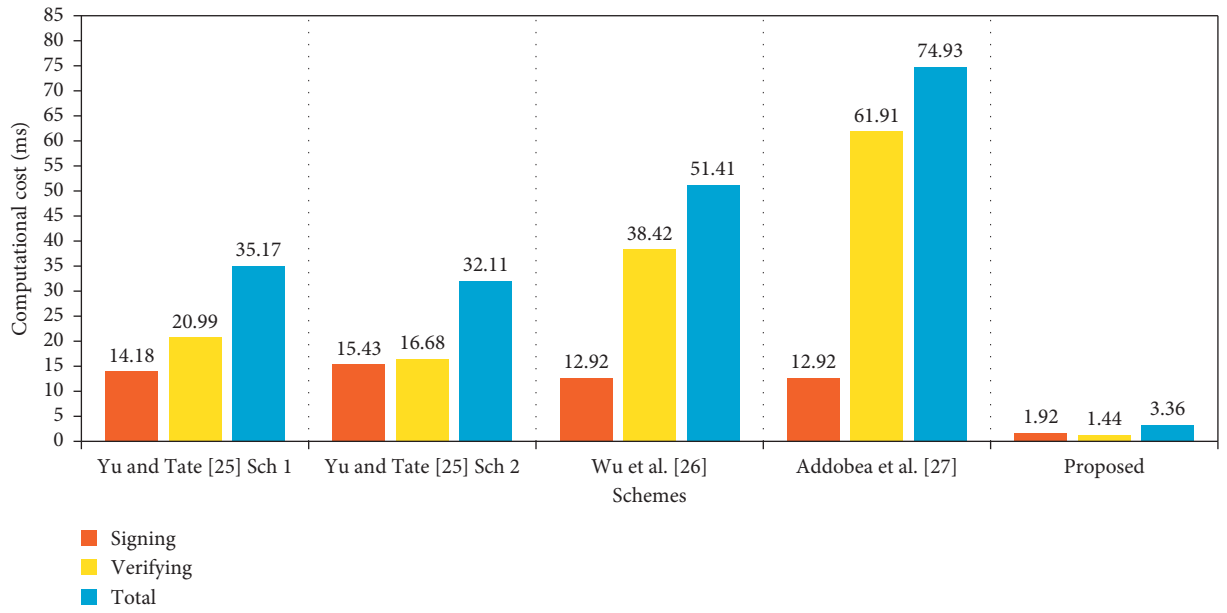

Figure 2: Computational cost (in ms).

Table 4: Communication cost in bits.

Schemes	Communication cost	Communication cost in bits
Yu and Tate [25] scheme 1	$3\|G\| + \|m\|$	4096
Yu and Tate [25] scheme 2	$3\|G\| + \|m\|$	4096
Wu et al. [26]	$3\|G\| + \|m\|$	4096
Addobea et al. [27]	$3\|G\| + \|m\|$	4096
Proposed	$2\|n\| + \|m\|$	1184

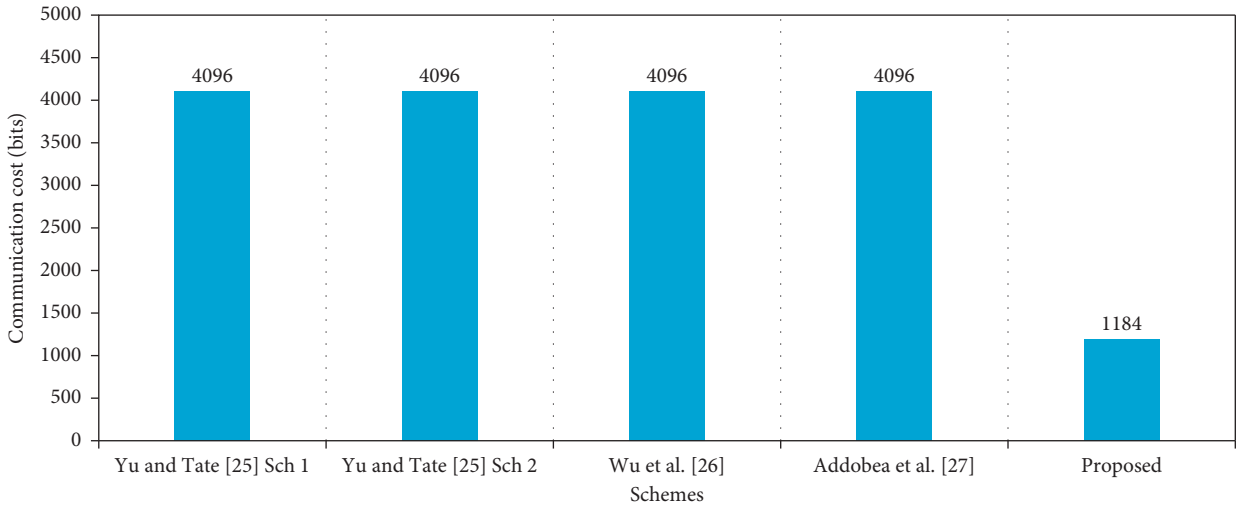

Figure 3: Communication cost (in bits).

Addobea et al. [27]. In comparative analysis, the variables, i.e. $|\mathbf{G}| = 1024$ bits, $|m| = 1024$ bits, and $|n| = 80$ bits, along with the respective values, are depicted in Table 4 and illustrated in Figure 3.

7. Conclusion

The Internet of Health Things (IoHT) plays an important role as an extension of the Internet of Things (IoT) in the remote data-sharing of multiple physical processes, such as patient monitoring, treatment progression, observation, and consultation. In IoHT, multiple sensors, actuators, and controllers allow communication, computation, and interoperability, thus providing seamless connectivity with efficient resource utilization. However, for the majority of IoHT implementations, conventional cryptographic methods are not feasible due to the energy constraints of low-power embedded devices. Therefore, we suggested a lightweight security scheme in this article, using the idea of the hyperelliptic curve (HEC), called an online-offline certificateless signature scheme. In the limited key size, the HEC solution is powerful and is also acceptable for IoHT environments. The formal security analysis shows the intensity of the proposed approach in avoiding multiple attacks. In addition, after a comparative comparison with the main existing schemes, the proposed scheme proved to be efficient in terms of both computational and communication costs.

An extension of the proposed scheme is required that offers encryption and digital signature in one go. We also plan to improve the security by adding some other aspects of formal analysis, such as the real-or-random (ROR) for the solutions against different attacks. All these aspects are in the development phase and will be taken into account in our future work.

Data Availability

All data generated or analyzed during this study are included in this published article.

Conflicts of Interest

The authors declare no conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] J. J. P. C. Rodrigues, D. B. De Rezende Segundo, H. A. Junqueira et al., "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 et al., "An IoT-aware architecture for smart healthcare systems," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 515–526, 2015.

[4] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: an overview," *Journal of Industrial Information Integration*, vol. 1, pp. 3–13, 2016.

[5] M. W. Woo, J. W. Lee, and K. H. Park, "A reliable IoT system for personal healthcare devices," *Future Generation Computer Systems*, vol. 78, pp. 626–640, 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 Generation Computer Systems*, vol. 78, pp. 659–676, 2018.

[7] F. Firouzi, A. M. Rahmani, K. Mankodiya et al., "Internet-of-things and big data for smarter healthcare: from device to architecture, applications and analytics," *Future Generation Computer Systems*, vol. 78, pp. 583–586, 2018.

[8] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[9] S. Ullah, L. Marcenaro, and B. Rinner, "Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications," *Sensors*, vol. 19, no. 2, p. 327, 2019.

[10] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proceedings of the of the CRYPTO 1984*, pp. 19–23, 1984.

[11] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 80–89, 2018.

[12] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. H. Islam, "Secure cls and cl-as schemes designed for vanets," *The Journal of Supercomputing*, pp. 1–23, 2019.

[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, 2018.

[14] M. Yu, J. Zhang, J. Wang et al., "Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, Article ID 155014771881584, 2018.

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

[16] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, Article ID 8405879, 17 pages, 2017.

[17] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2017.

[18] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, no. 6, 2018.

[19] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *International Journal of Advanced Studies of Scientific Research*, vol. 3, no. 8, 2019.

[20] V. S. Naresh, R. Sivaranjani, and N. V.E.S. Murthy, "Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor networks," *International Journal of Communication Systems*, vol. 31, no. 15, p. e3763, 2018.

[21] A. U. Rahman, I. Ullah, M. Naeem et al., "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, p. 5, 2018.

[22] V. D. Ta, C.-M. Liu, and G. W. Nkabinde, "Big data stream computing in healthcare real-time analytics," in *IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, China, July 2016.

[23] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," *Advances in Cryptology—CRYPTO' 89 Proceedings*, pp. 263–275, 1990.

[24] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," *Advances in Cryptology-CRYPTO 2001*, vol. 2139, pp. 355–367, 2001.

[25] P. Yu and S. R. Tate, "Online/offline signature schemes for devices with limited computing capabilities," in *The Cryptographers' Track at the RSA Conference 2008 (CT-RSA 2008)*, San Francisco, CA, USA, April 2008.

[26] T. Wu, Y. Chen, and K. Lin, "ID-based online/offline signature from pairings," in *Proceedings of the International Computer Symposium (ICS2010)*, Tainan City, Taiwan, December 2010.

[27] A. A. Addobea, J. Hou, and Q. Li, "MHCOOS: An Offline-Online Certificateless Signature Scheme for M-Health Devices," *Security and Communication Networks*, vol. 2020, Article ID 7085623, 12 pages, 2020.

[28] S. K. H. Islam and G. P. Biswas, "Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography," *International Journal of Computer Mathematics*, vol. 90, no. 11, pp. 2244–2258, 2013.

[29] 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, p. 16, 2019.

[30] Shamus Sofware Ltd. http://github.com/miracl/MIRACL.

[31] M. A. Khan, I. Ullah, S. Nisar et al., "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.

[32] 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, p. 30, 2020.

[33] M. A. Khan, I. Ullah, S. Nisar et al., "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, vol. 2020, Article ID 8861947, 15 pages, 2020.

[34] 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.