future internet

MDPI

Article

An Optimal Authentication Scheme through Dual Signature for the Internet of Medical Things

Zainab Jamroz [1], Insaf Ullah [2], Bilal Hassan [1], Noor Ul Amin [1], Muhammad Asghar Khan [2], Pascal Lorenz [3,*] and Nisreen Innab [4]

[1] Department Computer Science and Information Technology, Hazara University, Mansehra 21300, Pakistan; zainabjamroz32@gmail.com (Z.J.); bilalhassan797aa@gmail.com (B.H.); namin@hu.edu.pk (N.U.A.)
[2] Faculty of Engineering Sciences and Technology, Hamdard University, Islamabad 44000, Pakistan; insaf.ullah@hamdard.edu.pk (I.U.); m.asghar@hamdard.edu.pk (M.A.K.)
[3] Department of Network and Telecommunication, University of Haute Alsace, 68008 Colmar, France
[4] Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, P.O. Box 71666, Riyadh 11597, Saudi Arabia; ninnab@mcst.edu.sa
* Correspondence: pascal.lorenz@uha.fr

Abstract: The Internet of Medical Things (IoMT) overcomes the flaws in the traditional healthcare system by enabling remote administration, more effective use of resources, and the mobility of medical devices to fulfil the patient's needs. The IoMT makes it simple to review the patient's cloud-based medical history in addition to allowing the doctor to keep a close eye on the patient's condition. However, any communication must be secure and dependable due to the private nature of patient medical records. In this paper, we proposed an authentication method for the IoMT based on hyperelliptic curves and featuring dual signatures. The decreased key size of hyperelliptic curves makes the proposed scheme efficient. Furthermore, security validation analysis is performed with the help of the formal verification tool called Scyther, which shows that the proposed scheme is secure against several types of attacks. A comparison of the proposed scheme's computational and communication expenses with those of existing schemes reveals its efficiency.

Keywords: dual signature; internet of medical things; authentication; scyther tool; hyperelliptic curve

Citation: Jamroz, Z.; Ullah, I.; Hassan, B.; Amin, N.U.; Khan, M.A.; Lorenz, P.; Innab, N. An Optimal Authentication Scheme through Dual Signature for the Internet of Medical Things. *Future Internet* **2023**, *15*, 258. https://doi.org/10.3390/fi15080258

Academic Editor: Michael Sheng

Received: 8 June 2023
Revised: 22 July 2023
Accepted: 27 July 2023
Published: 30 July 2023

1. Introduction

The Internet of Things (IoT) has attracted a lot of attention recently and can connect any device to any other device, anytime, anywhere, by using any communication channel or service [1,2]. The IoT has many applications, as it is used in agriculture, smart homes, transportation, health care, etc. In this paper, we focus on healthcare because, due to the fast rise of the population, an IoT-based healthcare system will solve health-related issues in every person's life. Conventional healthcare systems cannot solve the demands of such a vast population [3], which necessitates additional resources and people. Due to manual management, there is always the possibility of a mistake that can be catastrophic for the patient [4]. The Internet of Medical Things (IoMT) offers a solution to these issues, which attempts to address the problems experienced by the traditional healthcare system by lowering manual involvement and increasing the system's precision and adaptability. The IoMT refers to the linking of healthcare equipment that can interact via a network without requiring human involvement [5].

As seen in Figure 1, the IoMT refers to the interconnection of medical equipment, such as wearables, smart chairs, smart belts, sphygmomanometers, and diabetic devices, among others. Wearable gadgets consist of smartwatches, fitness trackers, and blood pressure monitoring devices, among others, that continuously measure the pulse, blood pressure, and other health data. In the event of a sudden drop in a patient's pulse or blood pressure, an alarm is transmitted to the caretaker, who then dispatches an ambulance to the

patient's residence [6]. The IoMT enables the use of chairs with integrated sensors capable of detecting movements and is especially good for older people, who are more susceptible to falling. If a patient exits the chair, the smart chair recognizes it and, based on a risk assessment, generates an alarm to notify the nursing staff [7].

Similarly, tracking sensors are incorporated into smart belts to monitor the mobility of elderly patients. Patients with diabetes and hypertension require continual glucose and blood pressure monitoring; so, IoT-based diabetes gadgets and sphygmomanometers make remote monitoring simple by measuring glucose and blood pressure and making the data accessible in real-time to doctors via health applications. Further, remote monitoring allows seriously ill individuals to avoid hospitalization; they can communicate with their doctor and obtain a prescription using the health application [8]. In addition to the above-mentioned benefits, the health applications continually transmit patient data to the hospital, where physicians evaluate it to identify variances, which can permit the physician to monitor the patient's status and expedite his recovery. Similarly, use of the IoMT decreases manual involvement while performing machine-to-machine communication; again, the diagnostic centre sends an electronic medical report to a patient's mobile phone [9,10]. All IoMT devices are connected to cloud storage for data storage and subsequent analysis.

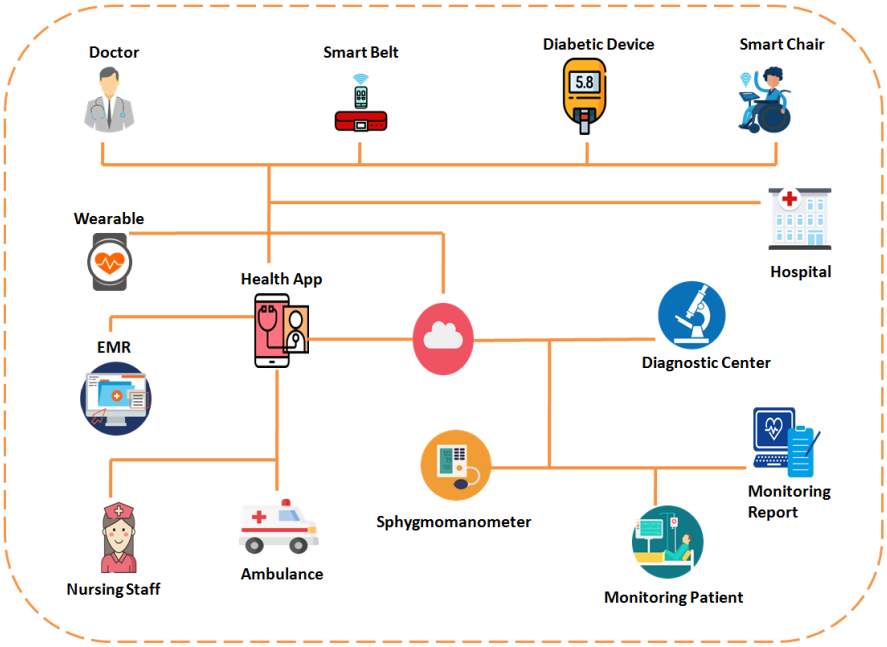

Figure 1. Internet of Medical Things (IoMT) [9].

Despite the numerous uses and benefits of the IoMT, there are a few issues, such as security, data privacy, and authentication, which must be handled. The above-mentioned problems can be solved through a dual digital signature, which can only authorize the legitimate user to access and use the health care data. A dual signature does not imply that there are two signatures; rather, it is a particular sort of signature that focuses on linking two distinct messages (information) meant for two separate recipients [11]. A dual-signature approach may be created using Rivest-Shamir-Adleman (RSA), elliptic-curve cryptography (ECC), and hyper elliptic-curve cryptography (HECC). Due to the 1024-bit key length, using a dual signature with RSA requires a lot of storage space, which can raise computation costs and communication overhead [12]. ECC, on the other hand, only needs 160 bits, which needs lower computational and transmission costs than RSA while still being able to offer the same level of security. Despite having better performance than RSA, ECC still has significant overhead costs associated with calculation and transmission. Since IoT devices are low-power and unable to do extensive processing, it is required somewhat to reduce the cost of computation and communication overhead. This feature is provided

by HEC, which utilizes only 80 bits of store space, reducing the amount of computing work and the cost of transmission while delivering an equivalent level of security [13].

Motivation and Contributions

Several dual-signature schemes have been presented in the published research; however, the majority of these schemes relied on RSA, ECC, etc., which resulted in significant computational and communication costs, or some of them were not evaluated using any formal security validation tool, which is very necessary to test the authenticity of the scheme. To overcome these issues, we propose a scheme entitled "the optimal authentication scheme through a dual signature for the IoMT". We have listed below the research contributions of the proposed scheme:

- We propose a dual-signature scheme using hyperelliptic curve cryptography (HECC), an advanced form of elliptic curve cryptography (ECC) that provides the same level of security as ECC with a key size that is half that of ECC.
- We provide an informal security analysis study in terms of authentication, integrity, and non-repudiation, and demonstrate that the proposed scheme is resistant to these attacks.
- In addition, we evaluated the security criteria using the security validation tool Scyther, and the results indicate that the proposed scheme is secure against man-in-the-middle attacks.
- Finally, we compared the performance of the proposed scheme to that of related schemes from the literature and observed that the proposed scheme lowered computation and communication costs.

The rest of the article is organized as follows. The preliminaries are detailed in Section 2. The related work and network model are included in Sections 3 and 4. Sections 5 and 6 contain the proposed dual signature scheme and informal security analysis. Sections 7 and 8 provide a performance evaluation in terms of the computational cost and communication overhead with existing schemes. Section 9 contains the concluding remarks and is followed by Appendices A and B.

2. Preliminaries

2.1. Hyperelliptic Curve

A hyperelliptic curve is a generalized form of an elliptic curve with a genus of ≥ 1. In cryptography, this sort of curve is considered a viable approach because its vital length and parameter size is significantly smaller than for an elliptic curve.

Let *Hec* be the hyperelliptic curve over the finite field $\mathfrak{f}$; the equation of hyperelliptic curve '*Hec*' over the field '$\mathfrak{f}$' having genus '$\mathfrak{g}$' is shown in the equation below:

$$Hec \ : u^2 + h(v)u = f(v)$$

In the equation above, $h(v)$ is a polynomial of degree $\leq \mathfrak{g}$, while $f(v)$ is a polynomial of degree $2\mathfrak{g} + 1$. The above equation represents a nonsingular curve, and it can verify the given curve equation and two partial derivatives $2u + h(v) = 0$, $h'(\mathrm{v})\mathrm{u} = 0$.

2.2. Divisor

The divisor D in the hyperelliptic curve is a finite sum (formal) of points [14]. It is shown in the equation below as follows:

$$\mathrm{D} = \sum_{p \in H} (c_p \mathrm{p})$$

In addition, the points on the hyperelliptic curve are not similar to the elliptic curve because they do not form a group; instead, they form an Abelian group, which is called the Jacobean Group J_H [15]. The order of J_H is

$$\left|(\sqrt{\mathrm{p}}-1)^{2\mathrm{g}} \leq \mathcal{O}\left(J_H\left(\mathrm{u_p}\right)\right) \leq (\sqrt{\mathrm{p}}+1)^{2\mathrm{g}}\right|$$

2.3. HECDLP

Suppose a divisor D was chosen randomly from the Jacobean group. The given equation is

$$D_2 = L \,.\, D1$$

where L is the integer, and finding L is called the hyper-elliptic curve discrete logarithm problem (HECDLP) [16].

2.4. Syntax

The following steps will be an explanation of the construction steps of our proposed scheme.

Setup: The central authority (CA) will be responsible for executing this step, in which he/she can select a hash function and hyperelliptic curve. Then, CA makes and publishes public parameters set to the network publicly.

Key generation: This step will be executed by a user with an identity (ID) that generates his public and private key ($\mathrm{PB_{ID}}$, φ_{ID}).

Dual signature: The IoMT Devices can execute this phase, in which they can generate a ciphertext and dual signature on medical data. Then, the tuple (DS, χ, $\mathcal{Q}$, C, θ) of the dual signature is sent to the PDA.

Personal digital assistant (PDA). Verification: The personal digital assistant can execute this phase and accept the tuple (DS, χ, $\mathcal{Q}$, C, θ) only if $\mathfrak{h} = \varphi_{\mathrm{PDA}}.\mathrm{DS}.(\chi + \mathrm{PB_{IoMT}})$ is qualified.

AP decryption and verification: When (DS, χ, $\mathcal{Q}$, C, θ) is received by the AP, then it can perform the decryption process to recover m and then perform the process for verifying the dual signature, if the process is successful then it will be able to accept the message, otherwise it will generate an error message.

3. Related Work

After its induction in the SET protocol, researchers have proposed various schemes based on dual signatures over the years. In 2008, Wu et al. [17] put forward an offline micropayment mechanism based on the dual signature, in which they make sure a valid coin must be signed by both parties, i.e., issuers and coin owners. The limitation of this scheme is its high computational cost due to the employment of RSA encryption. An authentication scheme for the wireless network was proposed in [18], which comprises two stages, i.e., authentication in the Internet Key Exchange (IKE) based on a dual signature involves stage 1. In stage 2, a different session is generated between two wireless nodes without affecting stage 1. This scheme results in the sender's authentication, provides confidentiality of user sessions, and is resistant to replay attacks. The drawback of the designed approach is that authentication using the dual signature in stage 1 results in high computational overhead.

A dual signature scheme based on the elliptic curve digital signature algorithm (ECDSA) in the SET protocol was proposed in [12]. This approach joins two messages that are meant for distinct recipients. One receiving party is unaware of the other recipient's information. However, it still suffers from high computational costs and the communication overhead due to the use of ECDSA. Cai et al. [19] designed a multi-domain authentication protocol based on the dual signature, which allows direct authentication between two parties while excluding the need for a third party. The developed approach provides not only privacy but also secure authentication for multiple domains.

Furthermore, this scheme provides faster access to resources, thereby solving bottleneck issues in the network and providing key escrow resilience in identity-based authentication protocols. This scheme's performance is its major drawback because it results in higher computational and communication costs. In [20], an online internet voting protocol scheme based on dual signature was put forth, enabling the voters to cast their ballot by simply scanning their thumbprint. Following the designed approach, once a voter has been successfully authenticated from the database, he can acquire a poll. When a voter submits a vote, the system performs these three operations (1) generates a dual signature (2) authenticates server envelope and (3) voting server envelope. The system sends an authentication server envelope concatenated with the voting server envelope to the authentication server using the transmission link. The received envelope is validated by the authentication server, which then delivers it to the voting server for the final tally. This designed scheme provides key properties such as privacy, anonymity, eligibility, and verifiability, which are necessary constraints for any online voting system.

Moreover, this approach is better than a blind signature regarding security and computational costs. However, this scheme's primary problem is the inability to display voting information that includes the voter's identity unless both the authentication server and the voting server desire to know this information. An elliptic curve digital signature algorithm (ECDSA) for IoMT based on dual signature was proposed by Cano et al. [21] to ensure privacy and authentication. This scheme utilizes ECDSA to compute signatures and simplify the process; however, instead of IoMT devices, signature verification is performed by edge computing devices because it is a task that demands substantial computational resources. The advantage of this work is message authentication, data privacy, and security against data tampering. This work exhibits flaws in the form of high computational costs and communication overhead, and a lack of formal security validation.

Zhang and Xie [22] proposed a dual blind signature for quantum computing; however, the proposed scheme is not appropriate for IoMT devices with resource constraints. Similarly, Gana et al. [23] proposed a dual signature for quantum computing; however, the proposed scheme is not appropriate for IoMT devices with resource constraints and has not been validated by a formal security validation tool. Shi et al. [24] proposed a dual signature for quantum computing; however, the proposed scheme is not appropriate for IoMT devices with resource constraints and has not been validated by a formal security validation tool.

All the above-mentioned schemes are not validated through some formal validation tools such as Scyther, which can be harmful due to some invisible security flaws. In addition, these schemes are unsuitable for resource-hungry IoMT devices because they utilize higher computational costs and more communication overheads.

4. Network Model

Figure 2 depicts the workflow of the proposed scheme, which comprised four major entities: medical sensing devices or IoMT devices, central authority (CA), personal digital assistant (PDA), and application providers (AP). The CA is a trusted third party whose responsibility is to establish the system by producing the parameters transmitted to the other three network entities. Wearables, smart belts, smart thermometers, smart oximeters, smart chairs, smart glucose gadgets, and smart sphygmomanometers are some examples of implanted IoMT devices. These devices continually monitor personal health information (PHI) by measuring the pulse rate, heart rate, body temperature, body movement, oxygen level in the body, blood pressure, breathing rate, and glucose levels, among others. In addition to data collection, connecting IoMT devices is a crucial duty for which wireless communication technologies such as Zigbee are utilized. Depending on the network's distance and characteristics, Bluetooth 4.0, Wi-Fi, and 5G can also be used. The communication methods are appropriate for wireless sensor networks due to their low cost and low power consumption [25,26]. The IoMT devices produce a dual signature and transfer it with the encrypted PHI to the PDA. When a PDA receives a message with a dual signature,

it checks the dual signature before forwarding the message to application providers (AP). The application provider (AP) is responsible for continually and effectively monitoring the patient's condition. When receiving a letter from a PDA, the application provider checks the dual signature and then decrypts the PHI-containing message. The doctors and nurses who are part of the application provider and linked to the hospital server act depending on the PHI received.

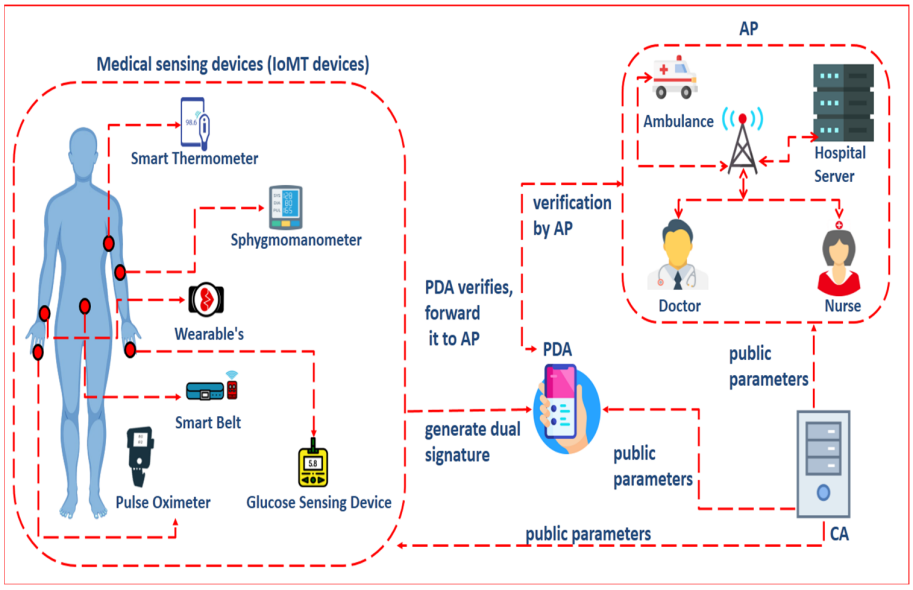

Figure 2. Proposed scheme.

5. Proposed Dual Signature Scheme

Our proposed dual signature scheme can be made by utilizing the following five sub-phases. All the symbols used in the proposed dual signature scheme are explained in Table 1. Figures labelled Appendices A and B depict formal validation of proposed protocol utilizing Scyther.

Table 1. Symbols used in the proposed scheme.

S. No	Symbols	Description
1	PB_{IoMT}	Public key of IoMT device
2	φ_{IoMT}	Private key of IoMT device
3	$\mathcal{D}$	Divisor on hyper elliptic curve
4	F^n	A finite field of hyper elliptic curve
5	PB_{PDA}	Public key of PDA
6	φ_{PDA}	Private key of PDA
7	PB_{AP}	Public key of AP
8	φ_{AP}	Private key of AP
9	m	Plaintext that contains patient health information
10	C	Cipher text that contains patient health information in encrypted form
11	$\mathscr{h}$	Used as a hash function
12	n	Represents a large number and its value as $n \geq 2^{80}$
13	DS	Represents a dual signature

5.1. Setup

Here, the central authority (CA) can select $\mathscr{k}$ as a hash function and genius 2 hyperelliptic curve with 80 bits key size and its finite field F^n, where $n \geq 2^{80}$. Then, it publishes these parameters to the network publicly.

5.2. Key Generation

We divide this phase into sub-phases as follows:

5.3. Key Generation for IoMT Devices

They compute $PB_{\text{IoMT}} = \varphi_{\text{IoMT}}.\mathcal{D}$ and set PB_{IoMT} as their public key and φ_{IoMT} as their private key.

5.4. Key Generation for PDA

They compute $PB_{\text{PDA}} = \varphi_{\text{PDA}}.\mathcal{D}$ and set PB_{PDA} as its public key and φ_{PDA} as its private key.

5.5. Key Generation for AP

They compute $PB_{\text{AP}} = \varphi_{\text{AP}}.\mathcal{D}$ and set PB_{AP} as the public key and φ_{AP} as the private key.

5.6. Dual Signature

Here, IoMT Devices do the following steps

- Compute $\mathfrak{h} = \alpha.PB_{\text{PDA}}$ and $\theta = \alpha.PB_{\text{AP}}$, where α belongs to F^n, which is private to IoMT devices
- Compute $\mathcal{Q} = \mathscr{k}(m)$, $C = \mathcal{E}_{PB_{\text{AP}}}(m)$, and $\chi = \mathcal{Q}.\mathcal{D}$
- Compute $\text{DS} = {}^{\alpha}/_{\mathcal{Q} + \varphi_{\text{IoMT}}}$ and send $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ to PDA.

5.7. PDA Verification

When $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ are received by the PDA, then it can do the following computations for its verification.

- Compute $\mathfrak{h} = \varphi_{\text{PDA}}.\text{DS}.(\chi + PB_{\text{IoMT}})$ if it is qualified then it accepts the signature
- Then send $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ to AP

5.8. AP Decryption and Verification

When $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ received by AP, then it can do the following computations for decryption and verification.

- It decrypts $m = \text{D}_{\varphi_{\text{AP}}}(C)$, where φ_{AP} is the private key of AP.
- It accepts the DS, when $\theta = \varphi_{\text{AP}}.\text{DS}.(\chi + PB_{\text{IoMT}})$ is satisfied.

5.9. Correctness

When $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ are received by the PDA, then it can do the following computations for its verification: $\mathfrak{h} = \varphi_{\text{PDA}}.\text{DS}.(\chi + PB_{\text{IoMT}})$
$= \varphi_{\text{PDA}}.\text{DS}.(\chi + PB_{\text{IoMT}}) = \varphi_{\text{PDA}}.{}^{\alpha}/_{\mathcal{Q} + \varphi_{\text{IoMT}}}.(\mathcal{Q}.\mathcal{D} + \varphi_{\text{IoMT}}.\mathcal{D})$
$= \varphi_{\text{PDA}}.{}^{\alpha.\mathcal{D}}/_{\mathcal{Q} + \varphi_{\text{IoMT}}}.(\mathcal{Q} + \varphi_{\text{IoMT}}) = \varphi_{\text{PDA}}.\alpha.\mathcal{D} = \alpha.PB_{\text{PDA}}$; hence, it is proved.

In addition, when $(\text{DS}, \chi, \mathcal{Q}, C, \theta)$ are received by the AP, then it can do the following computations for its verification: $\theta = \varphi_{\text{AP}}.\text{DS}.(\chi + PB_{\text{IoMT}})$
$= \varphi_{\text{AP}}.\text{DS}.(\chi + PB_{\text{IoMT}}) = \varphi_{\text{AP}}.{}^{\alpha}/_{\mathcal{Q} + \varphi_{\text{IoMT}}}.(\mathcal{Q}.\mathcal{D} + \varphi_{\text{IoMT}}.\mathcal{D})$
$= \varphi_{\text{Ap}}.{}^{\alpha.\mathcal{D}}/_{\mathcal{Q} + \varphi_{\text{IoMT}}}.(\mathcal{Q} + \varphi_{\text{IoMT}}) = \varphi_{\text{AP}}.\alpha.\mathcal{D} = \alpha.PB_{\text{AP}}$; hence, it is proved.

6. Informal Security Analysis

In this section, we perform an informal security analysis of our proposed scheme in which we consider the Dolev-Yao threat model. In this model we assume that the attacker

can attack our scheme in an open channel and in response our scheme provides important security attributes such as data privacy, authentication, prevention of data tampering attack, data integrity, resilience against replay attack, and nonrepudiation.

6.1. Data Privacy

Our designed dual signature scheme successfully provides data privacy by only allowing the AP to view the patient's health information (m) while hidden (m) from the PDA. Suppose an adversary makes an attempt to alter or decrypt (m). In that case, he/she cannot do so because (m) is encrypted using PB_{AP} and due to the hard nature of hyper elliptic curve discrete logarithm problem, it is impossible for an adversary to gain φ_{AP}.

6.2. Replay Attack

Suppose an intruder eavesdrops on a communication channel, intercepts the message, and then replays the same message to gain access to communication. We use fresh nonce in our scheme to thwart such an attack. According to our approach, whenever data is transmitted by IoMT devices, a nonce χ which is equal to $\mathcal{Q}.\mathcal{D}$ is transmitted along with it. Due to use of $\mathcal{Q}$, which is the hash of (m), an intruder cannot create a fresh nonce by themselves. Hence, in this way, it effectively counters replay attacks by satisfying the message's freshness requirement.

6.3. Authentication

In our scheme, the employment of a dual signature (DS) ensures the authenticity of the sending party. To compute the DS, in addition to $\mathcal{Q}$, the secret key of the IoMT $(\varphi_{\mathrm{IoMT}})$ and α are used. However, to accomplish authentication, it is not viable for an attacker to generate a DS because φ_{IoMT} and α are only known to IoMT devices.

6.4. Data Tampering

An attacker can use any unauthorized means to modify the information, which can directly impact the integrity of the whole system. To overcome such an attack, we have made use of the hash function $\mathscr{h}$, so when an attacker aims to tamper with the signature (DS) or the information (m), it will be spotted during verification since the computed hash will be entirely different. However, if an attacker tries to decrypt the cipher text C, it is not feasible because m is encrypted using PB_{AP} and logically an attacker cannot generate the decryption key φ_{AP}. Therefore, our scheme effectively protects against data tampering.

6.5. Integrity

An adversary might modify the contents of plaintext, which will result in loss of integrity. In our scheme, IoMT devices compute $\mathcal{Q}$, which is the hash of plaintext m and send that to the intended receiver along with the cipher text C and signature DS. Suppose an adversary tries to modify the contents of the cipher text. In that case, the resulting hash value will be completely different due to the collision-resistant property of the hash function. Hence, our scheme effectively provides integrity.

6.6. Nonrepudiation

According to nonrepudiation, a party cannot deny the information it has transmitted or received. Our mechanism offers nonrepudiation by ensuring that each participant successfully completes the verification process via a signature verification mechanism. Therefore, once information has been conveyed via communication, a party cannot deny it. Therefore, in such a way our scheme effectively provides this crucial security feature.

7. Computational Cost

A scheme's computational cost is usually measured by the time taken by the scheme's various operations. In this section, we compare our scheme with Cano et al. [21] with respect to the computational cost. For this purpose, we have neglected less expensive

operations and only considered costly operations in terms of time. For elliptic curve-based schemes, we have taken into account elliptic curve modular multiplication ($\mathcal{EMM}$). For the hyperelliptic curve, we have taken into account the hyperelliptic curve modular multiplication ($\mathcal{HEMM}$). According to [27], single $\mathcal{EMM}$ takes 2.848 milliseconds, and we assume that the single $\mathcal{HEMM}$ will takes 1.424 milliseconds. The experiment is conducted through the following hardware and software resources:

- Raspberry PI 4B (2019)
- CPU Architecture: 64 b
- Processor: 1.5 GHz Quad-core
- OS: Ubuntu 20.04.2 LTS with 8 GB memory

Table 2 depicts a computational cost comparison of Cano et al. [21] with our proposed scheme in terms of major operations. Table 3 provides the cost comparison in seconds and makes it evident that the proposed scheme outperforms the existing scheme. Additionally, it also indicates the cost reduction determined by the formula [28]. A graphical illustration of this comparison is also provided in Figure 3.

Table 2. Comparison of computational cost.

Schemes	IoMT Devices	PDA	AP	Total
Cano et al. [21]	2 $\mathcal{EMM}$	4 $\mathcal{EMM}$	4 $\mathcal{EMM}$	10 $\mathcal{EMM}$
Proposed scheme	3 $\mathcal{HEMM}$	2 $\mathcal{HEMM}$	2 $\mathcal{HEMM}$	7 $\mathcal{HEMM}$

Table 3. Comparison of computational cost (in milliseconds).

Schemes	IoMT Devices	Edge Node	Cloud Server	Total
Cano et al. [21]	2(2.848) = 5.696	4(2.848) = 11.392	4(2.848) = 11.392	10(2.848) = 28.48
Proposed scheme	3(1.424) = 4.272	2(1.424) = 2.848	2(1.424) = 2.848	7(1.424) = 9.968
Reduction	$\left(\frac{28.48-9.968}{28.48}\right) * 100 = 65\%$			

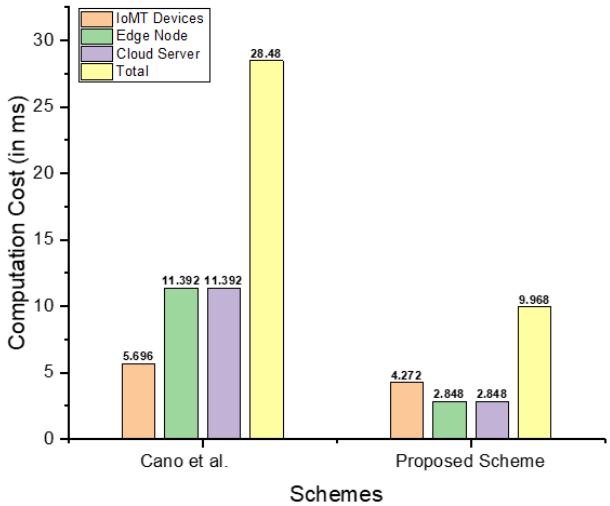

Figure 3. Comparison of the computation costs (in ms) of the proposed scheme to those of Cano et al. [21].

8. Communication Overhead

The size and number of extra bits exchanged during transmission between two entities is referred to as the communication overhead. In this section, we compare our scheme with Cano et al. [21] with respect to the communication overhead. To do this, we presume

the lengths of elliptic curve points $|q|$ are 160 bits and hyperelliptic curve points $|n|$ are 80 bits [29]. Our designed scheme only exchanges two messages between the IoMT device and the edge device and exchanges only two messages between the edge device and the cloud. Table 4 shows the communication overhead of the proposed scheme and Cano et al. [21] and also indicates the cost reduction of our scheme determined by the formula [28]. Figure 4 also shows a graphical illustration of this comparison.

Table 4. Comparison of communication overhead (in bits).

Scheme	Communication b/w IoMT and PDA	Communication b/w PDA and AP	Total
Cano et al. [21]	$2\|q\| = 2 * 160 = 320$	$2\|q\| = 2 * 160 = 320$	640
Proposed scheme	$1\|n\| = 80$	$1\|n\| = 80$	160
Reductions	$640 - 160/640 * 100 = 75\%$		

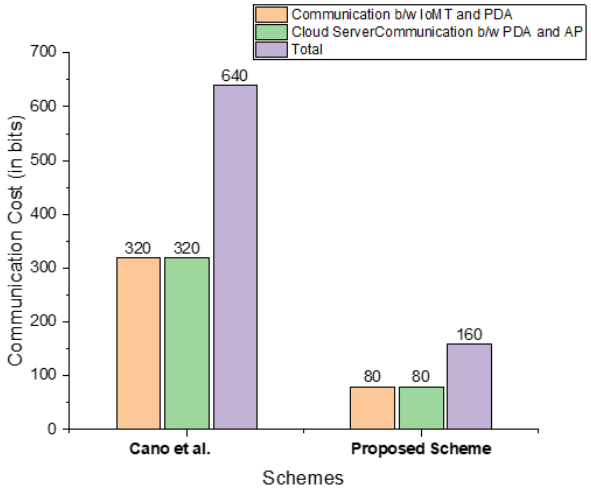

Figure 4. Comparison of the computation costs (in bits) of the proposed scheme to those of Cano et al. [21].

9. Conclusions

In this paper, we proposed an optimal authentication scheme a through dual signature for the Internet of Medical Things. The proposed schemes achieve authentication while simultaneously providing data privacy, integrity, and nonrepudiation. We carried out a thorough performance analysis in comparison with the existing scheme, and the study reveals that our scheme is more efficient in terms of computational cost and communication overhead compared to the existing scheme. We have used the Scyther tool for formal verification of the newly designed scheme and the results show our scheme is secure and authentic. The limitation of this paper is that it utilized the genus 2 hyperelliptic curve, which still needs more computational power and will not be suitable for resource-hungry IoMT devices. In the future, we will design a more lightweight dual-signature scheme using the genus 3 hyperelliptic curve cryptography.

Author Contributions: Conceptualization, Z.J., I.U., B.H., N.U.A. and M.A.K.; methodology, Z.J., I.U., M.A.K., P.L. and N.I.; software, I.U.; M.A.K. and P.L.; validation, Z.J., P.L. and I.U.; formal analysis, B.H., I.U. and M.A.K.; investigation, I.U., N.U.A., and M.A.K.; resources, P.L., N.U.A. and N.I.; data curation, M.A.K. and I.U.; writing—original draft preparation, B.H., I.U., M.A.K., P.L. and N.I.; writing—review and editing, M.A.K. and I.U.; visualization, P.L.; funds acquisitions, N.I.; supervision, I.U. and N.U.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that they have no conflict of interest.

Appendix A. Scyther Overview

To formally validate the security of our proposed protocol, Scyther is used, a tool designed for the verification of security protocols [28]. This validation tool works on the cryptographic assumption, according to which it is assumed that all of the cryptographic functions are perfect: The intruder cannot know anything from the encrypted text unless they know the decryption key. The Scyther has two main components (1) a command-line tool and (2) a graphical user interface. The command-line tool, as shown, takes the protocol description and some optimal parameters as its input and gives the output in the form of (1) a summary report and (2) a representation of trace patterns in XML (3) graph representations. The graphical user interface, as shown in Figure A1 provides the same feature as the command-line tool, but it offers the user ease of usability [30]. For the protocol verification, Scyther is used in three ways (1) for the confirmation of claims: in such cases, Scyther either verifies the security properties (likewise authentication, secrecy) or repudiates them. (2) Automatic claims: if the user does not mention which claims need to be verified, Scyther automatically generates claims and verifies the security properties. (3) Characterization: Scyther has this novel feature of characterization. Whenever a protocol is analysed in Scyther, Scyther provides all the possible trace representations of the roles being executed [30–33].

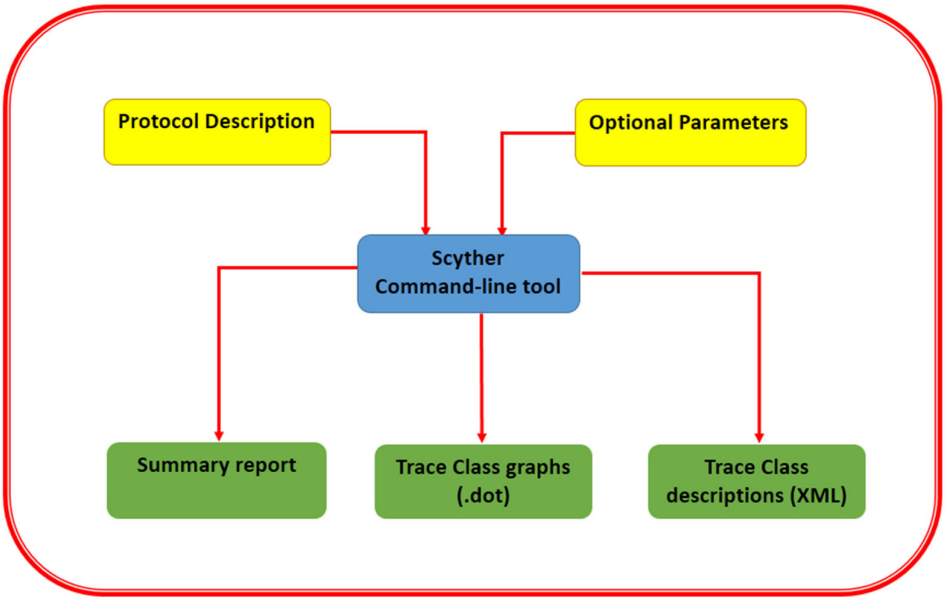

Figure A1. Scyther graphical user interface [28].

Appendix B. Formal Validation of Proposed Protocol Using Scyther

The input language used by Scyther, called the security protocol description language (SPDL), involves the definition of several security features called "claims" and further verifies them. These claims involve (1) message agreement, (2) secrecy, (3) alive, and (4) synchronization. Alive, secrecy, and synchronization form the base of strong authentication. If a claim of secrecy is accomplished, it means that certain information is kept secret from the intruder when data is transmitted over an insecure channel. The successful alive claim implies that when the sender is initiating the protocol run, the intended receiving party is alive or present. When a synchronization claim is successful, it shows that the communication partner sent the entire message that the receiving party received and the message is neither decrypted nor replayed during the communication. A successful message agreement claim assures that the information is safely transmitted and in the correct order [30–33]. To validate the security of our security protocol, we checked all of the claims

mentioned above and the result was labelled as "OK" by Scyther, which shows a successful outcome, as shown in Figure A2. For this experiment, the hardware resource we used is the Intel (R) Core (TM) i3-3110M CPU @ 2.40 GHz with a 64-bit supporting operating system and x64-based processor.

Figure A2. Formal validation result using Scyther.

In Table A1, we provide the acronyms with descriptions that are used in this paper.

Table A1. Acronyms used in this paper.

No	Acronym	Stands for
1	IoMT	Internet of medical things
2	IoT	Internet of things
3	ECG	electrocardiogram
4	SET	secure electronic transaction
5	RSA	Rivest-Shamir-Adleman
6	ECC	elliptic-curve cryptography
7	HECC	hyper-elliptic curve cryptography

Table A1. *Cont.*

No	Acronym	Stands for
8	HECDLP	hyper-elliptic curve discrete logarithm problem
9	IKE	Internet Key Exchange
10	ECDSA	elliptic curve digital signature
11	CA	central authority
12	AP	application providers
13	PDA	personal digital assistant
14	PHI	personal health information
15	EMM	elliptic curve modular multiplication
16	HEMM	hyper elliptic curve modular multiplication

References

1. Forestiero, A.; Papuzzo, G. Agents-Based Algorithm for a Distributed Information System in Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 16548–16558. [CrossRef]
2. Forestiero, A.; Papuzzo, G. Recommendation platform in Internet of Things leveraging on a self-organizing multiagent approach. *Neural Comput. Appl.* **2022**, *34*, 16049–16060. [CrossRef]
3. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain. *J. Commun.* **2017**, *12*, 240–247. [CrossRef]
4. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Tech. Rev.* **2021**, *39*, 775–788. [CrossRef]
5. Akhtar, M.; Shatat, R.S.A.; Shatat, A.S.A.; Alam Hameed, S.; Alnajdawi, S.I. IoMT-based smart healthcare monitoring system using adaptive wavelet entropy deep feature fusion and improved RNN. *Multimed. Tools Appl.* **2022**, *82*, 17353–17390. [CrossRef]
6. Ghorbel, A.; Bouguerra, S.; Ben Amor, N.; Jallouli, M. Cloud based mobile application for remote control of intelligent wheelchair. In Proceedings of the 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018; pp. 1249–1254. [CrossRef]
7. Udgata, S.K.; Suryadevara, N.K. COVID-19, Sensors, and Internet of Medical Things (IoMT). In *Internet of Things and Sensors Network for COVID-19*; Springer: Singapore, 2021; pp. 39–53. [CrossRef]
8. Ray, P.P.; Chowhan, B.; Kumar, N.; Almogren, A. BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. *IEEE Internet Things J.* **2021**, *8*, 10857–10872. [CrossRef]
9. Dilawar, N.; Rizwan, M.; Ahmad, F.; Akram, S. Blockchain: Securing Internet of Medical Things (IoMT). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [CrossRef]
10. Gatouillat, A.; Badr, Y.; Massot, B.; Sejdic, E. Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine. *IEEE Internet Things J.* **2018**, *5*, 3810–3822. [CrossRef]
11. Chen, C.-M.; Liu, S.; Chaudhry, S.A.; Chen, Y.-C.; Khan, M.A. A Lightweight and Robust User Authentication Protocol with User Anonymity for IoT-Based Healthcare. *Comput. Model. Eng. Sci.* **2022**, *131*, 307–329. [CrossRef]
12. Sarkar, A.; Tripathi, S. Design of a Dual Signature Scheme using ECDSA in Set Protocol. *Int. J. Comput. Appl.* **2014**, *88*, 1–5. [CrossRef]
13. Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Bin Zikria, Y. A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2401–2410. [CrossRef]
14. Ullah, I.; Amin, N.U.; Almogren, A.; Khan, M.A.; Uddin, M.I.; Hua, Q. A Lightweight and Secured Certificate-Based Proxy Signcryption (CB-PS) Scheme for E-Prescription Systems. *IEEE Access* **2020**, *8*, 199197–199212. [CrossRef]
15. Ullah, I.; Amin, N.U.; Khan, J.; Rehan, M.; Naeem, M.; Khattak, H.; Khattak, S.J.; Ali, H. A Novel Provable Secured Signcryption Scheme $\mathcal{PSSS}$: A Hyper-Elliptic Curve-Based Approach. *Mathematics* **2019**, *7*, 686. [CrossRef]
16. Ullah, Z.; Zeb, A.; Ullah, I.; Awan, K.M.; Saeed, Y.; Uddin, M.I.; Al-Khasawneh, M.A.; Mahmoud, M.; Zareei, M. Certificateless Proxy Reencryption Scheme (CPRES) Based on Hyperelliptic Curve for Access Control in Content-Centric Network (CCN). *Mob. Inf. Syst.* **2020**, *2020*, 4138516. [CrossRef]
17. Wuu, L.C.; Chen, K.Y.; Lin, C.M. Off-Line Micro Payment Scheme with Dual Signature. *J. Comput.* **2008**, *19*.
18. Yalamanchili, S.; Rao, K. Two-Stage Authentication for Wireless Networks Using Dual Signature and Symmetric Key Protocol. *Int. J. Comput. Sci. Commun.* **2011**, *2*, 419–422.
19. Cai, Z.; Zhang, Q.; Li, M.; Gan, Y.; Zhang, J. Multi-Domain Authentication Protocol Based on Dual-Signature. *TELKOMNIKA Telecommun. Comput. Electron. Control* **2014**, *13*, 290–298. [CrossRef]
20. Saqib, M.N.; Kiani, J.; Shahzad, B.; Anjum, A.; Malik, S.U.R.; Ahmad, N.; Khan, A.U.R. Anonymous and formally verified dual signature based online e-voting protocol. *Clust. Comput.* **2018**, *22*, 1703–1716. [CrossRef]

21. Cano, M.-D.; Cañavate-Sanchez, A. Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA. *Secur. Commun. Networks* **2020**, *2020*, 4960964. [CrossRef]
22. Zhang, M.-H.; Xie, J.-H. High fidelity quantum blind dual-signature protocols. *Mod. Phys. Lett. B* **2022**, *36*, 2250064. [CrossRef]
23. Zhang, K.; Zhao, X.; Zhang, L.; Tian, G.; Song, T. A Quantum Dual-Signature Protocol Based on SNOP States without Trusted Participant. *Entropy* **2021**, *23*, 1294. [CrossRef] [PubMed]
24. Shi, J.; Chen, S.; Liu, J.; Li, F.; Feng, Y.; Shi, R. Quantum Dual Signature with Coherent States Based on Chained Phase-Controlled Operations. *Appl. Sci.* **2020**, *10*, 1353. [CrossRef]
25. Sun, Y.; Lo, F.P.-W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
26. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
27. Yu, S.; Das, A.K.; Park, Y.; Lorenz, P. SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10374–10388. [CrossRef]
28. Ullah, I.; Amin, N.U.; Khan, M.A.; Khattak, H.; Kumari, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. *J. Med. Syst.* **2020**, *45*, 4. [CrossRef]
29. Ullah, I.; Khan, M.A.; Khan, F.; Jan, M.A.; Srinivasan, R.; Mastorakis, S.; Hussain, S.; Khattak, H. An Efficient and Secure Multi-message and Multi-receiver Signcryption Scheme for Edge Enabled Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 2688–2697. [CrossRef]
30. Cremers, C.J.F. *Scyther: Semantics and Verification of Security Protocols*; Technische Universiteit Eindhoven: Eindhoven, The Netherlands, 2006. [CrossRef]
31. Cremers, C.J.F. *Scyther: Unbounded Verification of Security Protocols*; Technical Report 572; ETH Zurich, Department of Computer Science: Zurich, Switzerland, 2011. [CrossRef]
32. Alharbi, E.; Alsulami, N.; Batarfi, O. An Enhanced Dragonfly Key Exchange Protocol against Offline Dictionary Attack. *J. Inf. Secur.* **2015**, *06*, 69–81. [CrossRef]
33. Kang, N.; Kim, J. Entity Authentication and Secure Registration for Lightweight Devices in Internet of Things. *Int. J. Control Autom.* **2018**, *11*, 37–48. [CrossRef]