A Secured and Optimized Broadcast Authentication Scheme for the Internet of Medical Things

Syed Waleed Riaz
Computer Science Department, Abdul Wali Khan University Mardan,
KPK, Pakistan
waleedriaz@awkum.edu.pk

Fazlullah Khan
School of Computer Science, Faculty of Science and Engineering, University of Nottingham Ningbo China, Ningbo
315104, Zhejiang, China
fazl.ullah@nottingham.edu.cn

Insaf Ullah
Institute for Analytics and Data Science, University of Essex,
CO4 3SQ Colchester, UK
insaf.ullah@essex.ac.uk

Bandar Alshawi
Department of Computer and Network Engineering, College of Computing, Umm Al-Qura University,
Makkah, Saudi Arabia
bmhshawi@uqu.edu.sa

Ryan Alturki
Department of Software Engineering, College of Computing, Umm Al-Qura University,
Makkah, Saudi Arabia
rmturki@uqu.edu.sa

Mohammad Wedyan
Department of Computer Sciences, Faculty of Information Technology and Computer Sciences, Yarmouk University (YU),
Irbid 21163, Jordan
mwedyan@yu.edu.jo

***Abstract*—This Internet of Medical Things (IoMT), facilitates the medical stop regarding real-time monitoring of patients, medical emergency management, remote surgery, patient information management, medical equipment, drug monitoring, etc. However, IoMT devices communicate with each other in an open environment that makes them vulnerable to a wide range of malicious threats from malicious entities. To protect the devices and their associated data, we designed a broadcast authentication scheme for IoMT devices using identity-based public key cryptography that exploits the lightweight features of the Hyper-Elliptic Curve (HEC). We then performed the security analysis based on the Random Oracle Model (ROM), in which we have proved that the proposed scheme is unforgeable under the hardiness of the hyperelliptic curve discrete logarithm problem. The proposed scheme is analyzed in terms of computational and communication overhead and the experimental results justify the superiority of the proposed work in comparison to the existing schemes.**

Keywords*—*Internet of Medical Things, Authentications, Identity Based Broadcast Signature, Random Oracle Model, Hyper Elliptic Curve.

I. INTRODUCTION

The Internet of Things (IoT) is made up of smart devices with computing, storage, and communication capabilities. These devices can be used for a variety of purposes, including smart agriculture, smart home technologies, and healthcare systems [1]. Combining the Internet of Things with smart healthcare devices, tools, and software makes it easier for users to access patient records from medical servers and other connected devices; we call this combination the Internet of Medical Things (IoMT). IoMT facilitates the medical stop regarding real-time monitoring of patients, medical emergency management, remote surgery, patient information management, and medical equipment and drug monitoring, etc [2, 3]. Fig. 1 [3], illustrates the basic communication structure of IoMT, which include a patient with injected medical devices (IMDs) that are neurostimulator, cardiac pacemaker, gastric stimulator, etc., there is a personal embedded device (PED) that could be responsible to collect data from injected medical devices through wireless technology with its protocols such as Z-Wave and Near Field Communication (NFC), Internet Protocol Version 6 (IPv6) over 6LoWPAN, ZigBee, and Bluetooth Low Energy (BLE). NFC is used to transfer data in a short range between IoT devices and the working capability of a 6LoWPAN is that the devices do not need any gateway and proxies to connect with other IP network devices because it is based on IP-based standard internetworking protocol. ZigBee supports several topologies such as tree, star, and mesh, further, it is based on the networking standard called low-power wireless IEEE802.15.4. BLE could be used for low latency, low bandwidth, and short-range IoMT applications. The data collected from injected medical devices, and personal embedded devices can be sent to the medical cloud server, which can further process, analyze, and store the received data. The users which may be Doctors, Nurses, and a person from emergency services can access the data from the medical cloud server.

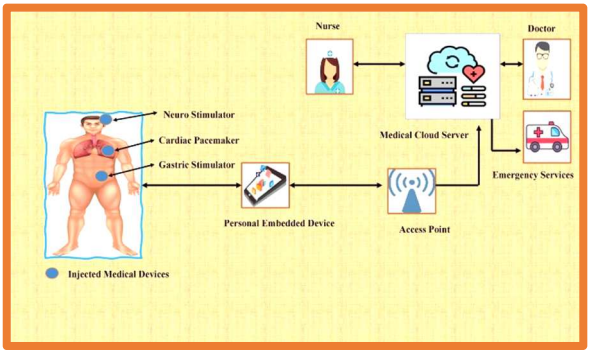

Fig. 1. General Architecture of an IoMT system

However, one of the most critical things is that if a harmful device joins the IoMT network, then it will destroy the whole system [4]. This process will be more difficult if the environment wants broadcast communication. So, authentication is the main pillar to avoid these types of situations [5], and for this purpose, the most attractive authentication process is broadcast digital signature [6], which can enable the sender to generate a digital signature on medical data utilizing his private key for multi-receiver. Later, each receiver can verify this signature by using the sender's public key. For the broadcast signature, several approaches based on old public key infrastructure (PKI) are designed [7],

however, due to certificate management and revocation problems they are not a suitable solution [8]. To replace PKI-based approaches, an identity-based broadcast signature is designed [9], in which the sender and receiver group first send their identities to a private key generation center (PKGC), then by using the identity (for sender or receiver) PKGC generate private and public key and send it to that user. Mathematical methods such as Bilinear Pairing (BLPNG), Elliptic Curve (ELCV), RSA, and Hyper Elliptic Curve (HEC) are the main pillars for broadcast identity-based signature schemes that are used to enhance the security hardiness for attackers [10]. The problem with BLPNG is that it requires heavy computational time during map to map-to-point hash function and performing a pairing operation. Besides BLPNG, RSA will be a good choice, but due to utilizing 1024-bit key sizes, the limited resource-oriented IoMT devices cannot afford it in a real-time communication environment. The second main thing that can avoid the usage of RSA for resource-hungry IoMT devices is that during the construction of the algorithm, it is required to use exponentiations which need heavy machine cycles which lead to the requirement of more time-consuming. The ELCV is known for fewer parameters and key sizes (160 bits) in public key cryptosystems, however, 160 bits are still not affordable for IoMT devices. So, HEC is the sub-type of ELCV that provides the same level of security hardiness as provided by RSA and ELCV by only utilizing an 80-bit key [11]. Inspired by the above discussion, we have made the following contribution to this paper.

- *We* have *designed an identity-based broadcast signature that generates a single signature for the broadcast set based on HEC*
- *We have performed the security analysis under the random oracle model to prove that the proposed scheme is unforgeable due hyperelliptic curve discrete logarithm problem.*
- *We have performed the computational and communication cost analysis in which we have compared the proposed scheme with existing relevant approaches and the results show that the proposed scheme is more efficient.*

II. Literature Review

Ren et al [12], contributed a broadcast authentication scheme with the help of bilinear pairing and identity-based signature. However, bilinear pairing is not a suitable choice when we consider this scheme for resource-constrained wireless sensor network devices. To avoid such type of disadvantages, Cao et al [13], consider elliptic curve cryptography for their newly proposed identity-based multi-user broadcast authentication scheme. However, the scheme is not safe from the attack of possible user compromise [14]. Benzaid et al [15] and Benzaid et al [16], designed a new broadcast authentication scheme with the help of elliptic curve cryptography and identity-based signature. However, these two schemes will not be a good selection for resource constraint low powered devices, because they need 160 bits key. Shim et al [17], proposed an efficient broadcast authentication scheme with the help of bilinear pairing and identity-based cryptography. However, when we consider resource constraints low powered devices, the bilinear pairing expensive operations will not be a good selection. Cheng et al [18], coined an efficient broadcast authentication scheme with the help of RSA and identity-based cryptography. However, RSA utilizes a 1024-bit key size, so it will need more time for resource-hungry low-powered devices. Siri and Karthik [19], claimed to propose a new scheme that incorporates identity-based cryptography and an elliptic curve for broadcast authentication. However, they failed to provide a proper algorithm. Also, elliptic curves utilize a 160-bit key size, so it will need more time for resource-hungry low-powered devices. A novel identity-based signature utilizing bilinear pairing is designed by Feng et al [20], for broadcast authentication in wireless sensor networks. However, bilinear pairing is not a good selection when we consider this scheme for resource-constrained low-powered devices. Recently, Kasyoka et al [21], designed a new broadcast authentication scheme with the help of elliptic curve cryptography and identity-based signature. However, the elliptic curve will not be a good selection for resource constraint low powered devices, because it needs 160 bits key, which is still more.

III. Preliminaries

This section discuses the preliminaries about the Syntax of Identity Based Broadcast Signature (IBBS), the Threat Model for our IBBS, and the Proposed Network Model using IBBS. The following are sub-phases that give brief explanations about the above topics.

A. Syntax of Identity-Based Broadcast Signature (IBBS)

The following are the steps that can complete the execution process of Identity-Based Broadcast Signature.

- *Setup: In the setup phase, the private key generation center (PKGC) sets its master key as $\hbar$ and the master public key as χ. Then PKGC made the public parameter set* Ö *and published* $(Ö, \chi)$ *to the IoMT network.*
- *Key Generations: Given* ID_u, *PKGC compute* (Ω_u, A_u), *and send* (A_u, Ω_u) *to identity* ID_u *through a secure network.*
- *Identity-Based Broadcast Signature: Given* $(ID_S, \Omega_S, ID_i, \Omega_i, m, A_S)$, *a Broadcaster can produce and send the broadcast signature* (S_i, m, φ_i) *to the set of receivers (*$i = 1,2,3, \dots, n$)
- *Identity-Based Broadcast Signature Verifications: Given* $(S_i, m, \varphi_i, \Omega_S, d_S, \chi)$, *the broadcast set (*$i = 1,2,3, \dots, n$) *can verify the broadcast signature.*

B. Threat Model of our IBBS

This section explains the security threats that can occur during the execution of the proposed IBBS scheme, in which with the help of challenger (C_{IBBS}) the adversary (A_{IBBS}) can generate a forged broadcast signature. For this purpose, $C_{IBBS}$and A_{IBBS} can perform the following game.

1. *Setup: Given 80 bits security parameter of the hyperelliptic curve (*H_{ypr}*), *C_{IBBS} *made the public parameter set* Ö *and sent* $(Ö, \chi)$ *to* A_{IBBS} *and keep private* $\hbar$.
2. *Hash Queries:* A_{IBBS} *can send the request for hash value,* C_{IBBS} *will respond with the particular value if it exists in the initialized list, otherwise* C_{IBBS} *will randomly choose the requested value and deliver it to* A_{IBBS}.

3. *Private Key Generation Query:* A_{IBBS} *can send the request for private key values,* C_{IBBS} *will execute the Key Generations algorithm to generate* A_j *and delivers it to* A_{IBBS}.
4. *Public Key Generation Query:* A_{IBBS} *can send the request for public key values,* C_{IBBS} *will execute the Key Generations algorithm to generate* Ω_j*and delivers it to* A_{IBBS}.
5. *IBBS Query:* A_{IBBS} *can send the request for IBBS with* m *and* ID_S, C_{IBBS} *returns IBBS tuple* (S_i, m, φ_i)*and delivers it to* A_{IBBS}.
6. *Forgery:* A_{IBBS} *can process a tuple* (S_i, m, φ_i) *if the following conditions hold.*
   - (S_i, m, φ_i) *is Identity-Based Broadcast Signature*
   - *The query for the private key of the broadcaster* (ID_S) *is not asked*
   - (S_i, m, φ_i) *is not produced through Identity Based Broadcast Signature*

The benefits of A_{IBBS} is $BFT_{A_{IBBS}}^{IBBS} = Prob(BFT_{A_{IBBS}} wins)$.

C. Proposed Network Model

The communication between devices in our proposed broadcast signature scheme is explained in Fig. 2, which includes the entity that are Smart Medical Devices, Private Key Generation (PKGC) Centre, Receiver Group, and Controller. The process begins when Smart Medical Devices collect medical-related data and handover it to the controller through Bluetooth Low Energy (BLE). Then Controller upon reception of medical-related data from Smart Medical Devices can send a request for private with his identity to the Private Key Generation Centre and as a response, PKGC sends the private and public keys to the controller through a secure network. Then by using his private key, the controller executes the computational steps for the broadcast signature and sends the broadcast signature tuple to the receiver group in the open network. The Receiver Group upon reception of the broadcast signature tuple can send a request for private with their identity to the Private Key Generation Centre and as a response, PKGC sends the private and public keys to the Receiver Group through a secure network. The receiver group executes the computational steps for broadcast signature verifications.

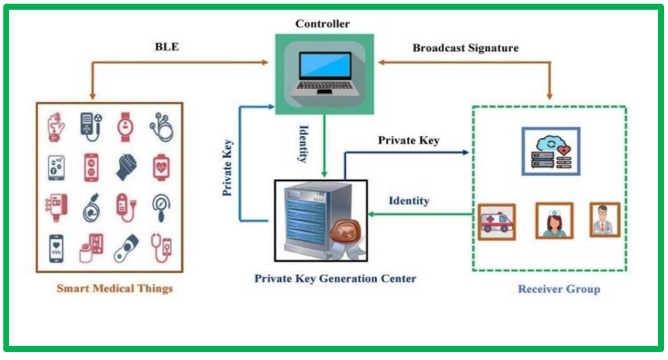

Fig. 2. Proposed Network Model of Identity-Based Signature

IV. The Proposed Scheme Constructions

The following are the steps that make our proposed scheme execution process and Table 1 explains the symbols.

Setup: In this phase, when the private key generation center (PKGC) receives the 80 bits security parameter of the hyperelliptic curve (H_{ypr}), then it picks two one-way and collision-resistant hash functions (H_0, H_1) from the SHA family, compute his master public key $\chi = \hbar.\mathcal{D}$ and make $\hbar$ as a master secret key which is selected randomly from (F_{hyprq}), where F_{hyprq} is the finite field belonging to H_{ypr} with order $q = 80$ bits. PKGC published $\ddot{O} = (H_0, H_1, \chi, \mathcal{D}, q = 80, H_{ypr}, F_{hyprq})$ to the IoMT network, where $\mathcal{D}$ is the devisor which belongs to H_{ypr}.

TABLE I. SYMBOLS USED IN PROPOSED IBBS

No	Symbol	Descriptions
1	H_{ypr}	Indicates hyperelliptic curve
2	H_0, H_1	Indicates two collisions resistant and one-way hash functions that belong to the SHA family
3	$\chi = \hbar.\mathcal{D}$	Master public key of private key generation center (PKGC)
4	$\hbar$	Master private key of private key generation center (PKGC)
5	F_{hyprq}	indicates is the finite field belonging to H_{ypr} with order $q = 80$ bits
6	$\mathcal{D}$	indicates if the devisor belongs to H_{ypr} with an 80 −bit size
7	ID_u	Indicates the identity of the authorized user
8	A_u, Ω_u	The public and private keys for authorized users with identity ID_u
9	A_S	The private key of the sender
10	m	Represents a plain text to be sent
11	Ω_S	The public key of the sender
12	$\ddot{O} = (H_0, H_1, \chi, \mathcal{D}, q = 80, H_{ypr}, F_{hyprq})$	The public parameter param which is available in the network

Key Generations: In this phase, when the private key generation center (PKGC) receives an identity ID_u from any authorized use, then it selects σ_u from the finite set of hyperelliptic curves randomly, compute $\Omega_u = \sigma_u.\mathcal{D}$, $d_u = H_0(ID_u, \Omega_u)$, $A_u = \sigma_u + d_u\hbar$, and send (A_u, Ω_u) to identity ID_u through a secure network. Upon reception of (A_u, Ω_u), the user with identity ID_u set A_u is his private key and $\Omega_u$is his public key.

Identity-Based Broadcast Signature: Our identity-based broadcast signature can be executed through the following sub-steps.

- It selects λ_i from the finite set of hyperelliptic curves randomly, compute $\varphi_i = \lambda_i.\mathcal{D}$
- Compute $B = H_1(ID_S, \Omega_S, ID_i, \Omega_i, m, \varphi_i)$ and $S_i = \lambda_i + BA_S$, where A_S is the sender's private key
- Broadcast (S_i, m, φ_i) to the set of receivers $(i = 1,2,3, \dots, n)$

Identity-Based Broadcast Signature Verifications: Upon receiving(S_i, m, φ_i), the broadcast set $(i = 1,2,3, \dots, n)$ can verify the broadcast signature as $S_i\mathcal{D} = \varphi_i + B(\Omega_S + d_S\chi)$, where Ω_S is the sender's public key, if it is satisfied then the broadcast user accepts the signature otherwise not.

Correctness

Upon receiving(S_i, m, φ_i), the broadcast set $(i = 1,2,3, \dots, n)$ can verify the broadcast signature as $S_i\mathcal{D} = \varphi_i + B(\Omega_S + d_S\chi) = S_i\mathcal{D} = (\lambda_i + BA_S).\mathcal{D} = (\lambda_i.\mathcal{D} + BA_S.\mathcal{D}) = (\lambda_i.\mathcal{D} + B(\sigma_S + d_S\hbar).\mathcal{D}) = (\lambda_i.\mathcal{D} + B(\sigma_S.\mathcal{D} + d_S\hbar.\mathcal{D})) = (\varphi_i + B(\sigma_S.\mathcal{D} + d_S\hbar.\mathcal{D})) = (\varphi_i + B(\Omega_S + d_S\hbar.\mathcal{D})) = (\varphi_i + B(\Omega_S + d_S\chi))$ hence proved.

V. Provable Security Analysis for Our IBBS

Using the provable security model called Random Oracle (RO), we have proved our proposed IBBS scheme is secure from the forge ability attack, with the help of challenger (C_{IBBS}) the adversary (A_{IBBS}) can generate a forged broadcast signature. For this purpose, $C_{IBBS}$and A_{IBBS} can perform the following game. The following is the A_{IBBS} winning benefits.

$$Prob\left(BFT_{A_{IBBS}} wins\right) = \left(1 - \frac{PRKG_{QIBBS}}{PBKG_{QIBBS}}\right)\left(1 - \frac{1}{2^k}\right)\left(\frac{1}{PBKG_{QIBBS} - PRKG_{QIBBS}}\right),$$

where $PRKG_{QIBBS}$, $PBKG_{QIBBS}$, and k denotes the Private Key Generation Query, Public Key Generation Query, and 80-bit security parameter.

Proofs: Given a hyperelliptic curve problem i.e., $\xi_{IBBS} = \zeta_{IBBS}.\mathcal{D}$, the ambition of C_{IBBS} is find ζ_{IBBS} by using the following steps.

Setup: Given 80 bits security parameter of the hyperelliptic curve (H_{ypr}), C_{IBBS} made the public parameter set $\ddot{O} = (H_0, H_1, \chi, \mathcal{D}, q = 80, H_{ypr}, F_{hyprq})$ and send $(\ddot{O}, \chi)$ to A_{IBBS} and keep private $\hbar.\, d_u$

H_0 Queries: C_{IBBS} initialized a list l_{H_0} with (ID_j, Ω_j), if A_{IBBS} ask for the $H_0(ID_j, \Omega_j)$, C_{IBBS} check d_j in l_{H_0}, if it exists, C_{IBBS} return to A_{IBBS} with value d_j. Otherwise, C_{IBBS} select d_j randomly and return to A_{IBBS} with value d_j. In the end, the value d_j is added to l_{H_0}.

H_1 Queries: C_{IBBS} initialized a list l_{H_1} with $(ID_j, \Omega_j, m, \varphi_j)$ if A_{IBBS} ask for the $H_1(ID_j, \Omega_j, m, \varphi_j)$ C_{IBBS} check B_j in l_{H_1}, if it exists, C_{IBBS} return to A_{IBBS} with value B_j. Otherwise, C_{IBBS} select B_j randomly and return to A_{IBBS} with value B_j. In the end, the value B_j is added to l_{H_1}.

Public Key Generation Query: C_{IBBS} initialized a list l_{PBKG} with (ID_j, Ω_j), if A_{IBBS} ask for Ω_j, C_{IBBS} check if $ID_j = ID_i$, then it computes $\Omega_j = \zeta_{IBBS}.\mathcal{D}$ and C_{IBBS} return to A_{IBBS} with value Ω_j. Otherwise, C_{IBBS} will select σ_j randomly, compute $\Omega_j = \sigma_j.\mathcal{D}$, and return to A_{IBBS} with value Ω_j. In the end, the value $\Omega_j$is added to l_{PBKG}.

Private Key Generation Query: C_{IBBS} initialized a list $l_{\text{PRKG}}$with (ID_j, Ω_j, A_j), if A_{IBBS} ask for A_j, C_{IBBS} check if $ID_j = ID$, then it aborts the process, otherwise, it can find (ID_j, Ω_j, A_j) in l_{PRKG} and return to A_{IBBS} with value $A_j = \sigma_j + d_j\hbar$. In the end, the value $A_j$is added to l_{PRKG}.

IBBS Query: A_{IBBS} can send the request for IBBS with m and ID_S, C_{IBBS} returns IBBS tuple $(S_j, m, \varphi_j)$and delivers it to A_{IBBS}. C_{IBBS} can perform the following steps.

- It selects λ_j from the finite set of hyperelliptic curves randomly, compute $\varphi_j = \lambda_j.\mathcal{D}$
- Pick B_j from l_{H_1} and A_j from l_{PRKG}
- Compute $S_j = \lambda_j + B_jA_j$ and send (S_j, m, φ_j) to A_{IBBS}

Forgery: A_{IBBS} can processed with a forge tuple(S_j, m, φ_j) by using the following steps.

- It can need the value for the private number (λ_j) from the finite set of hyperelliptic curves in a random way, he/she can compute $\varphi_j = \lambda_j.\mathcal{D}$, which will be equal to HECDLP.
- It must pick the original value for B_j from l_{H_1}, in which he/she needs λ_j from the finite set of hyperelliptic curves in a random way or also extract it from $\varphi_j = \lambda_j.\mathcal{D}$ which will be equal to HECDLP.
- It must pick the original value for A_j from l_{PRKG}, as we know from the Private Key Generation Query $A_j = \sigma_j + d_j\hbar$, in which he/she needs σ_j and $\hbar$ from $\Omega_j = \sigma_j.\mathcal{D}$ and $\chi = \hbar.\mathcal{D}$ that enable the process to compute two-time HECDLP.

Though, A_{IBBS} can process a forge tuple (S_j, m, φ_j) if the following conditions hold.

- $Cond_{IBBS1}$: (S_j, m, φ_j) is an Identity-Based Broadcast Signature
- $Cond_{IBBS2}$: The query for the private key of the broadcaster (ID_S) is not asked
- $Cond_{IBBS3}$: (S_j, m, φ_j) is not produced through Identity Based Broadcast Signature

The probability for each defined condition is followed.

$$Prob(Cond_{IBBS1}) = \left(1 - \frac{PRKG_{QIBBS}}{PBKG_{QIBBS}}\right),$$

$$Prob(Cond_{IBBS2}) = \left(1 - \frac{1}{2^k}\right), \text{ and } Prob(Cond_{IBBS3}) = \left(\frac{1}{PBKG_{QIBBS} - PRKG_{QIBBS}}\right)$$

$$Prob(Cond_{IBBS1}.Cond_{IBBS2}.Cond_{IBBS3}) = Prob(Cond_{IBBS1}) \wedge Prob(Cond_{IBBS2}) \wedge Prob(Cond_{IBBS3}) = \left(1 - \frac{PRKG_{QIBBS}}{PBKG_{QIBBS}}\right)\left(1 - \frac{1}{2^k}\right)\left(\frac{1}{PBKG_{QIBBS} - PRKG_{QIBBS}}\right)$$

From the above computation, we can conclude the following winning probability of A_{IBBS}.

$$Prob\left(BFT_{A_{IBBS}} wins\right) = \left(1 - \frac{PRKG_{QIBBS}}{PBKG_{QIBBS}}\right)\left(1 - \frac{1}{2^k}\right)\left(\frac{1}{PBKG_{QIBBS} - PRKG_{QIBBS}}\right)$$

A. Computational Cost Analysis

We have taken the most relevant two identity-based broadcast signature schemes that are Feng et al [20] and Kasyoka et al [21] for the computational cost analysis. Then, we made Table 2, which includes the major operations like bilinear pairing multiplications (BPM), pairing operations (PRNG), elliptic curve point multiplication (ECPMN), and hyperelliptic curve devisor multiplication (HECDMN), in the

proposed, Feng et al [20] and Kasyoka et al [21] scheme. The time in milliseconds for BPM, PRNG, ECPMN, and HECDMN, is given in Table 2 [3,11]. Then, we utilized the running time which is given in Table 3 for making Table 4, which includes the computational cost analysis in milliseconds, and the outcomes show that our scheme needs a lesser amount of computational capabilities in comparison to Feng et al [20] and Kasyoka et al [21]. Also, in Fig. 3 the computational cost comparisons between the proposed scheme, Feng et al [20], and Kasyoka et al [21] based on *ms* are shown.

TABLE II. COMPUTATIONAL COST ANALYSIS BASED ON MAJOR OPERATIONS

Schemes	Signature	Verifications	Total
Feng et al [20]	3 BPM	4 BPM + 2 PRNG	7 BPM + 2 PRNG
Kasyoka et al [21]	3 ECPMN	2 ECPMN	5 ECPMN
Proposed Scheme	2 HECDMN	3 HECDMN	5 HECDMN

TABLE III. TIME REQUIRED FOR EACH MAJOR OPERATION

No	Symbol	Used for and Time needed in Milli Seconds [ms]
1	BPM	Bilinear Pairing multiplications and time needed 4.31 ms
2	PRNG	Bilinear Pairing Operations and time needed 14.90 ms
3	ECPMN	Elliptic Curve Point Multiplication and time needed 0.97 ms
4	HECDMN	Hyper Elliptic Curve Devisor Multiplication and time needed 0.48 ms

TABLE IV. COMPUTATIONAL COST ANALYSIS BASED ON MS

Schemes	Signature	Verifications	Total
Feng et al [20]	3* 4.31=12.93	4*4.31 + 2 *14.90=67.04	7 *4.31+ 2 *14.90=29.80
Kasyoka et al [21]	3*0.97=2.91	2*0.97=1.94	5*0.97=4.85
Proposed Scheme	2* 0.48=0.96	3*0.48=1.44	5 *0.48=2.40

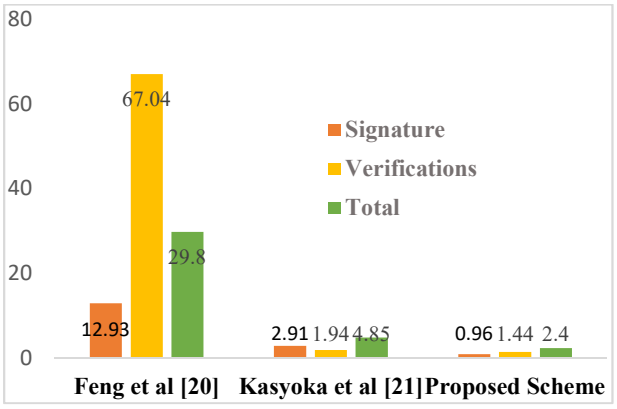

Fig. 3. Computational Cost [ms] Comparisons between Proposed Scheme, Feng [20], and Kasyoka [21]

B. Communication Cost Analysis

We have taken the most relevant two identity-based broadcast signature schemes that are Feng et al [20] and Kasyoka et al [21] for the communication cost analysis. Then, we made Table 5, which includes the consuming bits like bilinear pairing, elliptic curve, and hyperelliptic curve, in the proposed scheme, Feng et al [20] and Kasyoka et al [21] scheme. Fig. 4, illustrates the communication cost analysis in bits, and the outcomes show that our scheme needs a lesser amount of communication overhead in comparison to Feng et al [20] and Kasyoka et al [21].

TABLE V. COMMUNICATION COST ANALYSIS BASED ON MAJOR OPERATIONS.

Schemes	Communication Cost	Communication Cost in bits
Feng et al [20]	1|H|+2|q|+|m|	1*256+2*160+1024=1600
Kasyoka et al [21]	3|G|+|m|	3*1024+1024=4096
Proposed Scheme	2|n|+|m|	2*80+1024=1184

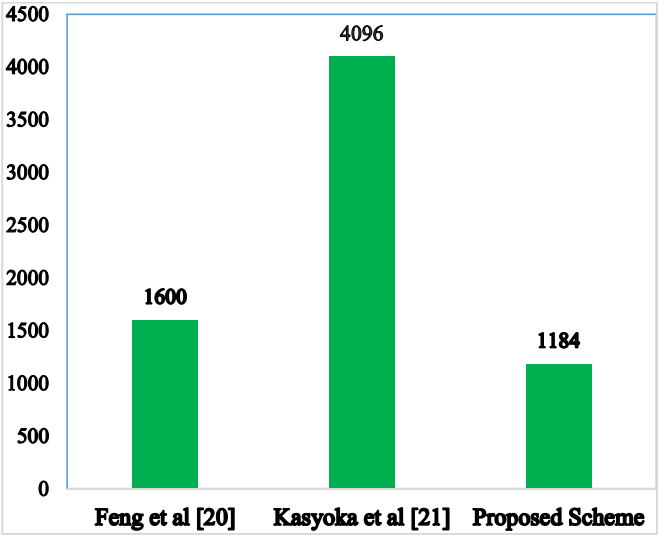

Fig. 4. Communication Cost Comparisons between Proposed Scheme, [20] and [21] based on bits

VI. CONCLUSION

In this paper, we proposed an efficient Broadcast Authentication scheme in which the Internet of Things (IoT) acts as a hotspot, which is merged with health monitoring devices to provide better services. Authentication is the main concern, because doing communicating in an open network, any malicious user can join the communication process and can cause danger. So, we have designed a broadcast authentication scheme for IoMT devices based on identity-based public key cryptography with the help of the lighter nature of the Hyper-Elliptic Curve (HEC). The designed scheme is analyzed in terms of computational and communication cost, and we believe that this scheme is superior to existing schemes due to HEC. We also performed the security validation RO Model and Proved that it is unforgeable under the hyperelliptic curve discrete logarithm problem.

REFERENCES

[1]. A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for internet of things," *Arabian Journal for Science and Engineering,* pp. 1-15, 2022.

[2]. S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols," in *2017 8th International conference on information technology (ICIT)*, 2017: IEEE, pp. 685-690.

[3]. M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar, and N. Stergiou, "LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics," *IEEE transactions on green communications and networking,* vol. 5, no. 3, pp. 1202-1211, 2021.

[4]. X. Jia, M. Luo, H. Wang, J. Shen, and D. He, "A Blockchain-Assisted Privacy-Aware Authentication scheme for internet of medical things," *IEEE Internet of Things Journal,* vol. 9, no. 21, pp. 21838-21850, 2022.
[5]. M. Kumar, S. Verma, A. Kumar, M. F. Ijaz, and D. B. Rawat, "ANAF-IoMT: a novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 12, pp. 8936-8943, 2022.
[6]. V. Kumar and S. Ray, "Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm," *Wireless Personal Communications,* vol. 123, no. 3, pp. 2341-2365, 2022.
[7]. Q. Xie, P. Zheng, Z. Ding, X. Tan, and B. Hu, "Provable Secure and Lightweight Vehicle Message Broadcasting Authentication Protocol with Privacy Protection for VANETs," *Security and Communication Networks,* vol. 2022, no. 1, p. 3372489, 2022.
[8]. I. Ullah *et al.*, "An efficient and secure multimessage and multireceiver signcryption scheme for edge-enabled internet of vehicles," *IEEE Internet of Things Journal,* vol. 9, no. 4, pp. 2688-2697, 2021.
[9]. Y. Zhao, Y. Wang, Y. Liang, H. Yu, and Y. Ren, "Identity-based broadcast signcryption scheme for vehicular platoon communication," *IEEE Transactions on Industrial Informatics,* 2022.
[10]. R. Aissaoui, J.-C. Deneuville, C. Guerber, and A. Pirovano, "A survey on cryptographic methods to secure communications for UAV traffic management," *Vehicular Communications,* p. 100661, 2023.
[11]. I. Ullah, A. Alkhalifah, S. U. Rehman, N. Kumar, and M. A. Khan, "An anonymous certificateless signcryption scheme for internet of health things," *IEEE Access,* vol. 9, pp. 101207-101216, 2021.
[12]. K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," *IEEE Transactions on Vehicular Technology,* vol. 58, no. 8, pp. 4554-4564, 2009.
[13]. X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Computer communications,* vol. 31, no. 4, pp. 659-667, 2008.
[14]. H. Y. Chien, C. I. Lee, and T. C. Wu, "Comments on IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks," *Security and Communication Networks,* vol. 6, no. 8, pp. 993-998, 2013.
[15]. C. Benzaid, S. Medjadba, and N. Badache, "Fast verification of an ID-based signature scheme for broadcast authentication in wireless sensor networks," in *2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, 2012: IEEE, pp. 1-6.
[16]. C. Benzaid, S. Medjadba, A. Al-Nemrat, and N. Badache, "Accelerated verification of an ID-based signature scheme for broadcast authentication in wireless sensor networks," in *2012 IEEE 15th International Conference on Computational Science and Engineering*, 2012: IEEE, pp. 633-639.
[17]. K.-A. Shim, Y.-R. Lee, and C.-M. Park, "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks," *Ad Hoc Networks,* vol. 11, no. 1, pp. 182-189, 2013.
[18]. C.-Y. Cheng, I.-C. Lin, and S.-Y. Huang, "An RSA-like scheme for multiuser broadcast authentication in wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 11, no. 9, p. 743623, 2015.
[19]. R. Maidhili and G. Karthik, "Energy efficient and secure multi-user broadcast authentication scheme in wireless sensor networks," in *2018 International Conference on Computer Communication and Informatics (ICCCI)*, 2018: IEEE, pp. 1-6
[20]. M. Feng, C.-F. Lai, H. Liu, R. Qi, and J. Shen, "A novel identity-based broadcast authentication scheme with batch verification for wireless sensor networks," *Journal of Internet Technology,* vol. 21, no. 5, pp. 1303-1311, 2020
[21]. P. Kasyoka, M. Kimwele, and S. M. Angolo, "Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography," *Engineering Reports,* vol. 2, no. 7, p. e12176, 2020.