Received: 11 April 2024 | Revised: 22 July 2024 | Accepted: 16 August 2024 | Published online: 23 August 2024

RESEARCH ARTICLE

Medinformatics
yyyy, Vol. XX(XX) 1–5
DOI: 10.47852/bonviewMEDIN42023088

Practical Heterogeneous Pairing-Free Signcryption Scheme for Internet of Medical Things Communications with Edge Computing

Kasyoka Philemon Nthenge[1,*], Anyembe Andrew Omala[1]

1 Department of Computer Science and Technology, South Eastern Kenya University, Kenya.

***Corresponding author:** Kasyoka Philemon Nthenge, Department of Computer Science and Technology, South Eastern Kenya University, Kenya. Email: pkasyoka@seku.ac.ke

Abstract: Internet of Medical Things technology is becoming popular because of recent advancements in sensor node technology. A sensor node is characterized as a resource limited device. This characteristic has led to several security challenges that underpin the necessity for cryptosystems that are both more effective and robust in protecting vital data. We propose an efficient and secure access control scheme where the transmitting node and receiving node are in certificateless cryptography and identity-based cryptographic environment respectively. The design of the access control protocol for use in Internet of Medical Things with mobile edge computing is based on a heterogeneous signcryption scheme and it is supported by 5G network. Random oracle model was used to provide the security proof of the proposed scheme. The proposed heterogeneous access control scheme provides public verifiability and ciphertext authentication properties. In addition, we have compared the efficiency of our access control scheme with other related existing schemes, our scheme has low energy consumption and computation cost.

Keywords: Internet of Medical Things, certificateless cryptography, 5G network, wireless body area network, signcryption

1. Introduction

The Internet of Medical Things (IoMT) entails the interconnection of hardware and software infrastructure and medical devices that enables healthcare systems to communication with each other over the internet [1]. IoMT has the capacity to play a vital role in implementing a secure ubiquitous medical system that can provide healthcare services anytime and from anywhere enabling real-time monitoring of patients [2]. To ensure real-time uninterrupted and reliable low latency communication (URLLC), ubiquitous healthcare systems should utilize both 5G and MEC technologies [3]. The IoMT sensors perform the task of sensing, processing and communicating physiological data to a sink in its communication network [4].

In healthcare ubiquitous system, the potential utilization of sensor nodes was shown in the study by Vanteru et al. in 2023[5]. A similar approach was demonstrated in the study by Nawaz et al. in 2024 [6] where continuous patient monitoring improved life quality of the patients. Sensors by their very nature are limited in terms of power required for computing, data storage and source of power hence, developing and implementing a more secure IoMT has been a difficult undertaking. It is crucial to ensure physiological data generated in IoMT is kept confidential as access of medical data by unauthorized persons can cause harm to patients.

Traditional cryptographic primitives require considerable computation energy rendering them unsuitable for use on sensor nodes. Elliptic Curve Cryptosystems (ECC) as proposed by both Koblitz in 1987 [7] and Miller in 1985 [8] has gained considerable recognition owing to its ability to produce small size keys. Through ECC it has become possible to develop efficient security protocol for use on devices that utilize less power and use less memory for functionality.

Communication in sensor networks should be able to achieve important properties such as anonymity, integrity, confidentiality, authenticity and non-repudiation [9-11]. Signing then encrypting has been proofed not to be an efficient concept [12], hence the use of signcryption [13] is more preferred. Signcryption is better suited for use on resource-limited devices since it can simultaneously achieve message authenticity, confidentiality, repudiation and integrity more efficiently than the process of encrypting then signing or vice versa [14].

Cryptosystems come in different forms such as public key infrastructure (PKI) based cryptosystems, identity-based cryptography (IBC) and certificateless cryptography (CLC) [15]. In IBC schemes, certificate management is not necessary as is

with PKI since such schemes make use of a key escrow mechanism [16]. Several IBC schemes have been proposed and developed in recent studies. In the study by Patil and Patil in 2022 [17], they proposed a secure signcryption to help share electronic health records. A study by Ramadan and Raza in 2023 [18] gave a secure IBC signcryption protocol for use in telemedicine systems to limit spread of contagious diseases. The concept of key escrow makes homogenous security schemes based on IBC not suitable for use in an IoMT environment [19].

To overcome the key escrow problem in IBC, a study by Al-Riyami and Paterson in 2003 [15] presented a certificateless scheme. A certificateless cryptosystem utilizes the services of a third party known as Key Generation Center (KGC) who does not know the full secret keys of the parties involved in a communication. The KGC generates and supplies a user with part of the final full private key. The user will then compute his/her final and full private key by combining the partial private key with some additional secret information. Since CLC was proposed in 2003 by Al-Riyami and Paterson [15], a number of access control protocols for WBANs have been proposed [20]. In the study by Jahan et al. in 2023 [21], they presented an end-to-end user authentication scheme for a medical system in a smart enabled environment. The medical system was constructed from inexpensive sensors, a personal device such as a medical server, mobile phone and a wireless body area network to prevent unauthorized behavior. In the study by Arfaoui et al. in 2020 [22], they presented a context-aware certificateless access control protocol that was able to achieve user anonymity for use on WBANs. An access control protocol capable of achieving authenticity, confidentiality, non-repudiation, user anonymity and integrity was proposed by Li and Hong [20]. The scheme was based on a certificateless signcryption with ciphertext authenticity, their scheme was a variant of the signcryption scheme proposed by Barreto et al. in 2005 [23]. The cost of running a pairing operation is an enormous burden to resource constrained sensor nodes [24]. Numerous studies have proposed different ways of accelerating the computation of pairing operation [25, 26]. To this end, the computation cost of pairing based operations remain complex and time-consuming. This has made pairing operations not a suitable choice designing security protocol for resource constrained network environments. In 2019, Gao et al. [24] went on to design a signcryption based access control schemes without the use of bilinear pairing for use on WBANs, their scheme did not provide ciphertext authenticity. In study by Kasyoka et al. in 2021 [27], a pairing-free access control protocol for WBANs based on CLC was designed. In the study by Ullah et al. in 2021 [28], they gave a signcryption protocol based on CLC for use on Internet of Health Things (IoHT).

Most of the security schemes discussed so far are homogeneous implying that the sender and the receiver operate in a similar environment and cannot support heterogeneous communications. In a study by Hou et al. in 2023 [29], an efficient heterogeneous scheme was proposed, where signcrypted communication was delivered from CLC to PKI system. A similar concept was used by Yang et al. in 2023 [30] where they proposed a heterogenous signcryption scheme where sending node in an IBC network environment can communicate data to a receiving node in a PKI network environment with multi-ciphertext equality test. However, PKI comes with an extra cost of certificate management. A heterogeneous access control protocol was put forward by Omala et al. in 2018 [31] for a WBANs based on a signcryption scheme (hereafter called OMMJL) where sender operates in CLC network environment and the receiver operates in IBC network environment. However, the scheme did not provide ciphertext authenticity.

Most cryptographic systems cannot achieve ciphertext authenticity. A protocol that lacks ciphertext authenticity can over burden a sensor node with unnecessary process of validating the communicated ciphertext through decryption. This can lead to unnecessary computations especially when the ciphertext is found to be invalid. We are encouraged to propose a new alternative solution with the following perspectives:

First, we proposed a pairing-free heterogeneous signcryption protocol that is able support public verifiability and ciphertext authentication. Second, we design an efficient and secure heterogeneous access control protocol using the signcryption protocol where the sending device is in CLC network environment and receiving device is in IBC network environment. Third, we propose a 5G communication architecture for use in IoMT with edge computing model. Fourth, we provide a formal security proof of the protocol where our protocol is secure in IND-CCA2 and EUF-CMA under GDH problem and DL problem in ROM. Lastly, we compared our proposed scheme with related access control schemes by OMMJL [31], LHJ [32] and LLWW [33] and our heterogenous scheme was found efficient in energy consumption, communication cost and overall computational time.

This paper is organized as follows: Section 2 presents materials and methods used in our study while in section 3 we give the results obtained during our study. An application scenario of the proposed scheme is given in section 4. Finally, section 5 concludes our paper.

2. Materials and Methods

2.1. Computational assumption

Definition 1: $ECDLP$: Let G be an elliptic curve group, P denote a generator of an order q. Given values $(P, aP) \in G$ for unidentified $a \in Z_q$. Given a probabilistic polynomial time (PPT) attacker denoted as A, we state its advantage or opportunity in solving the $ECDLP$ as $Adv^{ECDLP}(A) = Pr[A(P, aP) = a | a \in Z_p$. The $ECDL$ assumption is that for any PPT adversary A, the stated advantage must be is negligible.

Definition 2: $Decisional\ Diffie\ Hellman (DDH)$: G is cyclic group where P is given as its generator of order q. Given $(aP, bP, cP) \in G$ the task will be to decide if $c \equiv ab \bmod q$.

Definition 3: $Gap\ Diffie\ Hellman\ Problem\ (GDHP)$: Given G is a cyclic group, P is the generator of G and is of order q. Given $(aP, bP, cP) \in G$ for unknown $a, b \in Z_q$. The Decisional Diffie Hellman oracle on input (aP, bP, cP) will output value 1 if $c \equiv ab \bmod q$, else it will give the output of value 0.

2.2. Network model

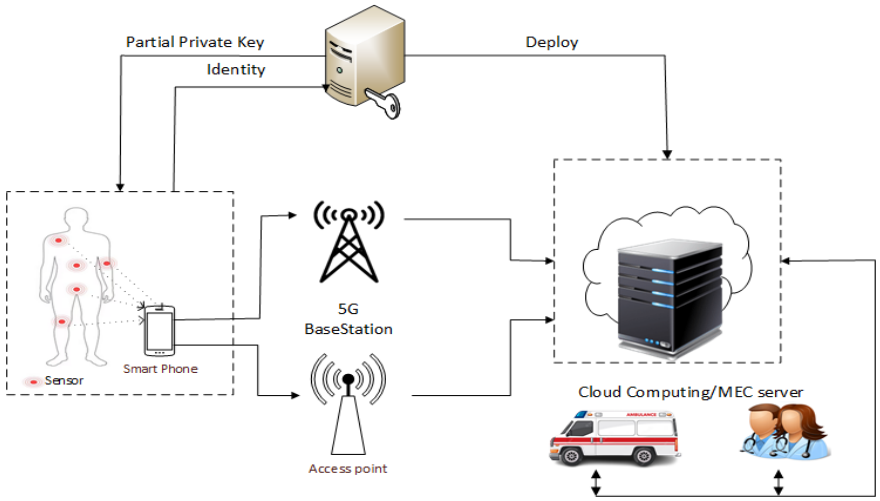

Figure 1. Network model

Figure 1. Illustrates the proposed protocol's network model. It comprises of wireless technology such as (Wi-Fi and 5G), WBAN, medical staff, Network Manager and ambulance. The WBAN is made up of biomedical sensor nodes and an access point (gateway) that plays the role of a network manager. The nodes can be connected to the access point using a short-range radio transceiver such as Zigbee [28] and Bluetooth Low Energy (BLE). The nodes may be surgically implanted in the body or placed on skin of a patient for the purpose of collecting required patient's physiological data periodically and transferring the collected data to a network controller. Through WiFi or 5G network the controller can be connected to a cloud computing/Multiaccess Edge Computing (MEC) server. MEC is vital for mobile healthcare devices as it redistributes computing resources from large-scale data centers to the edge nodes in a network allowing instantaneous processing of data at the source level [3]. In response to an authorized user request, the gateway will communicate physiological data to an authenticated request. Acting as a Public Key Generator (PKG), the Network Manager (NM) will manage the medical cloud server and it will manage the WBAN as a KGC. A KGC will play the role of processing the partial secret or private key of users in a CLC environment while the PKG will generate the private key and the public key of sensors in an IBC network environment through a registration process. All users that want to gain access to PGHD from the cloud server must first register on the NM and be validated by a gateway before gaining access to the WBAN data. The key notations used on the proposed protocol are shown in Table 1.

2.3. Formal model

CLC-IBC heterogeneous signcryption scheme will enable any user to communicate from a CLC environment to a receiver node in an IBC environment. Our KGC will be used to generate a private key that is partial for the sender and a private key for the receiving node.

The security component based on two different categories of adversaries: Type-I adversary: The attacker or adversary depicts an outsider attacker without knowledge of the master key of KGC and is denoted as A_I and Type II adversary: The adversary represents an insider attacker. The attacker or adversary has knowledge of the master key of KGC which is kept as a secret and it is denoted as A_{II} [15].

2.3.1. Confidentiality model

Definition 4: IND-CCA-Indistinguishability against and adaptive Chosen Ciphertext Attacks. A CLC-IBC scheme will be secure against IND-CCA2 if no adversary A can win with a non-negligible advantage.

Game 1: When simulating confidentiality of our proposed scheme we will follow the approach applied in the study by Omala et al. [31].

Initial: We assume that the challenger is an algorithm C. The challenger C will run Setup algorithm utilizing a secure parameter k to generate system parameters $params$ and master secret key s . C keeps s as a secret and forwards the $params$ to adversary A.

Phase 1: When adversary A submit queries as shown below:

Partial Private Key query: Using identity ID_i, adversary A can issue a partial private key query, C will run *CLC-PPrK* and return partial private key d_i to A.

Public Key query: When A submits the query on identity D_i , C respond with public key P_i if it exists. Otherwise, it will call the algorithm responsible for generating the public key generating to create it.

Key extraction query: When the adversary makes a query on D_i . C will call algorithm *IBC-KE* and returns *private key* d_i.

***Replace Public Key query*:** If A wants to replace public key the adversary will do so by submitting (ID_i, P_i') of its choice. C replaces corresponding P_i of the identity ID_i.

Private Key query: When A makes request using identity ID_i. If the public key had been replaced adversary will be expected to provide it. However, if it had not been replaced, the challenger C calls algorithm *CLC- PrK* to return full private key SK_A. Otherwise, algorithms *CLC- PrK* and *CLC-PPrK* will be run to obtain SK_A.

Signcrypt Query(Q_s): When adversary A makes this query on the tuple (ID_A, ID_B, m), C makes a request for public key oracle on ID_A to obtain public keys (P_A, R_A, Q_A) and the sender's private key SK_A. C will execute the signcryption algorithm to get σ and transmit the ciphertext to the adversary to A .

Unsigncrypt Query (Q_u): Attacker A will issue a query for ciphertext σ with identity ID_A and the identity ID_B. C who is the challenger will run Unsigncryption algorithm to generate an original m or the symbol $\perp$ and return it to the attacker.

Challenge: An Adversary A will select two messages (m_1, m_2) that are of equal length, the sender's ID_A^* and the receiver's ID_B^* on which the adversary will wish to be challenged. The ID_B^* must not run on key extraction query. Challenger C selects a bit $b \in_R \{0,1\}$ and compute ciphertext σ^* and returns it to adversary A.

Guess stage: Adversary A returns its guess b^* and will win in this game if $b^* = b$ with the advantage denoted as $Adv_A^{IND-CCA2} = |2\Pr[b^* - b] - 1|$ where $\Pr[b^* - b]$ implies the probability that $b^* = b$ exists.

2.3.2 Unforgeability model

Definition 5: The Existential Unforgeability against the Adaptive Chosen Message Attacks (EUF-CMA). A CLC-IBC scheme will be secure in EUF-CMA if there is no polynomially bound adversary A_I(including A_{II}) that wins the game with a non-negligible advantage.

Game 2 In this game a challenger C will interact with adversary A_I.

Initialize. Challenger C will run $Setup(1^k)$ to generate the system $params$ and its master secret key s. Finally, it will forward the system $params$ to adversary A_I.

Training Phase. The hash queries in this phase are generated using the approach in Game 1.

Forgery At the end of this training phase, the *adversary* A_I will output a ciphertext denoted as σ^* that will not have been generated by signcryption query on message m^* with ID_A^* and ID_B^* as sender and receiver respectively and wins the game if $m^* = USC(\sigma^*, ID_A^*, ID_B^*, d_B^*)$.

Game 3 In game 3 challenger C will interact with adversary A_{II}.

Initial challenger C will execute $Setup(1^k)$ to generate system $params$ and its own master secret key s. Finally, it will forward the master secret key s and $params$ to adversary A_{II}.

Training Phase. The hash queries generated are more like those in Game 2. Adversary A_{II} will not be allowed to make a replacement query for the public key. At this phase no key extraction query is permitted or query of the partial private key since A_{II} can perform them by itself.

Forgery At the conclusion of this phase, *adversary* A_{II} will output a ciphertext σ^* not generated by signcryption query for m^* with ID_A^* and ID_B^* belonging to the sender and the receiver respectively and wins the game if $m^* = USC(\sigma^*, ID_A^*, ID_B^*, d_B^*)$.

Table 1. List of notations

Symbol	Description
G	Cyclic additive group
P	Generator of group G
$E(F_q)$	An elliptic curve defined over a prime field
H_i	Secure cryptographic hash function where $i = 1,2,3$
ID_A	Sender's Identity
ID_B	Receiver's Identity
P_A, R_A, Q_A	Sender's public key
P_B, R_B, Q_B	Public key of receiver
$SK_A = (x_A, d_A)$	Full private key of sender, i.e partial private key and secret keys respectfully
d_B	Receiver's private key
s, P_{pub}	Master secret key and public key of KGC respectfully
m	Plaintext message
σ	Ciphertext

2.4. Proposed heterogenous signcryption scheme

In the proposed scheme, the sending party and the receiving party are in CLC environment and IBC environment respectively. The proposed protocol is constructed from the following algorithms:

KGC Set-Up: The KGC is expected to choose elliptic curve $E(F_q)$ of finite field F_q where $E(F_q)$ can be defined using system parameters. KGC will be responsible for defining the secure cryptographic hash functions $H_0: \{0,1\}^* \times G \times G \rightarrow Z_q^*$, $H_1: \{0,1\}^* \rightarrow G$, $H_2: G^2 \times \{0,1\}^* \times G^2 \rightarrow \{0,1\}^n$ and $H_3: \{0,1\}^n \times G^2 \times \{0,1\}^* \times G^2 \rightarrow Z_q^*$ where n will represent the bits of the message to transmit. The KGC will randomly select a secret master key $s \in_R Z_q^*$ and compute $P_{pub} = sP$ as a public key. P denotes the generator of an elliptic curve elliptic curve $E(F_q)$. KGC will keep s hidden and avails all system params to the public as $params = \{G, P, q, P_{pub}, H_0, H_1, H_2, H_3\}$.

CLC- SVS: This algorithm will be executed by the user. The user will randomly select a secret $x_A \in_R Z_q^*$.

***CLC-PuK*:** This algorithm will allow a user to enter secret key x_i and produce a public key as $P_A \leftarrow x_A \cdot P$.

CLC-PPrK: This algorithm will require a secret key denoted as s, public key $R_A = r_A P$ (where $r_A \in_R Z_q^*$ is a random value selected by KGC) and $params$ to produce the partial private key d_A for any system user. The *CLC-PPrK* algorithm is executed by a KGC, where the partial private key will be derived as $d_A = r_A + s.H_0(ID_A, R_A, P_A) mod\ q$, then computes $Q_A = (R_A + H_0(ID_A, R_A, P_A) \cdot P_{pub})$ and sends d_A to $user_i$ over a secure channel making Q_A and R_A public. A user can verify the authenticity of a partial private key d_i by simply checking if $d_A \cdot P = R_A + H_0(ID_A, R_A, P_A) P_{pub}$ holds.

IBC-PrK: Given the identity $ID_B \in \{0,1\}$ from a user in an IBC environment. The KGC proceeds to set user public key are $P_B = H_1(ID_B) \in G$ randomly select $r_B \in_R Z_q^*$, then computes $R_B = r_B P$ and private key as $d_B = r_B + s.H_0(ID_B, R_B, P_{pub}) mod\ q$, then computes $Q_B = (R_B + H_0(ID_B, R_B, P_{pub}) \cdot P_{pub})$and sends d_B to $user_i$ in IBC environment over a secure channel and makes Q_B and R_B public. The partial private key d_B of the user will be verified by confirming if $d_B \cdot P = R_B + H_0(ID_B, R_B, P_{pub}) P_{pub}$ holds.

CLC- PrK: The algorithm is run by $user_i$ in a CLC domain, who will set the full private key as $SK_s = (d_A, x_A)$.

SC: CLC network environment: With receiver's public key Q_B, system $params$ and identity ID_B. The signcrypting process is as follows:

i. Select random parameter $r \in_R Z_q^*$; $v = (x_A \cdot r) mod\ q$
ii. $U \leftarrow vP$;
iii. Compute $T = rQ_B$;
iv. Compute $h_2 = H_2(U, T, ID_B, R_B, Q_B)$;
v. Compute $c = h_2 \oplus m$;
vi. Compute $h_3 = H_3(c, U, P_A, ID_A, R_A, Q_A)$;
vii. Compute $w = (x_A \cdot d_A^{-1} \cdot h_3 \cdot r)\ mod\ q$

The sender will output ciphertext $\sigma = (w, c, h_3)$

USC: IBC network environment: After receiving ciphertext $\sigma = (w, c, h_3)$. The unsigncrypt process will proceed as follows:

i. Compute $U' = w \cdot h_3^{-1} \cdot Q_A$;
ii. $h_3' = H_3(c, U', P_A, ID_A, R_A, Q_A)$;
iii. Check If $h_3 = h_3'$ holds, if equal run the following steps else output symbol $\perp$.
iv. $T = d_B U$
v. $h_2 = H_2(U, T, ID_B, R_B, Q_B)$;
vi. Compute $m' = h_2 \oplus c$.

Our scheme has the property of ciphertext authenticity and public verifiability. A third party can confirm validity of the ciphertext $\sigma = (w, c, h_3)$ from our signcryption scheme without using the private key of the receiver and the message m by running the first three steps of the heterogeneous signcryption scheme.

The Proposed Scheme Correctness

The following is the correctness of the proposed scheme:

$$\begin{aligned} T &= rQ_B \\ &= r(R_B + h_B \cdot P_{pub}) \\ &= rR_B + r \cdot h_B \cdot P_{pub} \\ &= rR_B + r.H_0(ID_B, R_B, P_B) \cdot P_{pub} \\ &= d_B U \end{aligned}$$

$$\begin{aligned} U &= w \cdot h_3^{-1} \cdot Q_A \\ &= x_A \cdot d_A^{-1} \cdot h_3 \cdot r \cdot h_3^{-1} \cdot Q_A \\ &= x_A \cdot d_A^{-1} \cdot r \cdot d_A \cdot P \\ &= x_A rP \\ &= vP \end{aligned}$$

2.5 Security analysis of the scheme

The proposed heterogeneous scheme is both UF-CMA and IND-CCA2 secure against the Type-I attacker and Type-II attacker under ROM in the DLP assumption. Where Type-I attacker is an outsider who does not have access to the secret master key and is denoted as A_I. The Type-II attacker represents an insider adversary possessing the knowledge of the master secret key, denoted as A_{II}. The ROM is a formalized model used in security analyzing of cryptographic protocols, where a cryptographic hashing function is viewed as a black box containing a randomized function.

2.5.1. Proof of confidentiality

Theorem 1: *Our protocol is IND-CCA2 secure in ROM under GDH assumption.*

The proof for the theorem is provided in Lemma 1 as follows.

Lemma 1 *If there is an existence of an attacker A who can possess a non-negligible advantage ε in compromising our scheme, there will be a C algorithm defined as a challenger who can solve the GDH problem with the advantage:*

$$Pr[C] \geq \frac{\varepsilon}{q_{H_0}^2}\left(1-\frac{q_s(qH_2+qH_3)}{2^k}\right)\left(1-\frac{q_u}{2^k}\right)$$

Here, q_{H_0} represents the highest number of queries to H_0,while q_s and q_u represents both the signcryption queries and unsigncrypt queries respectively. Word limitation prevents the presentation of the remaining proof within this paper.

2.5.2. Proof of the unforgeability

Theorem 2: *Our proposed heterogenous protocol is EUF-CMA secure in the ROM under the Discrete Logarithm Problem assumption.*

Proof: Proof for the theorem is in Lemma 2.

Lemma 2 *The proposed protocol is secure in EUF-CMA under the Discrete Logarithm Problem assumption.*

in ROM. Given an attacker or adversary A_1 posing a non-negligible advantage ε who is capable of break the authenticity of our proposed protocol, then there will be a challenger C capable of solving the DLP problem with the advantage.

$$\Pr[C] \geq \varepsilon \frac{1}{qH_0}\left(1-\frac{q_s(qH_2+qH_3)}{2^k}\right).$$

Word limitation prevents the presentation of the remaining proof within this paper.

Table 2. The Performance comparison

	Computation Cost			Cost of Communication	
Scheme	User	Sensor	Gateway	Receive	Communication Direction
OMMJL	3PM	3PM	–	$\|G_1\|+\|ID\|+\|m\|+2\|Z_q^*\|$	CLC → IBC
LHJ	P+3PM+E	1P	3P	$\|G_1\|+\|m\|$	CLC → IBC
LLWW	3PM+E	1P	4P	$\|G_1\|+\|m\|$	CLC → IBC
Ours	2PM	1PM	1PM	$\|G_1\|+\|m\|$	CLC → IBC

3. Results

The proposed scheme was evaluated in terms of performance in comparison with the related schemes by OMMJL [31], LHJ [32] and LLWW [33]. Table 2 shows analysis of the proposed schemes in terms of communication and computation cost. As in the study by Shim et al. in 2013 [34], we use the energy consumption and the running time on a MICA2 mote that is implemented using ATmega128 4KB RAM and 128KB ROM and 8-bit processor that clocks at 7.3728 MHz. In our analysis, we only considered high computational cost operations such as pairing operation in G_2, point multiplication in G_1 and the exponentiation operations denoted as P, PM and E respectively. From the studies by Gura et al. in 2004 and Ma et al. in 2014 [35, 36], given that a PM operation will take 0.81s on an EC curve set on 160 bits p, an operation E in G_2 that is exponential will take 0.9s, the pairing operation denoted by P will take 1.9 s where η_T pairing is based on a subgroup with a prime 254-bit order on a super singular curve $y^2 + y = x^3 + x$ over a $\mathbb{F}_{2^{271}}$ with degree of 4. Therefore, the time it takes to perform computation using our proposed access control protocol is compared to access control schemes by OMMJL [31], LHJ [32], LLWW [33] is as follows:

Table 3. Ciphertext generation computation cost

Scheme	User	Sensor	Gateway
OMMJL	$3 * 0.81 = 2.43s$	$3 * 0.81 = 2.43s$	
LHJ	$1.9 + 3 * 0.81 + 0.9 = 5.23s$	$1 * 1.9 = 1.9s$	$3 * 1.9 = 5.7s$
LLWW	$3 * 0.81 + 0.9 = 3.33s$	$1 * 1.9 = 1.9s$	$4 * 1.9 = 7.6s$
Ours	$2 * 0.81 = 1.62s$	$1 * 0.81 = 0.81s$	$1 * 0.81 = 0.81s$

Figure 2 summarizes the computation time of our proposed protocol in comparison to related protocols by OMMJL, LHJ and LLWW. When developing or designing an access control scheme for WSNs, it is important to consider reducing the cost of computation of a given sensor node as they are resource constrained. Our scheme has reduced computation time at the sensor as follows: In OMMJL [31] $(2.43 - 0.81)/2.43 = 67\%$, in LHJ [32] and LLWW [33] $(1.9 - 0.81)/1.9 = 57\%$.

We have adopted the approach used in the studies by Shim in 2014 [37] and Cao et al. in 2008 [38] to calculate the energy consumption. A 3.0V is set as the power level of MICA2 and a data rate of 12.4kbps. The value set for active mode current draw 8.0mA, while the mode of transmitting and receiving are set as 27mA and 10mA respectively [37]. An operation in point multiplication will consume 19.44 mJ [36] while an operation in bilinear pairing will consume 45.6 mJ. The exponentiation operation in G_2 consumes 21.6 mJ. The energy computation cost at the sensor in the schemes by OMMJL [31] , LHJ [32], LLWW [33] and our scheme is shown in Table:

Table 4. Energy Computation and communication cost

	Energy Computation cost	Communication cost on Receiver
Scheme	Sensor	
OMMJL	$3 * 19.44 = 58.3$ mJ	$\|G_1\| + \|ID\| + \|m\| + 2\|Z_q^*\| = 520 + 80 + 160 + 2 * 160 = 1080$ bits.
LHJ	$45.6 + 3 \times 19.44 + 21.6 =$ 125.5 mJ	$\|G_1\| + \|m\| = 520 + 160 = 680$ bits
LLWW	$3\times 19.44 + 21.6 = 79.9$ mJ	$\|G_1\| + \|m\| = 520 + 160 = 680$ bits
Ours	$2\times 19.44 = 38.9$ Mj	$\|G_1\| + \|m\| = 520 + 160 = 680$ bits

Our proposed scheme has managed to reduce the energy computation cost at the sensor as follows: In OMMJL [31] $(58.3 - 38.9)/58.3 = 33\%$, in LHJ [32] $(125.5 - 38.9)/125.5 = 69\%$ and in LLWW [33] $(79.9 - 38.9)/79.9 = 51\%$. The energy computation cost is shown on table 4 and summarized in Figure.3. The computation of the cost of communication makes an assumption that $|m| = 160$ bits and $|ID| = 80$ bits as in Li et al. [32].The length of an element in $|G_1| = 1024$ bits is 1024 bits using an elliptic curve with $|p| = 160$ bits. From Shim et al. [34], the size of an element in G_1 can be reduced to 520 bits by standard compression technique. Therefore, the communication cost on receiving side of the controller in OMMJL [31], LHJ [32], LLWW [33] and our scheme is shown in Table 4. Therefore, the cost of communication of the proposed protocol is similar to that of LHJ [32] and LLWW [33], which is 37% more efficient than the communication cost in OMMJL [31] scheme.

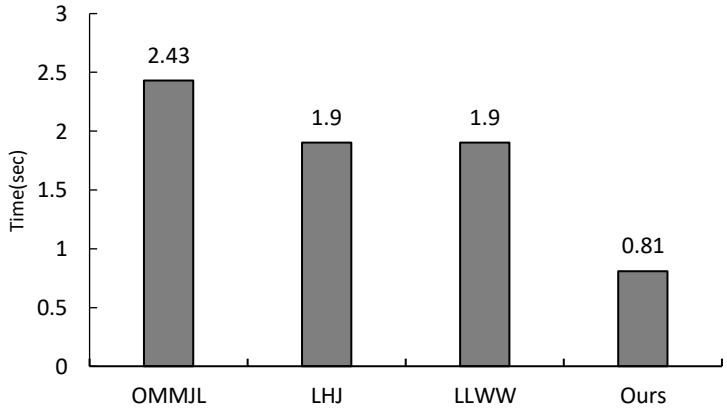

Figure 2. Computational time of sensor

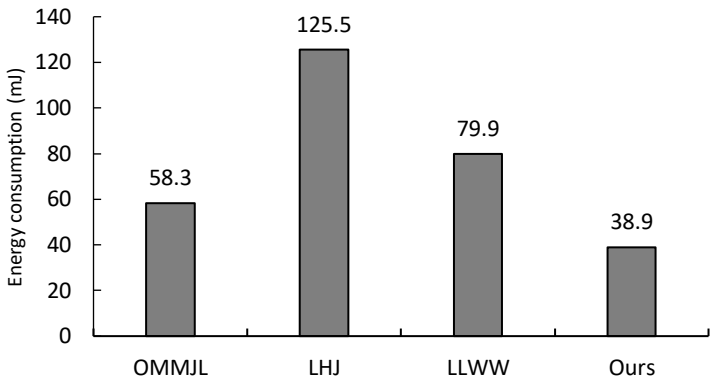

Figure 3. Energy consumption cost of the sensor

4. Application Scenario

This model is made up of five entities: KGC/PKG, WBANs, local servers/controller, MEC server and medical server. KGC/PKG will compute system parameters by running Set-up algorithm and circulate them to both CLC and IBC environment. Using both CLC-Puk and CLC-PPrk algorithms, KGC computes public and partial private keys and avails them to the WBAN. Algorithm IBC-Prk is used by PKG to compute the private key and public keys for the MEC server and medical server. All keys are availed to WBAN, MEC server and medical server through a secure channel. The WBAN will collect the patient's data and sends it signcrypted to MEC server and the MEC server forward it to the medical server. To send plaintext M from WBAN to the medical server, the sensor node runs signcryption algorithm SC to get ciphertext $\sigma = (w, c, h_3)$ and sends σ to a MEC server and the server forwards ciphertext σ to medical server. Both the MEC server and medical server can perform ciphertext authentication and recover plaintext M by executing algorithm USC. Authorized doctors can access PGHD from the MEC server that is closer to the patient, or the main medical server as shown in Figure 4.

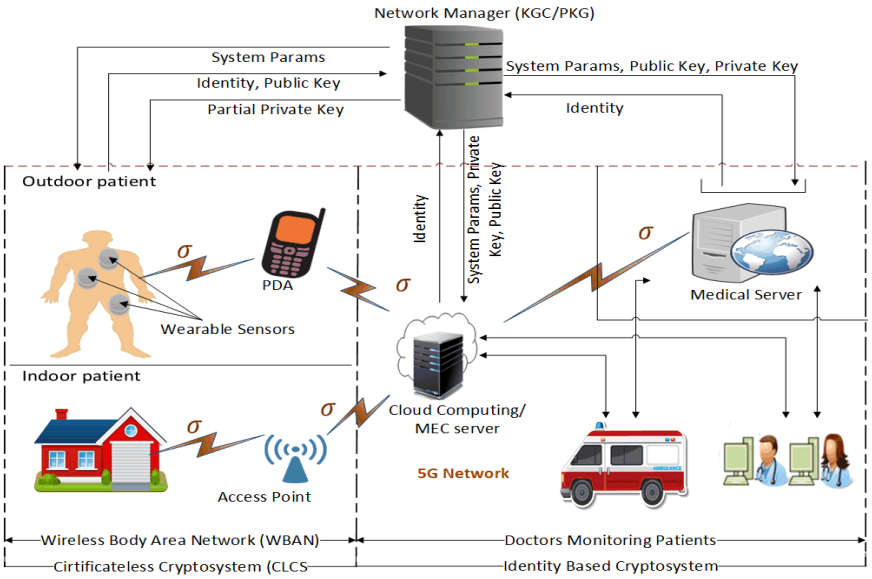

Figure 4. A secure healthcare monitoring system in the IoMTs

5. Conclusion

In this research paper, we have provided a signcryption protocol of a heterogeneous nature and used it in IoMT environment. IoMT devices and gateways are resource constrained and therefore are incapable of hosting elaborate cryptographic algorithms. There is a need for more efficient security algorithms. High efficiency may improve performance but may compromise the level of security required to protect data hence, there will always be a trade-off between efficiency and level of security. A Good choice of cryptographic operations is necessary when designing security schemes for IoMT since cryptographic operations can be energy-

intensive, leading to quicker depletion of battery life. Heavy cryptographic operations may also introduce latency that may not be acceptable in real-time sensor network applications. However, the use of 5G and MEC technologies may alleviate latency issues to some degree. The proposed scheme is both INDCCA2 and EUF-CMA secure in ROM. Our access control protocol has the capacity to demonstrate ciphertext authenticity at the MEC server reducing computation cost required to perform unsigncryption process as discussed in this paper. Further, we have compared our proposed scheme with three other related protocols and found it more efficient in terms of computational time and energy cost. The fact that our proposed scheme is more efficient makes it more suitable for implementing in resource limited environments such as IoMTs. The future direction of this work is to improve the signcryption scheme to support a multiuser and multi receiver framework.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support this work are available upon reasonable request to the corresponding author.

Author Contribution Statement

Kasyoka Philemon Nthenge: Conceptualization, Software, Formal analysis, Investigation, Resources, Writing - Original Draft, Visualization, Supervision, Project administration. **Anyembe Andrew Omala:** Methodology, Validation, Formal analysis, Resources, Writing - Review & Editing, Visualization.

References

[1] Praveen, R., & Pabitha, P. (2023). A secure lightweight fuzzy embedder based user authentication scheme for internet of medical things applications. Journal of Intelligent & Fuzzy Systems, 44(5), 7523-7542. https://doi.org/10.3233/JIFS-223617

[2] Lu, B., Xie, L., Lei, H., Liu, Y., Zhao, C., Sun, X., & Wen, Z. (2024). Research Progress in Self-Powered Pressure Sensors for Internet of Healthcare. Advanced Materials Technologies, 2301480. https://doi.org/10.1002/admt.202301480

[3] Ghadi, Y. Y., Shah, S. F. A., Mazhar, T., Shahzad, T., Ouahada, K., & Hamam, H. (2024). Enhancing patient healthcare with mobile edge computing and 5G: challenges and solutions for secure online health tools. Journal of Cloud Computing, 13(1), 93. https://doi.org/10.1186/s13677-024-00654-4

[4] Kumar, H. (2024). Wireless Sensor Networks in Healthcare System: A Systematic Review. Wireless Personal Communications, 134(2), 1013-1034. https://doi.org/10.1007/s11277-024-10954-2

[5] Vanteru, M. K., Jayabalaji, K. A., Ilango, P., Nautiyal, B., & Begum, A. Y. (2023). Multi-Sensor Based healthcare monitoring system by LoWPAN-based architecture. Measurement: Sensors, 28, 100826. https://doi.org/10.1016/j.measen.2023.100826

[6] Nawaz, A., Saidi, S., Osman, N., & Hai, N. (2024). A novel methodology for patient prescreening using wireless body area networks (WBANs). Journal of Medical Artificial Intelligence, 7. https://doi.org/10.21037/jmai-24-2

[7] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[8] Miller, V. S. (1985). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques, 417-426. https://doi.org/10.1007/3-540-39799-X_31

[9] Khan, M. A., Ullah, I., Abdullah, A. M., Mohsan, S. A. H., & Noor, F. (2023). An efficient and conditional privacy-preserving heterogeneous signcryption scheme for the Internet of drones. Sensors, 23(3), 1063. https://doi.org/10.3390/s23031063

[10] Rao, P. M., & Deebak, B. D. (2023). A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions. Ad Hoc Networks, 146, 103159. https://doi.org/10.1016/j.adhoc.2023.103159

[11] Li, F., Hong, J., & Omala, A. A. (2017). Efficient certificateless access control for industrial Internet of Things. Future Generation Computer Systems, 76, 285-292. https://doi.org/10.1016/j.future.2016.12.036

[12] Xiao, K., Chen, X., Li, H., Huang, J., Susilo, W., & Huang, Q. (2024). A fully secure lattice-based signcryption with designated equality test in standard model. Information Sciences, 658, 120015. https://doi.org/10.1016/j.ins.2023.120015

[13] Zheng, Y. (1997). Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In 17th Annual International Cryptology Conference, 1294, 165-179. https://doi.org/10.1007/BFb0052234

[14] Hussain, S., Ullah, S. S., Uddin, M., Iqbal, J., & Chen, C. L. (2022). A comprehensive survey on signcryption security mechanisms in wireless body area networks. Sensors, 22(3), 1072. https://doi.org/10.3390/s22031072

[15] Al-Riyami, S. S., & Paterson, K. G. (2003). Certificateless public key cryptography. In 9th International Conference on the Theory and Application of Cryptology and Information Security, 452-473. https://doi.org/10.1007/978-3-540-40061-5_29
[16] Khalafalla, W., Zhu, W. X., Elkhalil, A., & Elfadul, I. (2024). Efficient access control scheme for heterogeneous signcryption based on blockchain in VANETs. Cluster Computing, 1-21. https://doi.org/10.1007/s10586-024-04479-3
[17] Patil, R. Y., & Patil, Y. H. (2022). Identity-based signcryption scheme for medical cyber physical system in standard model. International Journal of Information Technology, 14(5), 2275-2283. https://doi.org/10.1007/s41870-022-00981-2
[18] Ramadan, M., & Raza, S. (2023). Secure Equality Test Technique Using Identity-Based Signcryption for Telemedicine Systems. IEEE Internet of Things Journal, 10(18), 16594-16604. https://doi.org/10.1109/JIOT.2023.3269222
[19] Rajkumar, Y., & Kumar, S. S. (2024). An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks. Wireless Networks, 30(1), 335-362. https://doi.org/10.1007/s11276-023-03473-8
[20] Li, F., & Hong, J. (2016). Efficient certificateless access control for wireless body area networks. IEEE sensors journal, 16(13), 5389-5396. https://doi.org/10.1109/JSEN.2016.2554625
[21] Jahan, M., Zohra, F. T., Parvez, M. K., Kabir, U., Al Radi, A. M., & Kabir, S. (2023). An end-to-end authentication mechanism for wireless body area networks. Smart Health, 29, 100413. https://doi.org/10.1016/j.smhl.2023.100413
[22] Arfaoui, A., Boudia, O. R. M., Kribeche, A., Senouci, S. M., & Hamdi, M. (2020). Context-aware access control and anonymous authentication in WBAN. Computers & Security, 88, 101496. https://doi.org/10.1016/j.cose.2019.03.017
[23] Barreto, P. S. L. M., Libert, B., McCullagh, N., & Quisquater, J. J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In 11th International Conference on the Theory and Application of Cryptology and Information Security, 515-532. https://doi.org/10.1007/11593447_28
[24] Gao, G., Peng, X., & Jin, L. (2019). Efficient Access Control Scheme with Certificateless Signcryption for Wireless Body Area Networks. International Journal of Network Security, 21(3), 428-437.
[25] Ouatu, A., Ghinita, G., & Rughinis, R. (2024). Accelerating Performance of Bilinear Map Cryptography using FPGA. In Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy, 103-113. https://doi.org/10.1145/3626232.3653250
[26] Barreto, P. S., Lynn, B., & Scott, M. (2004). Efficient implementation of pairing-based cryptosystems. Journal of Cryptology, 17, 321-334. https://doi.org/10.1007/s00145-004-0311-z
[27] Kasyoka, P. N., Kimwele, M., & Mbandu, S. A. (2021). Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems. Wireless Personal Communications, 118(4), 3349-3366. https://doi.org/10.1007/s11277-021-08183-y
[28] Ullah, I., Khan, M. A., Alkhalifah, A., Nordin, R., Alsharif, M. H., Alghtani, A. H., & Aly, A. A. (2021). A multi-message multi-receiver signcryption scheme with edge computing for secure and reliable wireless internet of medical things communications. Sustainability, 13(23), 13184. https://doi.org/10.3390/su132313184
[29] Hou, Y., Cao, Y., Xiong, H., Song, Y., & Xu, L. (2023). An efficient online/offline heterogeneous signcryption scheme with equality test for IoVs. IEEE Transactions on Vehicular Technology, 72(9), 12047-12062. https://doi.org/10.1109/TVT.2023.3264672
[30] Yang, X., Li, S., Li, M., Du, X., & Wang, C. (2023). Heterogeneous Signcryption Scheme From PKI to IBC With Multi-Ciphertext Equality Test in Internet of Vehicles. IEEE Internet of Things Journal. 11(8), 14178-14191. https://doi.org/10.1109/JIOT.2023.3341146
[31] Omala, A. A., Mbandu, A. S., Mutiria, K. D., Jin, C., & Li, F. (2018). Provably secure heterogeneous access control scheme for wireless body area network. Journal of Medical Systems, 42, 1-14. https://doi.org/10.1007/s10916-018-0964-z
[32] Li, F., Han, Y., & Jin, C. (2016). Practical access control for sensor networks in the context of the Internet of Things. Computer Communications, 89, 154-164. https://doi.org/10.1016/j.comcom.2016.03.007
[33] Luo, M., Luo, Y., Wan, Y., & Wang, Z. (2018). Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT. Security and Communication Networks, 2018(1), 6140978. https://doi.org/10.1155/2018/6140978
[34] Shim, K. A., Lee, Y. R., & Park, C. M. (2013). EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Networks, 11(1), 182-189. https://doi.org/10.1016/j.adhoc.2012.04.015
[35] Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, 119-132. https://doi.org/10.1007/978-3-540-28632-5_9
[36] Ma, C., Xue, K., & Hong, P. (2014). Distributed access control with adaptive privacy preserving property for wireless sensor networks. Security and Communication Networks, 7(4), 759-773. https://doi.org/10.1002/sec.777
[37] Shim, K. A. (2014). S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks. Ad Hoc Networks, 19, 1-8. https://doi.org/10.1016/j.adhoc.2014.01.011
[38] Cao, X., Kou, W., Dang, L., & Zhao, B. (2008). IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. Computer communications, 31(4), 659-667. https://doi.org/10.1016/j.comcom.2007.10.017

How to Cite: Nthenge, K. P., & Omala, A. A. (2024). Practical Heterogeneous Pairing-Free Signcryption Scheme for Internet of Medical Things Communications with Edge Computing. Medinformatics. https://doi.org/10.47852/bonviewMEDIN42023088