Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5569365, 13 pages
https://doi.org/10.1155/2021/5569365

Research Article

Securing NDN-Based Internet of Health Things through Cost-Effective Signcryption Scheme

Aroosa[1], **Syed Sajid Ullah**[2], **Saddam Hussain**[2], **Roobaea Alroobaea**[3] and **Ihsan Ali**[4]

[1]*Department of Computer Sciences, The Institute of Management Sciences, Lahore 54660, Pakistan*
[2]*IT Department, Hazara University, Mansehra 21120 KP, Pakistan*
[3]*Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia*
[4]*Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia*

Correspondence should be addressed to Ihsan Ali; ihsanalichd@siswa.um.edu.my

Received 7 February 2021; Revised 10 March 2021; Accepted 19 March 2021; Published 7 April 2021

Academic Editor: Habib Ullah Khan

The Internet of Health Things (IoHT) is an extended version of the Internet of Things that is acting a starring role in data sharing remotely. These remote data sources consist of physiological processes, such as treatment progress, patient monitoring, and consultation. The main purpose of IoHT platform is to intervene independently from geographically remote areas by providing low-cost preventive or active healthcare services. Several low-power biomedical sensors with limited computing capabilities provide IoHT's communication, integration, computation, and interoperability. However, IoHT transfers IoT data via IP-centric Internet, which has implications for security and privacy. To address this issue, in this paper, we suggest using named data networking (NDN), a future Internet model that is well suited for mobile patients and caregivers. As the IoHT contains a lot of personal information about a user's physical condition, which can be detrimental to users' finances and health if leaked, therefore, data protection is important in the IoHT. Experts and scholars have researched this area, but the reconstruction of existing schemes could be further improved. Also, doing computing-intensive tasks leads to slower response times, which further worsens the performance of IoHT. We are trying to resolve such an error, so a new NDN-based certificateless signcryption scheme is proposed for IoHT using the security hardness of the hyperelliptic curve cryptosystem. Security analysis and comparisons with existing schemes show the viability of the designed scheme. The final results confirm that the designed scheme provides better security with minimal computational and communicational resources. Finally, we validate the security of the designed scheme against man-in-the-middle attacks and replay attacks using the AVISPA tool.

1. Introduction

The Internet of Health Things (IoHT) refers to the collection of biomedical sensors and applications coupled with the networks as shown in Figure 1. Many healthcare providers use IoHT applications to improve treatments and patients' experience, reduce defects, control diseases, and reduce costs [1]. However, different healthcare things are introducing new aggressive approaches to healthcare infrastructure. This is attributed to the subsequent reasons:

(1) Medical things mainly transmit the sensitive data of patients

(2) Problems of incompatibility and complexity arise from the interaction of emerging devices and the various networks connected to them [2]

(3) As a growing sector, healthcare manufacturers are adopting IoT solutions regardless of safety. As a result, new security challenges related to confidentiality, authenticity, and availability

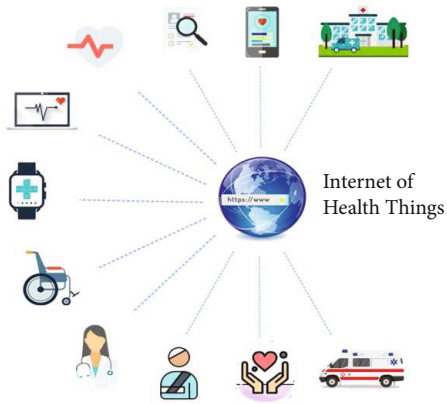

Figure 1: Internet of Health Things.

(4) As most IoT devices transmit and receive sensitive data wirelessly, this can put IoHT at risk for wireless sensor network security breaches [3]. Based on the IoHT environment's criticality, such security and privacy accidents can have devastating consequences such as loss of life and financial loss. In a healthcare information system, the details of patients can be preserved in the form of electronic health records accessible to medical specialists whenever the patient travels to the hospital. However, IoHT transfers data over the traditional Internet paradigm with risks associated with mobility and security. Therefore, IoHT risks need to be identified and assessed to provide better decision-making when adopting or constructing a secure and reliable IoHT scheme [4]

To tackle this, named data networking (NDN) is a best-chosen architecture of information-centric networking (ICN) [5]. The NDN application uses semantically meaningful, application-defined, and hierarchical names for the publication of data. Once the data is named and published, the user can send an interest packet to the network by specifying the requested content's name. Simultaneously, the intermediate NDN routers preserve a name-based forwarding table, which makes the longest prefix match in the name of interest and is sent through the appropriate interfaces [6]. Once the provider of the content receives the interest, it returns the signed data packet. The intermediate routers store these data packets in the content store for future requests. For more details regarding NDN, we refer the reader to some related publications [7, 8].

Traditionally, with a strong cryptographic scheme, malicious attacks can be prevented. Consequently, the cryptographic scheme must meet the security requirements of such as authentication, confidentiality, antireplay attack, integrity, and nonrepudiation [9]. On the other hand, the cryptographic perspectives that are used to secure the information are RSA-based cryptography [10, 11], symmetric key cryptography [12, 13], bilinear pairing [14, 15], elliptic curve cryptography (ECC) [16, 17], and hyperelliptic curve cryptography (HCC) [18, 19]. However, symmetric key-based schemes have major problems of key distribution. In contrast, RSA-based schemes incur high computational and communicational costs due to modular exponential complexities, bilinear pairing-based schemes suffer from heavy pairing operations, and ECC-based schemes outperform RSA. At the same time, HCC surpasses ECC in providing the same security features with lower cost complexities such as communication overhead, computation cost, and memory requirements.

HCC-based schemes require less storage and a smaller key of size of 80 bits in contrast to the 160 bits key of ECC and 1024 bits of RSA. They produce fewer ciphers compared to other public key cryptographic schemes. Because of these features, HCC is an attractive cryptographic phenomenon that provides security for systems utilizing limited computing resources. On the other hand, Zheng [20] introduced the concept of signcryption, which connects encryption and signature logically in a single step to reduce the cost complexities. Prior to the actual construction of signcryption, the encryption-than-signature was used to obtain privacy and authenticity. Zheng in his proposal showed that signcryption saves 50% of computation time and 85% of communicational costs as compared to the encryption-than-signature process. However, the proposed scheme of Zheng was constructed on public key cryptography (PKC) where the user's public key is a randomly selected string, so it requires a trusted entity such as certification authority (CA) to issue a certificate to link the user's public key with his/her corresponding identity. Unfortunately, the PKC suffers from the high cost of certificate management. This prevents the PKC from spreading to the real world. To reduce the burden of certificate management, Shamir [21] introduced an identity-based cryptography (IBC), where the identity of the particular users like IP address and telephone number can be used as his/her public key, thereby removing the certificate and simplifying key management. In an IBC, a reliable private key generator (PKG) is required to generate the user's private key, so the key escrow problem is inborn in the IBC.

Al-Riyami and Paterson [22] introduced certificateless cryptosystem (CLC), to eliminate key escrow problems encountered in IBS and certificate management issues in traditional PKC. In a CLC, trusted KGC is used to generate the partial private key for both the sender and receiver. The user must produce a secret value for himself/herself to combine the partial private key (PPK) with secret value to create a full private key. There has been a lot of focus on it since the introduction of CLC.

However, the first CLC scheme was presented by Barbosa and Farshim [23], combining the concepts of CLC and signcryption. Since then, many CLC schemes have been proposed in the literature [24–34].

1.1. Motivation and Contributions. Security for all health fields is always a priority in modern communication technology. However, due to limited computing resources, the implementation of an efficient and appropriate security scheme for IoHT remains an ongoing challenge. The IoHT requires a security scheme that minimizes computing, communication, and storage overhead. Although the current complex cryptographic methods, i.e., ECC and bilinear pairing, are resulting in high-cost complexities, these cryptographic algorithms are

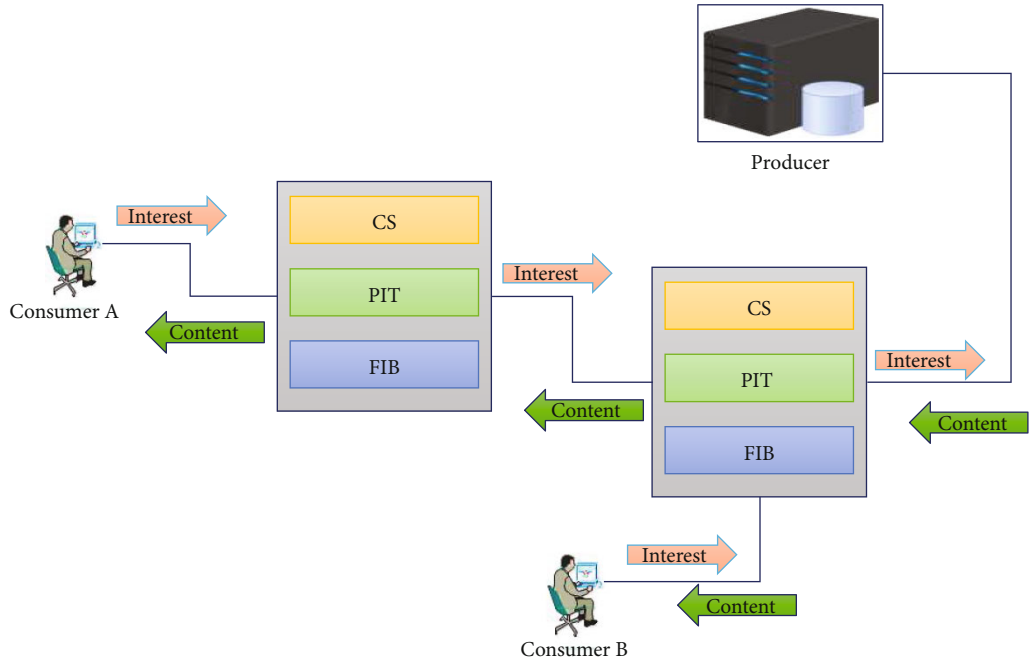

Figure 2: Basic NDN architecture with content distribution.

not compatible with low computing devices of IoHT systems. For creating a practical IoHT solution that requires minimal computation, it is necessary to use HCC. As the HCC offers the same level of security utilizing smaller key sizes in contrast to ECC and bilinear pairing, we describe our major contribution below.

(i) We designed an NDN-based IoHT scheme using the security hardness of HCC

(ii) The designed scheme offers the security services of confidentiality, authenticity, integrity, unforgeability, and nonrepudiation

(iii) Security analysis and comparisons with existing schemes show the designed scheme's viability. The obtained results confirm that the designed scheme provides better security with minimal computational and communicational resources

(iv) We validate the security of the designed scheme using the AVISPA tool

(v) Finally, we deployed the newly designed scheme on NDN-based IoHT

1.2. Overview of NDN. NDN is a future network architecture designed to cover IoT users' demands such as efficient content distribution, improved mobility, and scalable connectivity to the end-users [5]. NDN is designed to offer in-network caching and named-based routing that eliminates the location dependency, connectivity, and content distribution problems of IP-based Internet. Moreover, NDN supports 2 types of packets, namely, interest packet (IP) and data packet (DP). The IP consists of the requested content by name, while the DP consists of the requested content with information about the provider. Moreover, each NDN node maintains 3 kinds of data structures [6] as shown in Figure 2. The CS is used as a local cache memory that stores the copies of passing contents for future use to facilitate the end-users. The PIT is used as an entry list that keeps the records of incoming/outgoing IP and DP. The FIB forwards the IP and DP from one node to another using traditional protocols such as OSPF and BGP [7].

1.3. Road Map of the Article. The rest of the paper is structured as follows: Section 2 provides the knowledge about the existing literature, Section 3 provides the preliminaries of HCC, Section 4 presents the construction and the proposed network model, Section 5 provides the security analysis, Section 6 delivers the performance and discussion with the existing scheme in terms of cost complexities, and Section 7 contains the overall deployment of the designed scheme on IoHT. Finally, Section 8 contains the conclusion and implementation of the designed scheme using AVISPA tool.

2. Preliminaries

2.1. Hyperelliptic Curve Discrete Logarithm Problem (HCDLP)

(i) Let $\Theta \in \{1, 2, 3, 4, 5, \cdots, n-1\}$and $\mathscr{B} = \Theta \cdot D$, then finding Θ and $\mathscr{B}$ is known as HCDLP

2.2. Hyperelliptic Curve Computational Diffie-Hellman Problem (HCCDHP)

(i) Let $\Theta, \Omega \in \{1, 2, 3, 4, 5, \cdots, n-1\}$ and $\mathscr{B} = \Theta \cdot D, \delta = \Omega \cdot \Theta \cdot D$, then finding Θ and Ω from $\mathscr{B}$ and δ is known as HCCDHP

2.3. Syntax for the Design Scheme. The proposed scheme for NDN-based Internet of Health Things consists the following algorithms:

(i) Setup: the network manager (NM) picks a parameter of security (ℓ) as input and generates the master secret key ($\mathcal{M}$), master public key ($\mathcal{M}_{\text{pub}}$), and public parameter set ($\mathcal{P}$)

(ii) Generation of partial private key: the NM takes the users' identities (ID_u), $\mathcal{M}$, $\mathcal{M}_{\text{pub}}$, and $\mathcal{P}$ as in input and generates the partial private keys ($\mathcal{X}_u$) for users

(iii) Secret value setting: the users pick a private number as a secret value ($\mathcal{S}$)

(iv) Private key generation: the users generate private keys (PV_K) by taking $\mathcal{S}$ and $\mathcal{X}_u$ as input

(v) Public key generation: the users generate their public keys PK_u by taking $\mathcal{S}$ and deviser of HCC ($\mathcal{D}$) as input

(vi) Signcryption: the provider of the content will produce the signcrypted content (δ) by taking as input ID_u, PK_u,$\mathcal{S}$, $\mathcal{P}$, and $\mathcal{X}_u$

(vii) Unsigncryption: the consumer of the content will unsigncrypt the received δ. For this process, it takes as input δ, ID_u, PK_u,$\mathcal{S}$, $\mathcal{P}$, and $\mathcal{X}_u$

2.4. Threat Model. In the designed scheme, we adopt the most popular treat model, i.e., Dolev-Yao [35]. According to this model, the communication among two or more than two entities is not secure and trusted because the attacker has full instructions to expose the signcrypted content and to forge the signature. There are several security threats in the NDN-based IoHT environment. It means that a user can edit or delete strategic information from competitors. To preserve the security and authenticity of NDN-based IoHT devices, authentic and secure communication between entities is required.

For the security explanation of the designed scheme, we take two types of adversaries, i.e., (type I and type II) [30, 36].

(i) Type I adversary: type I adversary is often considered to be an external attacker who does not have the master secret key and can request a user's public key and replace it with its own chosen value

(ii) Type II adversary: type II adversary is also considered as malicious KGC that can compute a user's PPK using the master secret key; however, this type of adversary is not able to replace the public key of the users

3. Related Work

The related work consists of two parts like IoHT schemes in NDN and certificateless signcryption approaches.

3.1. IoHT Schemes in NDN. Saxena et al. [37] in 2015 presented a healthcare scheme for NDN. The given scheme was the first solution for NDN-based healthcare. Two years later [38], Saxena and Raychoudhury proposed another healthcare scheme in the NDN network. The goal of the scheme is to provide authenticity for emergency messages. Unfortunately, both schemes did not provide security for NDN-based healthcare. Wang and Cai [39] designed a framework to secure healthcare in NDN-enabled edge cloud. It was the first security framework of healthcare NDN. The author highlights the positive aspects of NDN for the enhancement and efficiency of healthcare. However, the authors used weighty pairing operations of bilinear pairing in attribute-based encryption.

3.2. Certificateless Signcryption Schemes. Nowadays, data transmission through the Internet is a famous communication technique because of which security becomes a major issue of concern. To save the personal information of the users and avoid unauthorized access to data, we must ensure authentication, confidentiality, and integrity of data [24]. To overcome confidentiality, the encryption method is in use. Simultaneously, for integrity, authentication, and nonrepudiation, the digital signature is operative. In the previous era, the sender uses to encrypt and then sign the document before sending it to the receiver which is known as the sign-then-encrypt method. But the sign-then-encrypt method has a flaw as it is a time-consuming process and the system needs more power which intrudes the system efficiency.

To remove the KEP, Barbosa and Farshim [23] together introduce a CLC signcryption method by achieving the CLC encryption and signature in one step. Zhou et al. [25] presented a new CLC signcryption and proved the security of their scheme based on security according to Diffie-Hellman problem. Later on, efficient CLC signcryption based on the standard scheme was introduced by Rastegari and Berenjkoub [26]. Their work shows their scheme is safer and more effective than all existing oracle model-based CLC signcryption schemes. Without BP, in 2017, Yu and Yang [27] come up with a new CLC signcryption scheme and proved the security in ROM.

Further, according to Yu and Yang, the proposed algorithm is suitable for applications like an email system and online sale. Zhou [28] proposed a new CLC signcryption technique. The security of the scheme is based on BP using the standard model. Based on the efficiency and the hardiness of the elliptic curve discrete logarithm problem (ECDLP), for the best solutions of cloud storage, Luo and Ma [29] introduced a CLC hybrid signcryption technique. However, the given scheme was constructed on the security hardness of the ECDLP, which is not suitable for the IoT environment. In 2020, Liu et al. [30] proposed a scheme for access control in WBS networks by using CLC signcryption. The design scheme is based on RSA. The security proved under the ROM. In the same year, Kasyoka et al. [31] found out the security shortcoming and provided an improved CLC signcryption scheme.

In 2017, Li et al. [32] constructed a CLC signcryption with access control for industrial wireless sensor networks.

According to the authors, the given scheme achieves the additional security properties of ciphertext authenticity, insider security, and public verifiability. Though the given scheme is more efficient than the previous access control schemes, however, the scheme of Li et al. was based on bilinear pairing which makes it inefficient for the resource-constrained environment of IoT due to heavy pairing costs.

In late 2020, Swapna et al. [34] presented a new CLC signcryption scheme under the security hardness of ECDLP under ROM. According to the authors, the proposed scheme achieves the additional security requirement of public verifiability with strong security against various types of malicious adversaries. Unfortunately, the scheme of Swapna et al. was constructed on the concept of ECC, which utilizes 160 bits keys for providing security, which is still not affordable for the limited resource devices.

However, all the above [24–34] schemes suffer from heavy communication and computation costs due to using heavy bilinear pairing, RSA, and ECC.

4. Proposed Scheme for NDN-Based Internet of Health Things

4.1. Proposed Network Model for NDN-Based Internet of Health Things. Figure 3 shows our proposed network model for NDN-based Internet of Health Things. The suggested model consists of the following entities and their functions.

(i) Network manager (NM): the NM is an authentic authority that manages and ensures secure data transformation among IoHT devices or users (consumer, producer)

(ii) Consumer: any IoHT device (such as smartphone and body sensor) or user (such as hospital, patient, and doctor) that are interested in IoHT data (like patient record stats and monitoring) in a secure way

(iii) Producer: any IoHT device (such as smartphone and body sensor) or user (such as hospital, patient, and doctor) that provides IoHT data (like patient record stats and monitoring) in a secure way

(iv) NDN nodes: the NDN nodes transfer IoHT interest and data/content between consumer and producer using NDN routing policy

In the suggested NDN-based IoHT model, at the start of communication, the IoHT devices or users need to be registered with NM. For this process, users or devices send their own identities to NM. Upon receiving, the NM generates a partial private key for users and sends it. Then, users use the partial private key and make their own public and private keys.

Let a consumer show interest in some healthcare-related data/content, then the NDN nodes will forward the interest to the producer using the traditional routing protocols such as OSPF and EIGRP. After receiving the interest, the producer will simply signcrypt the data/content and send it to the interested consumer using the reverse path. After the reception, the NDN node will forward the signcrypted data/-content through FIB. However, none of the NDN nodes will cache the content/data as it is signcrypted for a particular receiver. This process will repeat until the particular receiver user receives the interesting content/data. Here, we focus on the confidentiality and authenticity of NDN-based IoHT data, so the copy data/content will not be cached in any NDN node. Also, the data/content can only be verified with the private key of interested consumers to not facilitate any user if the content/data is cached in the intermediate NDN nodes.

4.2. Proposed Algorithm. The proposed algorithm comprises seven steps as described below. The symbols used in the construction of the designed scheme are mentioned in Table 1.

4.2.1. Setup. Given the security parameter (ℓ), this algorithm generates a master secret key ($\mathcal{M}$) and public parameter set ($\mathcal{P}$). The given algorithm is executed by the KGC and performs the following tasks.

(i) Select ($\mathcal{D}$) as a devisor of HCC of order q

(ii) Select a prime number $\mathcal{M}$, where $\mathcal{M} \in \preceq 1 \preceq (q-1)$

(iii) Compute $\mathcal{M}_{\text{pub}} = \mathcal{M} \cdot \mathcal{D}$ as his master public key

(iv) Select one-way hash functions of $(\text{SHA} - 512) = H_1, H_2, H_3, H_4$

(v) The given algorithm keeps the master secret key with itself and advertises the public parameter set $\mathcal{P} = \{\mathcal{M}_{\text{pub}}, \mathcal{D}, q, H_1, H_2, H_3, H_4\}$ in the network

4.2.2. Set Secret Value. The given algorithm is executed on the participant's side (i.e., client and producer) with identity ID_u the participants select a random number from $S \in \preceq 1 \preceq (q-1)$ as a secret value and compute their public keys as $\text{PK}_u = \mathcal{S} \cdot \mathcal{D}$.

4.2.3. Partial Private Key Generation. The KGC executes the given algorithm. It selects a random number $R_n \in \preceq 1 \preceq (q-1)$ and computes $\mathcal{N}_u = R_n \cdot \mathcal{D}$. The KGC then computes the partial private key as follows:

(i) Compute $h_1 = H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u, \mathcal{GD})\, \mathcal{M}_{\text{pub}}$

(ii) Compute $\mathcal{X}_u = R_n + \mathcal{M} \cdot h_1 \mod q$

(iii) Compute $\mathcal{T}_u = \mathcal{N}_u + H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u, \mathcal{GD})\, \mathcal{M}_{\text{pub}}$

The KGC then forwards $(\mathcal{X}_u, \mathcal{T}_u, \mathcal{N}_u)$ to the participants using a private channel. The participants, upon receiving the $\mathcal{X}_u$, can verify the validity by checking $\mathcal{X}_u \cdot \mathcal{D} = \mathcal{N}_u + H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u)\, \mathcal{M}_{\text{pub}}$.

4.2.4. Private Key Generation. In this algorithm, the participants set their private key as $\text{PV}_K = (\mathcal{X}_u, \mathcal{S})$

4.2.5. Signcryption. This given algorithm is performed on the producer side. For signcryption, the producer performs the following operations:

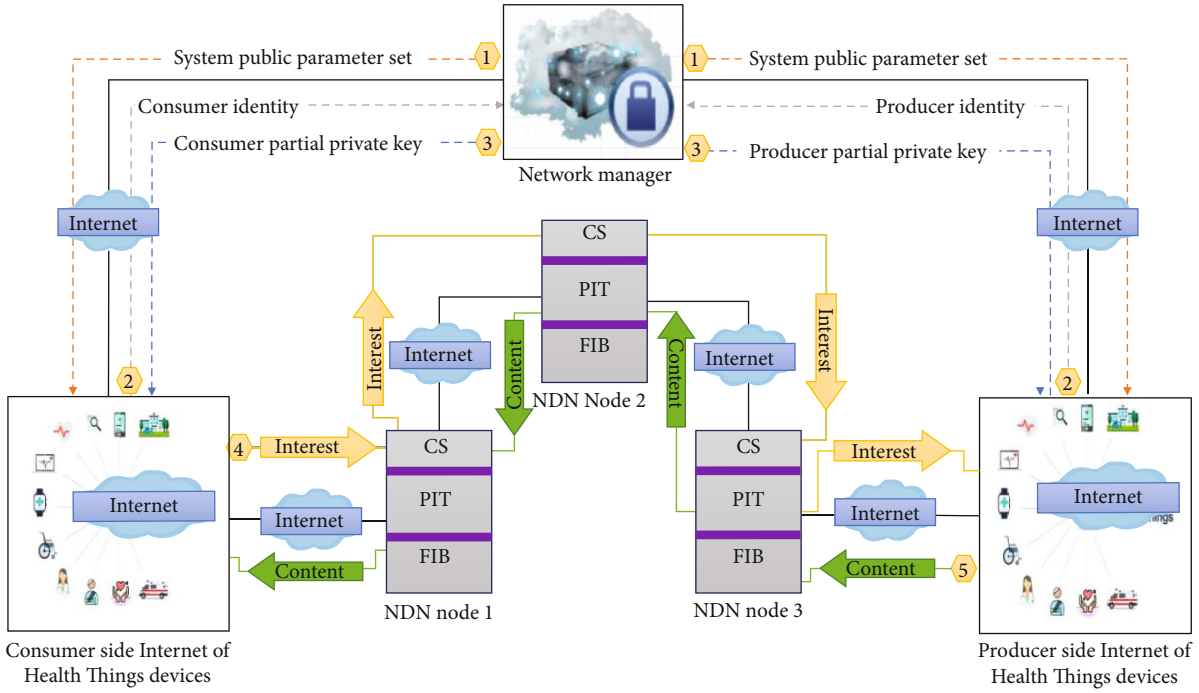

Figure 3: Proposed network model for NDN-based Internet of Health Things.

Table 1: List of notations.

S/no	Notations	Explanation
1	ℓ	Parameter of security with 80 bits size
2	$\mathcal{P}$	Public parameter set
3	H_1, H_2, H_3, H_4	Hash functions
4	ID_u	User identities
5	$\mathcal{M}$	Master secret key
6	$\mathcal{S}$	Secret values
7	$\mathcal{M}_{\mathrm{pub}}$	Master public key
8	$\mathcal{X}_u$	User partial private key
9	PV_K	User private key
10	$\mathcal{GD}$	Fresh nonce
11	δ	Signcrypted content

Table 2: Software and hardware details.

System	Specification
Library	Multiprecision integer and rational arithmetic *C*
Operating system	Windows 7-64 bits
CPU	Intel Core i7-4510
RAM	8 GB

Table 3: Running time of major operations in computation complexity.

$\mathbb{HECDM}$	$\mathbb{SPMEC}$	$\mathbb{E}$	$\mathbb{BP}$	$\mathbb{PBPM}$
0.48	0.97	1.25	14.90	4.31

(1) Pick a random number $\in \preceq 1 \preceq (q-1)$

(i) Compute $\mathcal{J} = \mathcal{W} \cdot \mathcal{D}$

(ii) Compute $\mathcal{Z}_c = \mathcal{W}_p \cdot \mathcal{T}_c$

(iii) Compute $\hbar_2 = H_2(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_p)$

(iv) Compute $\hbar_3 = H_3(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_c)$

(v) Compute $\mathcal{B}_p = \mathcal{X}_p + \mathcal{W}_p \cdot \hbar_2 + \mathcal{S}_p \cdot \hbar_3 \bmod q$

(vi) Compute $\hbar_4 = H_4(\mathcal{Z}_p, \mathcal{J}, \mathcal{T}_c, \mathrm{ID}_c)$

(2) Produce a signcrypted text as $\delta = (\mathcal{J}, \mathcal{B}_p, \hbar_4)$ and send it to the consumer

4.2.6. Unsigncryption. With δ, ID_p, and $(\mathcal{T}_p, \mathrm{PK}_p)$, the decryption is as follows:

(i) Compute $\mathcal{Z}_p = \mathcal{X}_p \cdot \mathcal{T}_p$

(ii) Compute $\hbar_2 = H_2(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_p)$

(iii) Compute $\hbar_3 = H_3(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_c)$; if $\mathcal{B}_p \mathcal{D} = \mathcal{T}_p + \hbar_2 \cdot \mathcal{J} + \hbar_3 \cdot \mathrm{PK}_p$ holds, then the received signature is valid otherwise forged.

$$\hbar_4 = H_4(\mathcal{X}_c . \mathcal{J}, \mathcal{T}_c, \mathrm{ID}_c). \quad (1)$$

Table 4: Computation cost in terms of costly mathematical operations.

Schemes	Signcryption	Unsigncryption	Total cost in (ms)
[32]	$3\mathbb{E}$	$3\mathbb{E} + 1\mathbb{BP} + 1\mathbb{PBPM}$	$6\mathbb{E} + 1\mathbb{BP} + 1\mathbb{PBPM}$
[34]	$3\mathbb{SPMEC}$	$4\mathbb{SPMEC}$	$7\mathbb{SPMEC}$
[29]	$4\mathbb{SPMEC}$	$4\mathbb{SPMEC}$	$4\mathbb{SPMEC}$
Proposed	$4\mathbb{HECDM}$	$3\mathbb{HECDM}$	$7\mathbb{HECDM}$

Table 5: Computation cost analysis in milliseconds.

Schemes	Signcryption	Unsigncryption	Total cost
[32]	3.75	22.96	26.71
[34]	2.91	3.88	6.79
[29]	3.88	3.88	7.76
Ours	1.92	1.44	3.36

4.2.7. Consistency.

$$\mathcal{Z}_c = \mathcal{W}\mathcal{T}_c = \mathcal{W}\left(\mathcal{N}_c + \hbar_1 \mathcal{M}_{\text{pub}}\right),$$
$$\mathcal{Z}_c = \mathcal{X}_c \cdot \mathcal{J} = \mathcal{W}\,\mathcal{D}(R_n + \mathcal{M}\hbar_1) = \mathcal{W}\left(\mathcal{N}_c + \hbar_1 \mathcal{M}_{\text{pub}}\right). \tag{2}$$

5. Security Analysis

Here, we provide a detailed analysis of the designed scheme for the security aspects of confidentiality, integrity, authentication, nonrepudiation, and unforgeability. Each of these aspects is discussed in more detail in the following sections.

5.1. Theorem (Confidentiality). A certificateless signcryption scheme is known to accomplish the security requirement of confidentiality if there is no possible adversary that can attain the provider's encryption key.

Proof. The designed scheme certifies the requirement of confidentiality if the adversary desires to obtain the content from signcrypted text (δ) where $\delta = (\mathcal{J}, \mathcal{B}_p, \hbar_4)$. In this case, he/she must have to find $\mathcal{J}$, $\mathcal{B}_p$, and $\hbar_4$. To fix $\mathcal{J}$, the adversary also needs to find $\mathcal{W}$ from $\mathcal{J} = \mathcal{W} \cdot \mathcal{D}$ which is infeasible due to the use of HCDLP. Furthermore, the adversary needs to calculate $\mathcal{B}_p$ here for $\mathcal{B}_p$ adversary should calculate $\mathcal{X}_p$ and $\mathcal{S}_p$ from $\mathcal{B}_p = \mathcal{X}_{p+}\mathcal{W}_p \cdot \hbar_2 + \mathcal{S}_p \cdot \hbar_3 \bmod q$ which is infeasible due to the use of HCDLP.

5.2. Theorem (Authentication). A certificateless signcryption scheme is known to accomplish the security requirement of authenticity if the content receiver is somehow able to verify the original source of content.

Proof. A client can use ID_p and $(\mathcal{T}_p, \text{PK}_p)$ to verify the signature from δ. Here, to generate δ in the producer side, the producer uses $(\mathcal{X}_p)$ and $(\mathcal{S}_p)$ which are equal to the private key of the producer of the content. Hence, the content is signed with the private key of the provider. So, the receiver of the content/message can easily verify the respective producer's identity to check the authenticity.

5.3. Theorem (Integrity). A certificateless signcryption approach is known to attain the security requirement of integrity if there is no possible adversary that can produce the equivalent hash value for the different sizes of the message.

Proof. The producer of the content/message takes the "hash value" "$\mathcal{B}_p = \mathcal{X}_{p+}\mathcal{W}_p \cdot \hbar_2 + \mathcal{S}_p \cdot \hbar_3 \bmod q$" before sending the content/message to the consumer. Suppose an adversary tries to change the cipher content, in that case, the content receiver can verify the ciphertext by doing the subsequent steps. The consumer of the content/message first computes $\mathcal{B}_p\mathcal{D} = \mathcal{T}_p + \hbar_2 \cdot \mathcal{J} + \hbar_3 \cdot \text{PK}_p$ and $\hbar_4 = H_4(\mathcal{X}_c \cdot \mathcal{J}, \mathcal{T}_c, \text{ID}_c)$; if it holds, then the content is valid; else, the content/-message has been changed.

5.4. Theorem (Unforgeability). Suppose an adversary is able to negotiate the $\mathcal{X}_p$) of the provider, in that case, the certificateless signcryption approach meets the security requirement of unforgeability.

Proof. In the designed approach, if an adversary attempts to produce a legal signature, they need to compute $\mathcal{B}_p$ from $\delta = (\mathcal{J}, \mathcal{B}_p, \hbar_4)$, and for doing that, he/she needs to find $\mathcal{J}$. To fix $\mathcal{J}$, the adversary needs to obtain $\mathcal{W}$ from $\mathcal{J} = \mathcal{W} \cdot \mathcal{D}$, which is infeasible due to the security hardness of HCDLP.

5.5. Theorem (Nonrepudiation). A certificateless signcryption scheme is known to accomplish the security requirement of nonrepudiation if a producer/provider of the content/message cannot deny from his/her generated signcrypted ciphertext.

Proof. The content/message is normally signed with the private key $(\mathcal{X}_p)$ and $(\mathcal{S}_p)$ of the producer/provider. In the designed scheme, the consumer/receiver of the content/message can authenticate the identity ID_p of the provider. So, the provider of the content/message later cannot repudiate his own signature.

6. Complexity Analysis

We compared our scheme with previously suggested certificateless signcryption schemes on the following two bases.

6.1. Computation Cost. In the following section, we will demonstrate the computational cost complexity of our scheme

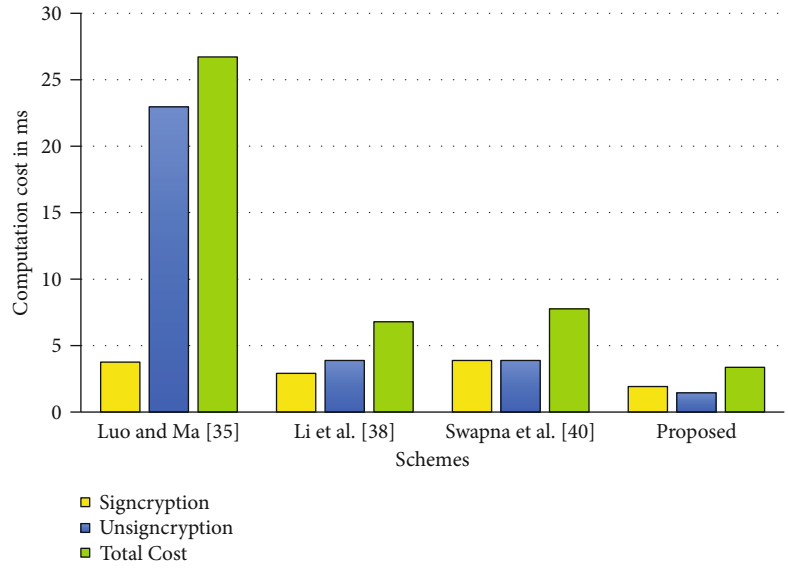

Figure 4: Computation cost complexity.

and previously suggested certificateless signcryption schemes such as Li et al. [32], Swapna et al. [34], and Luo and Ma [29]. To estimate the computational complexity, we considered the cost of signcryption and unsigncryption. However, to calculate the operational computation cost of any scheme, we mostly consider the costly mathematical operation used in that particular cryptographic scheme. For our computation complexity analysis, we take bilinear pairing ($\mathbb{BP}$), pairing-based point multiplication ($\mathbb{PBPM}$), exponential ($\mathbb{E}$), scalar point multiplication of elliptic curve ($\mathbb{SPMEC}$), and hyperelliptic curve devisor multiplication ($\mathbb{HECDM}$), respectively. The software and hardware specification [19, 33] used with the running time is shown in Tables 2 and 3.

From the results in Tables 4 and 5 and Figure 4, it is clear that our scheme works more efficiently in terms of computational complexity than the previous ones.

6.1.1. Cost Reduction. The cost reduction/percentage improvement can be attained using the given formula [18].

$$= \left(\frac{\text{Computation cost of previous scheme} - \text{Computation cost of designed scheme}}{\text{Computation cost of previous scheme}}\right) * 100. \quad (3)$$

(i) The percentage improvement of the designed scheme from Li et al. [32] is as follows:

$$= \left(\frac{26.71 - 3.36}{26.71}\right) * 100 = 87.42\%. \quad (4)$$

(ii) The percentage improvement of the designed scheme from Swapna et al. [34] is as follows:

Table 6: Variables used in our analysis.

Name	Notation	Size (bits)
BP	$(\mathbb{G})$	1024
HCC	$(\mathbb{q})$	80
ECC	$(\mathbb{n})$	160
Message	$(\mathbb{m})$	512

Table 7: Communication overhead analysis in bits.

Schemes	Ciphertext size	Size (bits)
Luo and Ma [29]	$3(\mathbb{n}) + (\mathbb{m})$	992
Li et al. [32]	$3(\mathbb{G}) + (\mathbb{m})$	3584
Swapna et al. [34]	$3(\mathbb{n}) + (\mathbb{m})$	992
Ours	$3(\mathbb{q}) + (\mathbb{m})$	752

$$= \left(\frac{6.79 - 3.36}{6.79}\right) * 100 = 50.51\%. \quad (5)$$

(iii) The percentage improvement of the designed scheme from Luo and Ma [29] is as follows:

$$= \left(\frac{7.76 - 3.36}{7.76}\right) * 100 = 56.70\%. \quad (6)$$

6.2. Communication Overhead. Here, we show a comparative analysis of the given scheme with the relevant existing schemes [29, 32, 34]. However, to calculate the operational communication overhead of any scheme, we mostly study the additional bits that an original message will carry. For our scheme, we used variables such as elliptic curve cryptosystem (ECC): $(\mathbb{n})$, hyperelliptic curve cryptosystem (HCC):

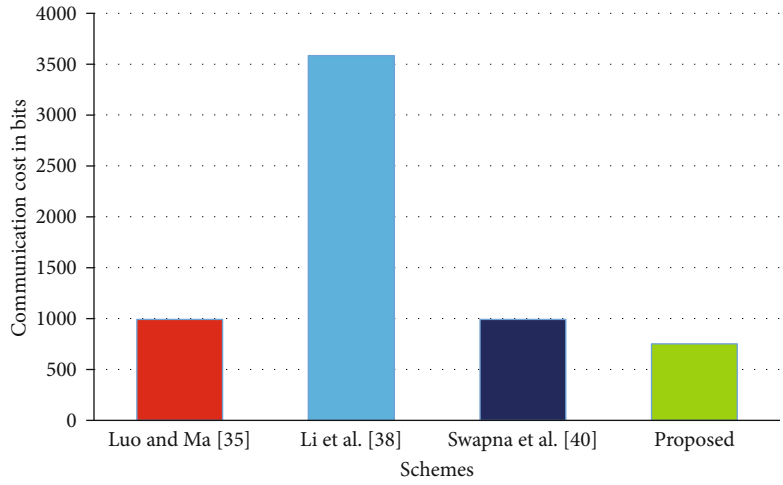

Figure 5: Communication cost complexity.

($\mathbb{q}$), bilinear pairing (BP): ($\mathbb{G}$), and message: ($\mathbb{m}$) as further shown in Table 6.

From the results in Tables 7 and Figure 5, it is clear that our scheme works more efficiently in terms of communicational overhead than the previous ones.

6.2.1. Cost Reduction. The cost reduction/percentage improvement can be attained using the given formula [18].

$$= \left(\frac{\text{Computation cost of previous scheme} - \text{Computation cost of designed scheme}}{\text{Computation cost of previous scheme}}\right) * 100. \quad (7)$$

(i) The percentage improvement of the designed scheme from Li et al. [32] is as follows:

$$= \left(\frac{3584 - 752}{3584}\right) * 100 = 79.01\%. \quad (8)$$

(ii) The percentage improvement of the designed scheme from Swapna et al. [34] and Luo and Ma [29] is as follows:

$$= \left(\frac{6.79 - 3.36}{6.79}\right) * 100 = 50.51\%. \quad (9)$$

7. Deployment on NDN-Based Internet of Healthcare

Figure 6 shows a robust and secure deployment of the given scheme on the NDN-based Internet of IoHT. We consider many connected IoH devices that can exchange healthcare information for this deployment. Furthermore, the medical devices are linked to NDN policy [7, 8]. The complete deployment for secure communication is described in the subsequent steps.

7.1. Registration and Key Generation. In this phase, the KGC enrolls both the participants with itself. To do so, the KGC picks a security parameter (ℓ), selects D of HCC of order q, selects a prime number $\mathcal{M}$, where $\mathcal{M} \in \preceq 1 \preceq (q-1)$, as a master secret key, then computes $\mathcal{M}_{\text{pub}} = \mathcal{M} \cdot \mathcal{D}$, and selects one-way hash functions H_1, H_2, H_3, H_4. The KGC keeps the master secret key with itself and advertises the public parameter set $\mathcal{P} = \{\mathcal{M}_{\text{pub}}, \mathcal{D}, q, H_1, H_2, H_3, H_4\}$ in the network. After the advertisement of KGC, the consumer and producer first select random number from $\mathcal{S} \in \preceq 1 \preceq (q-1)$ as a secret value and compute their public keys as $\text{PK}_c = \mathcal{S} \cdot \mathcal{D}$ and $\text{PK}_p = \mathcal{S} \cdot \mathcal{D}$. Then, the participants send their identities (ID_c, ID_p) to KGC. It selects a random number $R_n \in \preceq 1 \preceq (q-1)$ and compute $\mathcal{N}_u = R_n \cdot \mathcal{D}$. The KGC then computes the partial private key as compute $h_1 = H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u)\,\mathcal{M}_{\text{pub}}$, compute $\mathcal{X}_u = R_n + \mathcal{M} \cdot h_1 \bmod q$, and compute $\mathcal{T}_u = \mathcal{N}_u + H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u)\,\mathcal{M}_{\text{pub}}$. The KGC then forwards the $(\mathcal{X}_u, \mathcal{T}_u, \mathcal{N}_u)$ to the client/consumer/receiver of the content and provider of the content through a private channel. The consumer and producer upon receiving the $\mathcal{X}_u$ can verify the validity by checking $\mathcal{X}_u \cdot \mathcal{D} = \mathcal{N}_u + H_1(\text{ID}_u, \mathcal{N}_u, \text{PK}_u)\,\mathcal{M}_{\text{pub}}$.

7.2. Signcryption. Whenever a consumer of the content shows an interest in some healthcare information, after receiving, the producer will generate signcrypted content for the consumer as to pick a random number $\mathcal{W} \in \preceq 1 \preceq (q-1)$, compute $\mathcal{J} = \mathcal{W} \cdot \mathcal{D}$, compute $\mathcal{Z}_c = \mathcal{W}_p \cdot \mathcal{T}_c$, compute $\hbar_2 = H_2(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \text{ID}_c, \text{PK}_p)$, compute $\hbar_3 = H_3(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \text{ID}_c, \text{PK}_c)$, compute $\mathcal{B}_p = \mathcal{X}_{p+}\mathcal{W}_p \cdot \hbar_2 + \mathcal{S}_p \cdot \hbar_3 \bmod q$, and compute $\hbar_4 = H_4(\mathcal{Z}_p, \mathcal{J}, \mathcal{T}_c, \text{ID}_c)$. Finally, produce a signcrypted text as $\delta = (\mathcal{J}, \mathcal{B}_p, \hbar_4)$ and send it to the consumer.

7.3. Unsigncryption. When the consumer receives the signcrypted content, it verifies the signature and decrypts the

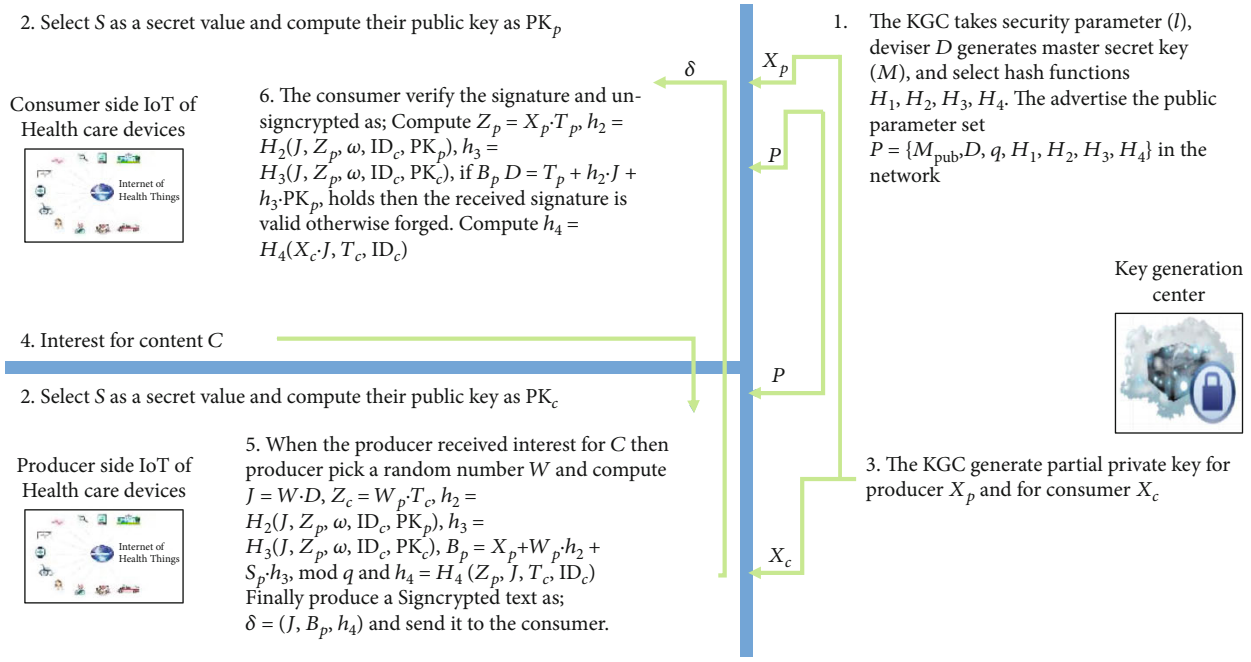

Figure 6: Deployment of the designed scheme.

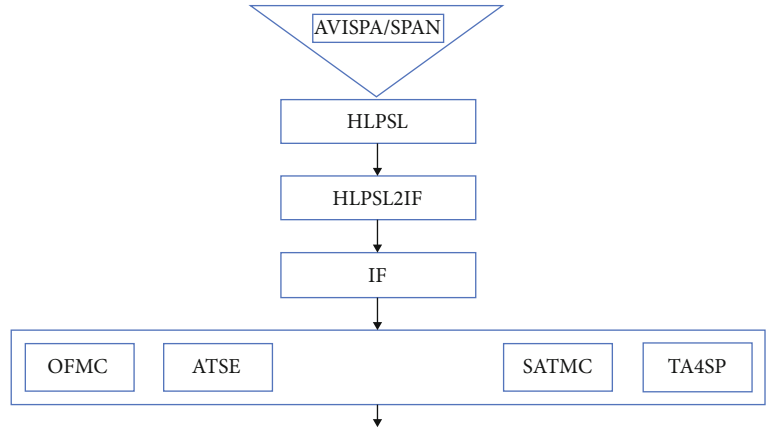

Figure 7: Pushdown flow of AVISPA.

content as compute $\mathcal{Z}_p = \mathcal{X}_p \cdot \mathcal{T}_p$, compute $\hbar_2 = H_2(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_p)$, and compute $\hbar_3 = H_3(\mathcal{J}, \mathcal{Z}_p, \mathcal{GD}, \mathrm{ID}_c, \mathrm{PK}_c)$. If $\mathcal{B}_p \mathcal{D} = \mathcal{T}_p + \hbar_2 \cdot \mathcal{J} + \hbar_3 \cdot \mathrm{PK}_p$ holds, then the received signature is valid otherwise forged. Also, the consumer can decrypt $\hbar_4 = H_4(\mathcal{X}_c \cdot \mathcal{J}, \mathcal{T}_c, \mathrm{ID}_c)$.

8. Simulation of the Designed Scheme through AVISPA

AVISPA tool [40] is a top-down automated validation of the security protocols used to verify the resistivity of a given security protocol against replay attacks and man-in-the-middle attacks. AVISPA uses the rule-oriented high-level protocol specification language (HLPSL) [41], to verify the security protocol. The code of the HLPSL is transformed to an intermediate format (IF) via a translator known as HLPSL-2-IF [42]. The IF is then given to the required four backend checkers, namely, OFMC, CL-AtSe, SATMC, and TA4SP. For more details regarding NDN, we recommend readers to study [40]. A generic structure of AVISPA is illustrated in Figure 7.

This section implemented mandatory roles for the session, goals, and environment. We evaluate the newly designed scheme using the two backend checkers of AVISPA such as constraint-logic-based attack searcher (CL-AtSe) and on-the-fly model checker (OFMC) with the help of the graphical user interface (GUI) of security protocol animator (SPAN) [43]. Moreover, for evaluation, AVISPA implements the Dolev-Yao threat model [35]. The simulation results reported in Figures 8 and 9 show the formal verification and security of the designed scheme against man-in-the-middle attacks and replay attacks.

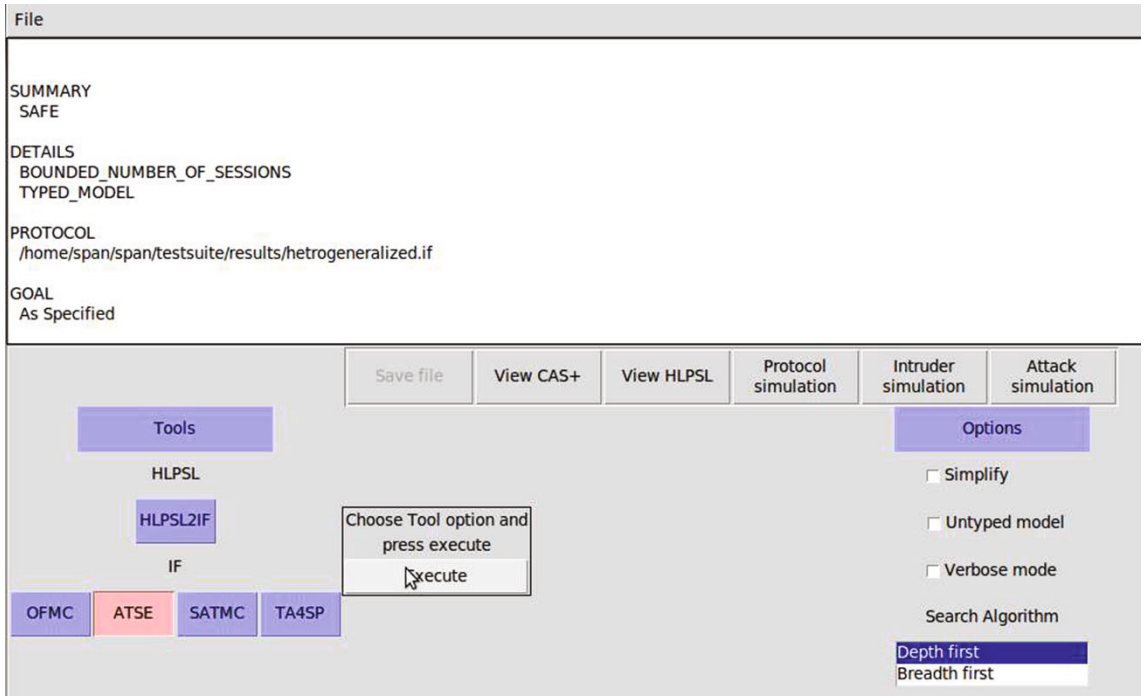

Figure 8: Proposed scheme simulation results of ATSE.

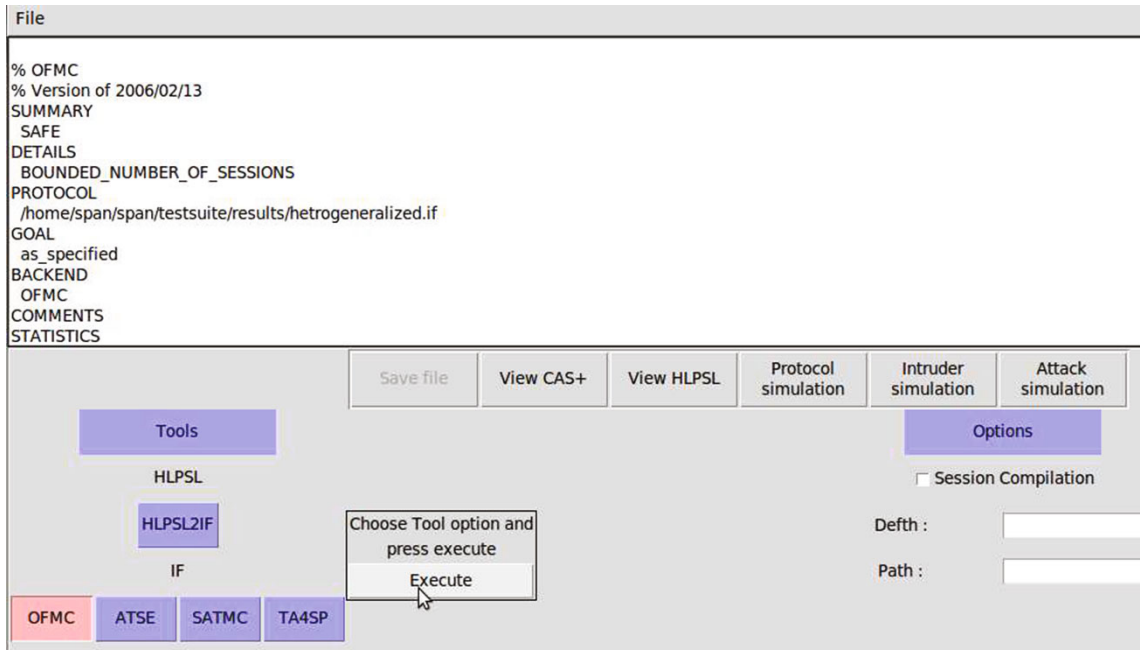

Figure 9: Proposed scheme simulation results of OFMC.

9. Conclusion

As the number of biomedical devices coupled with the Internet grows, providing strong security with privacy is becoming a prime concern. The overuse of IoHT devices raises a serious issue in the medical domain. Due to the critique and sensitivity of the data within the healthcare domain, proper security and privacy in IoHT undermines patient privacy and endangers patients' lives. However, IoHT transfers data via a public channel, which has implications for security and privacy. Researchers suggest named data networking (NDN), a future Internet model that suits the caregivers and mobile patients to address this issue. Hence, in this article, we have proposed a lightweight certificateless signcryption scheme for NDN-based IoHT. For most IoHT applications, traditional cryptographic algorithms are not

practical due to low power-embedded devices' power constraints. For this cause, we use hyperelliptic curve cryptosystem (HCC) which utilizes minimal key size. In addition, after comparing with the relevant schemes, the designed scheme has proven to be effective in terms of cost complexities. For more evidence, we validate the designed scheme attacks' security using the formal verification tool AVISPA.

An extension of the designed scheme is essential that provides simultaneous encryption and signature. We also aim to improve the security of the given scheme by adding some other elements of official formal analysis, such as random oracle model. All these factors are under development stages and will be taken into consideration in the near future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

The authors are grateful to the Taif University Researchers Supporting Project (number TURSP-2020/36), Taif University, Taif, Saudi Arabia. This research work was also partially supported by the Faculty of Computer Science and Information Technology, University of Malaya, under Postgraduate Research Grant PG035-2016A.

References

[1] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: taxonomy and risk assessment," in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 112–120, Singapore, 2017.

[2] P. Waurzyniak, *Securing Manufacturing Data in the Cloud*, Advanced Manufacturing, 2016.

[3] S. Prakash, "An overview of healthcare perspective based security issues in wireless sensor networks," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2016.

[4] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 457–464, Santorini, Greece, 2019.

[5] A. Afanasyev, J. Burke, T. Refaei, L. Wang, B. Zhang, and L. Zhang, "A brief introduction to named data networking," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pp. 1–6, Los Angeles, CA, USA, 2018.

[6] R. K. Thelagathoti, S. Mastorakis, A. Shah, H. Bedi, and S. Shannigrahi, "Named data networking for content delivery network workflows," 2020, https://arxiv.org/abs/2010.12997.

[7] L. Zhang, A. Afanasyev, J. Burke et al., "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[8] A. Afanasyev, J. Shi, B. Zhang et al., *NFD Developer's Guide*, Department of Computer Science, University of California, Los Angeles, Los Angeles, CA, USA, 2014.

[9] U. Ali, *RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption*, IEEE Access, 2021, http://ieeexplore-ieee-org.ezproxy.um.edu.my/document/9389538.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 26, no. 1, pp. 96–99, 1983.

[11] W. P. Wardlaw, "The RSA public key cryptosystem," in *Coding Theory and Cryptography*, pp. 101–123, Springer, 2000.

[12] M. Agren, *On Some Symmetric Lightweight Cryptographic Designs*, Department of Electrical and Information Technology, Faculty of Engineering, 2012.

[13] H. Delfs, H. Knebl, and H. Knebl, *Introduction to Cryptography*, vol. 2, Springer, Heidelberg, 2002.

[14] R. Dutta, R. Barua, and P. Sarkar, *Pairing-Based Cryptography: A Survey*, 2004.

[15] A. Menezes, "An introduction to pairing-based cryptography," *Recent Trends in Cryptography*, vol. 477, pp. 47–65, 2009.

[16] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[17] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2018.

[18] S. Hussain, I. Ullah, H. Khattak et al., "A lightweight and formally secure certificate based Signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[19] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C. M. Chen, and S. Kumari, "A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT)," *Journal of Information Security and Applications*, vol. 58, p. 102625, 2021.

[20] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+cost (encryption)," in *Annual International Cryptology Conference*, pp. 165–179, Berlin, Heidelberg, 1997.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 196, pp. 47–53, Heidelberg, 1984.

[22] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International conference on the theory and application of cryptology and information security*, vol. 2894, pp. 452–473, Berlin, Heidelberg, 2003.

[23] M. Barbosa and P. Farshim, "Certificateless signcryption," in *2008 ACM Symposium on Information, Computer and Communications Security*, pp. 369–372, ACM, New York, 2008.

[24] A. Mehmood, I. Noor-Ul-Amin, and A. I. Umar, "Public verifiable generalized authenticated encryption based on hyper elliptic curve," *Journal of Applied Environmental and Biological Sciences*, vol. 7, pp. 194–200, 2017.

[25] C. Zhou, G. Gao, and Z. Cui, "Certificateless signcryption in the standard model," *Wireless Personal Communications*, vol. 92, pp. 495–513, 2016.

[26] P. Rastegari and M. Berenjkoub, "An efficient *certificateless signcryption* scheme in the standard model," *ISeCure*, vol. 9, pp. 3–16, 2017.

[27] H. Yu and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *The Computer Journal*, vol. 60, no. 8, pp. 1187–1196, 2017.

[28] C. Zhou, "Certificateless signcryption scheme without random oracles," *Chinese Journal of Electronics*, vol. 27, no. 5, pp. 1002–1008, 2018.

[29] W. Luo and W. Ma, "Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage," *Electronics*, vol. 8, p. 590, 2019.

[30] X. Liu, Z. Wang, Y. Ye, and F. Li, "An efficient and practical certificateless signcryption scheme for wireless body area networks," *Computer Communications*, vol. 162, pp. 169–178, 2020.

[31] P. Kasyoka, M. Kimwele, and S. M. Angolo, *Cryptoanalysis of a Pairing-Free Certificateless Signcryption Scheme*, ICT Express, 2020.

[32] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial Internet of Things," *Future Generation Computer Systems*, vol. 76, pp. 285–292, 2017.

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

[34] G. Swapna, K. A. Ajmath, and G. Thumbur, "An efficient pairing-free certificateless signcryption scheme with public verifiability," *Journal of Mathematics and Computer Science*, vol. 11, no. 1, pp. 24–43, 2020.

[35] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[36] S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, and S. M. Arif, "A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking based Internet of Things," *IEEE Access*, vol. 9, pp. 40198–40215, 2021.

[37] D. Saxena, V. Raychoudhury, and N. Sri Mahathi, "SmartHealth-NDNoT: Named Data Network of Things for healthcare services," *MobileHealth@ MobiHoc*, pp. 45–50, 2015.

[38] D. Saxena and V. Raychoudhury, "Design and verification of an NDN-based safety-critical application: a case study with smart healthcare," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 5, pp. 991–1005, 2017.

[39] X. Wang and S. Cai, "Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud," *Future Generation Computer Systems*, vol. 112, pp. 320–329, 2020.

[40] L. Vigano, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.

[41] D. von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proceedings of 3rd APPSEM II (Applied Semantics II) Workshop (APPSEM'05)*, pp. 1–17, Germany, 2005.

[42] S. S. Ullah, I. Ullah, H. Khattak et al., "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with Internet of Things," *IEEE Access*, vol. 8, pp. 98910–98928, 2020.

[43] S. S. Ullah, S. Hussain, A. Gumaei, and H. AlSalman, "A secure NDN framework for Internet of Things enabled healthcare," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 223–240, 2021.