Computers, Materials & Continua
DOI:10.32604/cmc.2021.014413
Article

Tech Science Press

A Secure NDN Framework for Internet of Things Enabled Healthcare

Syed Sajid Ullah[1], Saddam Hussain[1,*], Abdu Gumaei[2,3] and Hussain AlSalman[2,4]

[1]IT Department, Hazara University, Mansehra, 21120, Pakistan
[2]Research Chair of Pervasive and Mobile Computing, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh, 11543, Saudi Arabia
[3]Department of Computer Science, Taiz University, Taiz, Yemen
[4]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, 11543, Saudi Arabia
[*]Corresponding Author: Saddam Hussain. Email: saddamicup1993@gmail.com
Received: 18 September 2020; Accepted: 18 October 2020

Abstract: Healthcare is a binding domain for the Internet of Things (IoT) to automate healthcare services for sharing and accumulation patient records at anytime from anywhere through the Internet. The current IP-based Internet architecture suffers from latency, mobility, location dependency, and security. The Named Data Networking (NDN) has been projected as a future internet architecture to cope with the limitations of IP-based Internet. However, the NDN infrastructure does not have a secure framework for IoT healthcare information. In this paper, we proposed a secure NDN framework for IoT-enabled Healthcare (IoTEH). In the proposed work, we adopt the services of Identity-Based Signcryption (IBS) cryptography under the security hardness Hyperelliptic Curve Cryptosystem (HCC) to secure the IoTEH information in NDN. The HCC provides the corresponding level of security using minimal computational and communicational resources as compared to bilinear pairing and Elliptic Curve Cryptosystem (ECC). For the efficiency of the proposed scheme, we simulated the security of the proposed solution using Automated Validation of Internet Security Protocols and Applications (AVISPA). Besides, we deployed the proposed scheme on the IoTEH in NDN infrastructure and compared it with the recent IBS schemes in terms of computation and communication overheads. The simulation results showed the superiority and improvement of the proposed framework against contemporary related works.

Keywords: Named data networking; healthcare; identity-based signcryption

1 Introduction

The IoTEH has recently been introduced to alleviate the issue of scarce resources due to the growing aging population [1,2]. The IoTEH system with all available resources to perform healthcare activities such as diagnosis, monitoring, and remote surgery [3]. The whole framework is devoted to extending the healthcare amenities from hospitals and communities to homes.

Throughout wireless technology has been applied widely to integrate monitoring devices, including front-end network manager [4]. The system connects patients with all healthcare resources available in the community such as hospitals, physicians, rehabilitation centers, nurses, paramedics, and ambulances. All the content is networked together to the Internet, supported by programs based on Radio-Frequency Identification (RFID) technology [5,6]. Automated resource allocation has been developed to identify rehabilitation solutions to meet the specific needs of individual patients. However, IoTEH exchanges data/information over IP-based Internet with the risks related to security, privacy and mobility.

To overcome the aforementioned limitations of the IP-based Internet paradigm, a new Internet paradigm called Named Data Networking (NDN) has been introduced [7]. NDN aimed to offer in-network caching, built-in mobility support, and named-based routing that can provide scalable connectivity to the IoT devices with efficient information access to the end-users [8,9]. By keeping the positive aspects of NDN, a few schemes have been suggested for NDN based healthcare [10–12].

However, until now, there is no concrete security plan suggested that can protect the NDN based healthcare information. As the IoTEH in NDN requires the essential properties of authentication and confidentiality, which can easily be achieved by implementing a secure digital signature and encryption (sign-then-encrypt) scheme [13,14]. Unfortunately, the trivial combination of sign-then-encrypt is costly and subject to some subtle attacks [15]. For this purpose, in 1997, Zheng [16], tossed the concept of a new cryptographic primitive toned as Signcryption, which provides the services of confidentiality and authenticity at a reasonable cost than the traditional sign-then-encrypt approach. Since then plenty of practical and innovative signcryption schemes have been suggested in recent years [17–20]. However, the idea Zheng was primarily based on the old concept of Public Key Infrastructure (PKI) and therefore suffers from the certificate-related overheads.

In 1984, in a seminar, Shamir coined the concept of Identity-Based Cryptography (IBC), which is aimed to provide a viable alternative to traditional PKI in terms of convenience and efficiency [21]. An interesting feature of this type of cryptosystem is that any binary string that identifies the user, such as an email address, can be the public key of the users. Using identities as a public key eliminates the need for public-key certificates [22]. The first identity-based signature was mentioned in the Shamir proposal; however, the Identity-Based Encryption (IDBE) scheme was not established until 2001, when a practical IDBE scheme was proposed from bilinear pairing [23]. Since then, IBC and its applications have been the talk of the town for the past decade.

To provide efficient and robust security with minimal computation overheads, the common approaches used are Bilinear Pairing (BRPG), RSA, ECC, and HCC [24–29]. However, HCC provides the same level of security in contrast with ECC, RSA, and BRPG [30–32] using small key sizes. Therefore, HCC is considered as the most compact and efficient cryptographic mechanism that provides better performance than ECC, BRPG, and RSA with high efficiency and lower-key length [15]. The HCC uses 80-bit keys with strong security that will better suit the IoTEH in NDN infrastructure.

1.1 NDN Overview

NDN is a new data-centric architecture that defines three different roles, such as Routers, Clients/Customer, and Providers with two types of packets (i.e., Interest Packet and Data Packet). Moreover, each router maintains three kinds of data structures, such as Pending Interest Table

(PIT), Forwarding Information Base (FIB), and Content Store (CS) [33]. The data attainment process begins by sending an Interest with a particular name from the client's side. The routers rely on FIBs for transferring the interest to a potential provider and generate a PIT entry list on each router to establish an opposite path. Based on the opposite path, the provider of any interest returns the data to the client with the target data. The CS then stores the targeted data that pass through it for future use [34].

Suppose Client A begins the data attainment process by sending an Interest with a particular name, as shown in Fig. 1. Initially, the Interest of Client A will be transferred using the services of FIB to the potential provider of the content/data. The feedback to that particular interest will be stored inside the CS of Router 4, Router 3, and Router 1 for future reuse. Later on, if another Client B needs the same content/data, then the interest will be satisfied locally from the CS of Router 3, instead of transferring the Interest of Client B to the original provider of the content/data [35].

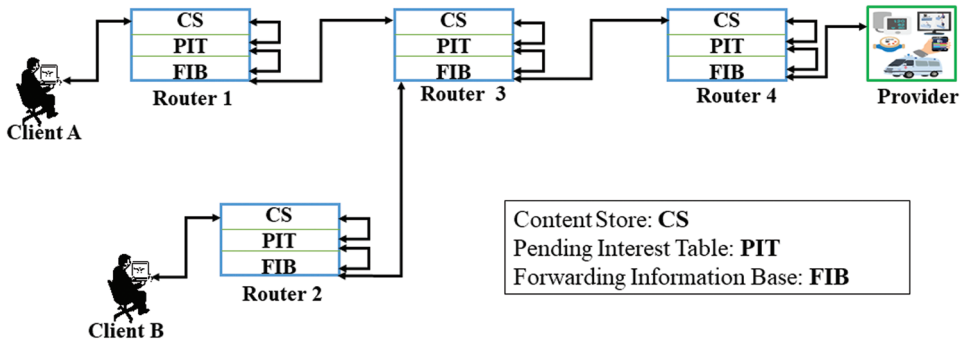

Figure 1: Generic illustration of information distribution in NDN

1.2 Contributions

Inspired by the above-mentioned discussion, we propose an IBS scheme for IoTEH in NDN networks. The proposed scheme is based on the concept of HCC, which provides the same level of security in contrast with ECC, RSA, and BRPG using small key sizes. The key research finding is mentioned below:

- We proposed a secure NDN framework for Internet of Things Enabled Healthcare (IoTEH) using Identity-Based Signacryption (IBS) cryptography.
- We used a lightweight Hyperelliptic Curve Cryptosystem (HCC) for the efficiency in terms of computation and communication overheads.
- We also validate our scheme using the simulation tool "AVISPA."
- We deployed the newly proposed scheme on IoT enabled healthcare in NDN networks.
- To conclude, we also compared our proposed scheme with relevant existing IBS schemes and the results show that the given scheme is more efficient in terms of computation and communication overheads than the previous.

1.3 Paper Organization

In Section 2, we discuss the related work about NDN based healthcare and IBS schemes. Section 3 comprises the preliminaries, threat model, and syntax of the proposed scheme. Section 4 includes the proposed network model and the proposed algorithm. Section 5 describes the security

analysis for the proposed scheme. Section 6 includes a comparative analysis. In Section 7, we deployed our scheme on IoTBH in NDN networks, and Section 8 concludes our research.

2 Related Work

In this section, we divide the given literature into two portions, such as NDN based schemes for healthcare and IBS schemes.

2.1 NDN Based Schemes for Healthcare

In 2015, Saxena et al. [10] proposed an NDN based solution for healthcare. The proposed scheme can locate a network-based healthcare service. Later in 2017, Saxena et al. [11] tossed another NDN based scheme for emergency healthcare services. The author's aims to verify the authenticity of emergency messages in NDN based healthcare. However, in both the schemes [10,11], the authors did not provide a concrete security plan for the proposed scheme.

Recently, Wang et al. [12] proposed a monitoring framework to secure NDN-based healthcare infrastructure using the services of edge cloud. The authors, for the first time, introduce a security framework for NDN-based healthcare. In the given framework, the author exploits the advantages of NDN to enhance the efficiency of medical data. Unfortunately, the author used heavy attribute-based encryption using bilinear pairing.

2.2 Identity-Based Signcryption (IBS) Schemes

Signcryption and IBC [36] is an exciting research topic to develop a secure and effective IBS scheme. In 2002, Malone-Lee [23] provided the first IBS scheme using BRPG. Later in 2006, Duan et al. [37], proposed a multi-receiver IBS scheme for multiple receivers. However, the given scheme is subject to massive pairing operation due to BRPG. In 2008, Li et al. [38] coined an identity-based broadcast signcryption scheme for application to transmit a message securely and authentically. However, the given scheme is subject to massive pairing operation due to BRPG.

Later in 2013, Libert et al. [39] showed that the scheme of Malone-Lee's did not provide the semantic security because the signature of the signed message appears in the ultimate ciphertext. The authors also proposed three new IBS schemes, but they did not provide the essential security properties of public verifiability and forward secrecy. Similarly, the concept of IBS was further expanded to cater to further applications. In 2017, Nayak [40] constructed a new IBS scheme based on ECC. Unlike the previous schemes, the given approach reduces the computational and communicational resources. Besides, the given scheme provides the security assets of authentication, integrity, confidentiality, and unforgeability. However, there is still a need for improvement in the communication and computation cost because the cost of the scalar point multiplication on the elliptic curve is still not affordable for the resource-constrained environment. Later, in the same year, Reddi et al. [41] presented an IBS that is used to authenticate and verify both parties involved in the communication. In the proposed work, the author incorporated the idea of IBS into the Key Agreement Protocol. However, the given scheme is subject to massive pairing operation due to BRPG. Later, in 2017, Karati et al. [42] proposed an IBS scheme for the Industrial Internet of Things (IIoT).

Conversely, the proposed scheme suffers from a massive pairing operation due to the use of BRPG. Later in 2017, Swapna et al. [43] presented an IBS scheme to secure the communication between end-users and smart homes. The given scheme can provide the security assets of integrity, authentication, and confidentiality to protect the communication between end-users and smart

homes from different types of possible security attacks. Unfortunately, the given scheme was constructed on bilinear pairing.

In 2020, Dharminder et al. [44] presented an IBS scheme for IIoT crowdsourcing under the standard model. In the proposed framework, the user adds a pairing free computation signing, making it efficient for the user. According to the authors, the proposed scheme is efficient in terms of computational and communicational costs. However, the given scheme suffers from high bandwidth usage and heavy computation costs due to the utilization of BRPG.

3 Preliminaries

3.1 Complexity Assumptions

For conducting the security analysis, we performed the following complexity assumptions:

- The $f_{\mathfrak{q}}$ is a finite field with the order $\mathfrak{q}$, where $(\mathfrak{q}) \approx 2^{160}$.
- D is the divisor of the hyperelliptic curve (hec), which is the finite sum of the points; $\mathrm{D} = \sum p_i \, \boldsymbol{\varepsilon} \, \mathrm{hec} \, m_i p_i$, where $m_i \, \varepsilon \, f_{\mathfrak{q}}$.

3.1.1 Hyperelliptic Curve Discrete Logarithm Problem (HDLP)

The following supposition has been made for HDLP.

- Ω belongs to $\{0, 1, 2, 3, 4, 5, \ldots, n-1\}$.
- Probability computation Ω from $\boldsymbol{\mathcal{M}} = \Omega \cdot D$ is negligible.

3.1.2 Hyperelliptic Curve Computational Diffie–Hellman (HCDH)

We also make the subsequent suppositions for *HCDH*.

- The Ω and $\boldsymbol{\mathcal{R}}$ belongs to $\{0, 1, 2, 3, 4, 5, \ldots, \mathrm{n}-1\}$.
- Probability computation of Ω and $\boldsymbol{\mathcal{R}}$ from $\Upsilon = \Omega \cdot \boldsymbol{\mathcal{R}} \cdot \mathrm{D}$ is negligible.

3.2 Threat Model

In our scheme, we examine and consider the Doley–Yao [45,46] threat model. According to Doley–Yao, communication between two or more entities are not trusted and secure, as attackers have full command to expose the contents of the ciphertext and inject false encryption/signature text into the network. As NDN-based healthcare is posed to various types of security threats, this means that the user's sensitive information can be easily forged or delete by any adversaries. To maintain the security and authentication of IoTEH in NDN networks, authentication and secure communication between entities are required.

3.3 Syntax of the Proposed Scheme

The syntax of our newly proposed scheme consists of the following phases:

- Setup Phase: In this phase, the Private Key Generation (PKG) produces its master secret key (ν) and computes the master public key (λ) and the security parameter set ρ.
- Key Extraction Phase: In this phase, PKG makes a public key and private key for the consumer (ς_c, ϱ_c) and producer (ς_p, ϱ_p) on behalf of both consumer and producer identities (ID_c, ID_p). The PKG then send the keys to the consumer and producer by using a secure channel.
- Signcryption Phase: In this phase, the producer generates signcrypted message ($\mathcal{s}$) by taking the consumer and its own identities (ID_c, ID_p), consumer public key ($\varsigma_{c,}$), its private key (ϱ_p) as an input. Then send signcrypted message ($\mathcal{s}$) to the consumer.

- Unsigncryption Phase: In this phase, the consumer unsigncrypt the signcrypted message (δ). For this purpose, the consumer takes its private key (ϱ_c), the public key of producer (ς_p) its own and producer identity (ID_c, ID_p) and signcrypted message (δ) as an input.

4 Proposed NDN Framework for Internet of Things Enabled Healthcare

4.1 Proposed Network Model

In Fig. 2, we have shown the secure network modal for IoTEH in NDN networks. The proposed modal consists of the participants, such as consumer, producer, NDN routers, and PKG. The role of each participant is explained below:

- Role of Consumer: The consumer can be a hospital, patient, doctor, or any IoT device (smartphone, smartwatch, sensor, etc.) that want secure healthcare-related information like (patient records, patient stats, online patient monitoring).
- Role of Producer: Producer can be a hospital, patient, doctor, or any IoT device (smartphone, smartwatch, sensor, etc.) that provide healthcare-related information like (patient records, patient stats, online patient monitoring).
- Role of NDN Routers: The NDN routers is responsible for providing a communication route among producer and consumer for sending healthcare-related information. Every NDN router maintains three types of Tables, such as CS, PIT, and FIB.
- Private Key Generator (PKG): The PKG is a trustable authority that establishes and manage a secure communication between consumer and producer.

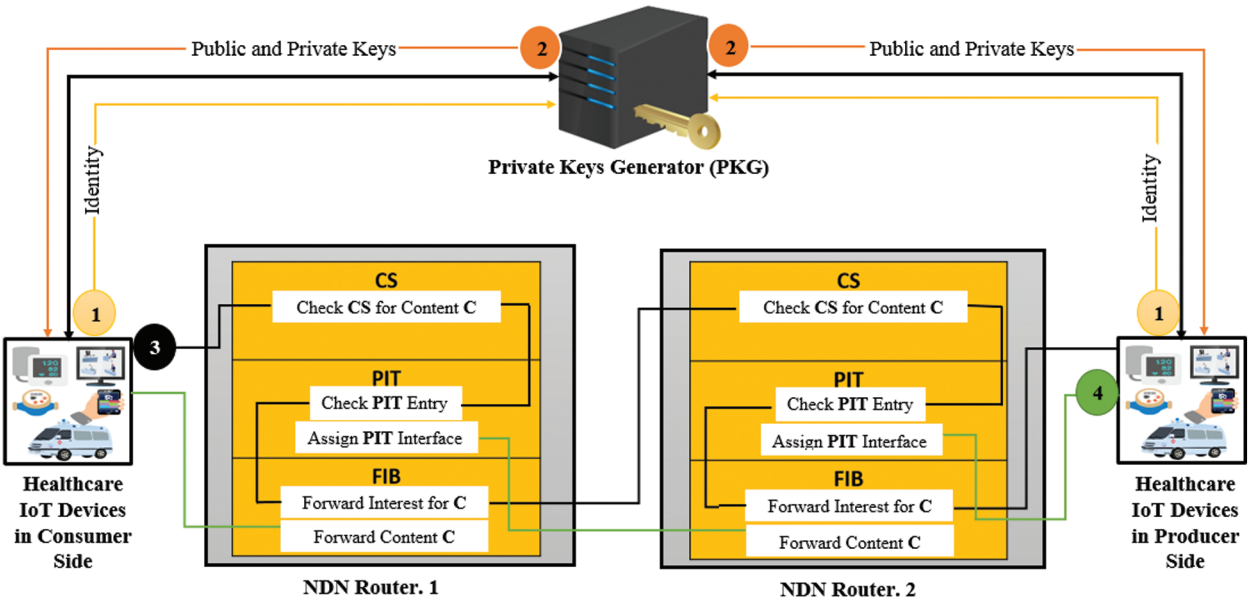

Figure 2: Proposed network modal

In our proposed scheme, before starting a secure communication, the consumer and producer send their identities to PKG. After receiving the identities of both the consumer and producer, the PKG generates the private and public keys for both of them and delivers it using a secure connection.

Suppose a consumer sends an interest for healthcare-related information, the NDN routers will transfer that interest to the producer. The producer will signcrypt the information based on the interest of the consumer. The signcrypted information is then forwarded to the consumer through the NDN routers. The NDN router, after receiving the information from the producer, it will forward the information using the services of FIB by assigning a PIT interface without caching. The process of forwarding without caching will continue until the information is reached to the original consumer. Obviously, the caching of this information will not facilitate any consumer later because the information can only be designcrypted using the private key of the requested consumer.

4.2 Proposed Algorithm

The proposed algorithm consists of the following 4 phases, such as setup phase, key extraction phase, signcryption phase and unsigncryption phase [40].

The notation used in our algorithms is mentioned in Tab. 1.

Table 1: Notation for the proposed algorithm

Name	Notation
Security parameter	μ
Finite field	$\mathbb{F}_n$
Divisor	D
Master secret key	ν
Master public key	λ
Public parameter set	ρ
Identity of users (consumer and producer)	ID_u
Identity of producer & consumer	ID_p, ID_c
Producer private key and public key	ϱ_p, ς_p
Message	m
Fresh nonce	Λ
Random and private number	r, b
Message digest	$\mathcal{Z}$
Signature	∇
Signed message	s
Consumer private key & public key	ϱ_c, ς_c

Setup:

This algorithm is running by the PKG.

- It takes the security parameter (μ)
- Select a hec of the genus ($g = 2$)
- Select a parameter (n) of length 80 bits
- Select a finite field ($\mathbb{F}_n$)
- Select a hec divisor (D) of order n
- Select a master secret key (ν) where $\nu \in (0, 1, 2, 3, 4, \ldots, (n-1))$
- Compute master public key as $\lambda = \nu \cdot \mathrm{D}$

- $\hbar_0$, $\hbar_1$ are one-way collision functions.
- Then publish all the parameter set $\rho = \{n, \mathfrak{f}_n, \hbar_0, \hbar_1, \mu, \lambda, \mathtt{hec}, \mathrm{D}\}$.

Key Extraction:

This algorithm is executed by the PKG that takes the identities of users ($\mathrm{ID_u}$) and compute the public and private keys for the users using the $\mathrm{ID_u}$ as:

- Compute provider private key (ϱ_p): $\varrho_p = \nu \cdot \hbar_0(\mathrm{ID}_p) mod\, n$.
- Compute provider public key (ς_p): $\varsigma_p = \varrho_p \cdot \mathrm{D}$.
- Compute consumer private key (ϱ_c): $\varrho_c = \nu \cdot \hbar_0(\mathrm{ID}_c) mod\, n$.
- Compute consumer public key (ς_c): $\varsigma_c = \varrho_c \cdot \mathrm{D}$.

After that, it sends the public and private key ($\varrho_\mathrm{u}, \varsigma_\mathrm{u}$) by using a secure network.

Signcryption:

This algorithm is run by the producer. It takes the message (m), fresh nonce (Λ), $\mathrm{ID_c}$, $\mathrm{ID_p}$, D, ϱ_p, ς_c as input and then perform the following computations.

- Take a random number $\mathscr{r}\, \boldsymbol{\varepsilon}\, (0, 1, 2, 3, 4, \ldots, (n-1))$.
- Compute private number as: $\mathscr{b} = \mathscr{r} \cdot \mathrm{D}$.
- Compute $\mathfrak{J} = \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c$.
- Compute encrypted text $\mathfrak{w} = \mathfrak{w}_\mathfrak{J}(\mathrm{m})$.
- Compute message-digest $\mathscr{Z} = \hbar_1(\mathrm{m}||\Lambda|\,|\mathrm{ID_p}|\,|\mathrm{ID_c}||\varsigma_c)$.
- Generate signature $\nabla = \mathrm{ID_c} \cdot \mathscr{r} - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b}\, mod\, n$.

Send the signcrypted text $\mathscr{s} = (\mathfrak{w}, \mathscr{Z}, \nabla, \mathscr{b})$ to the consumer.

Unsigncryption:

This algorithm is run on the consumer side. It takes $\mathscr{s} = (\mathfrak{w}, \mathscr{Z}, \nabla, \mathscr{b})$, $\varrho_\mathcal{C}$, ς_p.

- Compute $\mathfrak{J} = \nabla \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varsigma_p \cdot \varrho_\mathcal{C}$.
- Decrypt text $\mathrm{m}' = d_\mathfrak{J}(\mathfrak{w})$.
- Compute $\mathscr{Z}' = \hbar_1(\mathrm{m}'||\Lambda|\,|\mathrm{ID_p}|\,|\mathrm{ID_c}||\varsigma_c)$. If $\mathscr{Z} = \mathscr{Z}'$ valid otherwise invalid.

4.3 Correctness

$$
\begin{aligned}
\mathfrak{J} &= \nabla \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varsigma_p \cdot \varrho_\mathcal{C} \\
&= (\mathrm{ID_c} \cdot \mathscr{r} - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b}) \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varsigma_p \cdot \varrho_\mathcal{C} \\
&= \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b} \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varsigma_p \cdot \varrho_\mathcal{C} \\
&= \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b}.\varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varrho_p \cdot \mathrm{D}\varrho_\rfloor \\
&= \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b} \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathscr{Z} \cdot \mathscr{b} \cdot \varrho_p \cdot \varsigma_c \\
&= \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c = \mathfrak{J}
\end{aligned}
$$

5 Security Analysis

In this section, we discuss the proposed scheme to maintain the basic security assets, including confidentiality, authentication, unforgeability, integrity and Non-Repudiation. Each of the mentioned features is briefly analyzed in the following sections.

5.1 *Confidentiality*

An IBS scheme is supposed to succeed in the property of confidentiality if no adversary can compromise the encryption key of the sender.

Proof: The proposed plan ensures the property of confidentiality. If an intruder wants to steal the original content or secret key of the message, he/she must have information about the key in advance as $\mathfrak{J} = \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c$. To determine $\mathfrak{J}$, the intruder needs to compute $\mathscr{r}$ from $\mathscr{b} = \mathscr{r} \cdot \mathrm{D}$, which infeasible due to the properties of HDLP.

5.2 *Authentication*

An IBS is considered to achieve the security asset of authentication if the consumer can verify the source of the message.

Proof: The consumer can use his public key ς_c and signature ∇ to verify the authenticity of the producer. As the message is signed with the private key ϱ_p of the producer. In our scheme, the consumer can authenticate the identity of the producer.

5.3 *Integrity*

An IBS scheme is likely to achieve the security asset of integrity if no adversary can generate the same hash value for two different sizes/nature messages.

Proof: The provider takes the "hash value" "$\mathscr{Z} = \hbar_1(\mathrm{m}||\Lambda|\left|\mathrm{ID_p}\right||\mathrm{ID_c}||\varsigma_c)$" of the message before sending the message. If the attacker changes the ciphertext of the message, then the consumer can perform the following operation for verification of the ciphertext. The consumer take $\mathrm{m}' = d_{\mathfrak{J}}(\mathfrak{w})$ and compute the $Z' = \hbar_1(\mathrm{m}||\Lambda|\left|\mathrm{ID_p}\right||\mathrm{ID_c}||\varsigma_c)$. After that, the consumer compares the $\mathscr{Z} = Z'$ if they are equal, then the integrity of the message holds; otherwise, the message has been altered.

5.4 *Unforgeability*

An IBS scheme is considered to achieve the security assets of unforgeability if there exists no intruder which can compromise the private key of the producer.

Proof: In our scheme, if an intruder tries to generate a valid signature, he/she must need to calculate ∇ from $(\mathrm{ID_c} \cdot \mathscr{r} - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b})$ and to do so, the attacker needs to find $\mathscr{r}$ from the $\mathscr{b} = \mathscr{r} \cdot \mathrm{D}$. Further, the attacker also needs to find ϱ_p from $\varsigma_p = \varrho_p \cdot \mathrm{D}$. So, it is computationally infeasible for the attacker to solve a two-time HDLP.

5.5 *Non-Repudiation*

An IBS scheme is supposed to succeed in the security service of non-repudiation if a sender cannot repudiate his signcrypted text.

Proof: As the message is signed with the private key ϱ_p of the producer. In our scheme, the consumer can authenticate the provider identity $\mathrm{ID_p}$. So, the provider later can't deny from his signature.

6 Cost Analysis

In this section, we will analyze the performance of our newly proposed scheme in relation to computation cost and communication cost. First, we compared our scheme with four related schemes of Yosef et al. [43], Nayak [40], Karate et al. [42] and Dharminder et al. [44], to show the computational and communicational efficiency. The computational efficiency is determined by

the computational cost of the algorithm, and the communication efficiency is determined by the length of the ciphertext. The symbol (P) indicates the pairing operation, the symbol (Σ) represents an exponential operation, and the symbol ($\mathcal{P}$BM) indicates a pairing based point multiplication operation, the symbol (**SBPM**) represent scalar point multiplication of elliptic curve and the symbol (HE**D**M) represent the hyperelliptic curve divisor multiplication. Here, we ignore the cost of other operations like hashing, addition, and subtraction because they take a much shorter time than the other operations mentioned above.

According to [27], the operation cost and their timing are listed in Tab. 3 below. The hardware and software specifications used for the simulation results are Intel Core i74510UCPU, Processor 2.0 and 8 GB RAM, Operating system of Windows 7, and C Library (MIRACL) [32]. Similarly, the HE**D**M will consume 0.48 ms [15,47].

The symbols represent the length of the element. For example, $|\mathrm{G}| = 1024$ bits denote the length of the element in the group, $|\mathrm{m}| = 512$ bits represent the length of the message space. Similarly, $|q| = 160$ bits and $|n| = 80$ bits represent the length of elements in the elliptic curve and hyperelliptic curve cryptosystem, as shown in Tab. 2. Our scheme has a lower communication overhead cost as compared to Yosef et al. [43], Nayak [40], Karate et al. [42], and Dharminder et al. [44].

Table 2: Comparative analysis based on major operations

Schemes	[43]	[40]	[42]	[44]	Proposed
Signcryption	$3\mathcal{P}\mathrm{BM} + 1P$	8 SBPM	$4\mathcal{P}\mathrm{BM} + 4\Sigma$	3Σ	6HEDM
Unsigncryption	$3P$	5 SBPM	$2P + 2\mathcal{P}\mathrm{BM} + 2\Sigma$	$2P + 1\Sigma$	5HEDM
Total	$3\mathcal{P}\mathrm{BM} + 4P$	13 SBPM	$2P + 6\mathcal{P}\mathrm{BM} + 6\Sigma$	$2P + 4\Sigma$	11HEDM

Table 3: Operations cost in milliseconds

Operation	P	Σ	$\mathcal{P}$BM	SBPM	HEDM
Cost in millisecond	14.31	1.25	4.32	0.97	0.48

In accordance, Tabs. 4 and 6 show a comparative illustration of our proposed work with Yosef et al. [43], Nayak [40], Karate et al. [42], and Dharminder et al. [44], in term of computation and communication overheads. According to our comparative analysis, our scheme shows efficiency in terms of computation and communication overheads, as shown in Figs. 3 and 4. Furthermore, an exact computation and communication cost reduction are shown in Tabs. 5 and 7.

Table 4: Comparative analysis based in milliseconds

Schemes	[43]	[40]	[42]	[44]	Proposed
Signcryption	27.86	7.76	22.28	3.75	2.88
Unsigncryption	44.7	4.85	40.94	29.87	2.4
Total	72.56	12.61	63.22	33.64	5.28

Table 5: Percentage computation cost reduction

Schemes	[43]	[40]	[42]	[44]
Total computation cost of ($\boldsymbol{\alpha}$)	72.56	12.61	63.22	33.64
Total computation cost of the proposed ($\boldsymbol{\beta}$)	5.28	5.28	5.28	5.28
Cost reduction in % ($\boldsymbol{\gamma}$)	92.72	58.12	91.64	84.30

Improvement in percentage (γ): $\left(\frac{\alpha-\beta}{\beta}\right)*100$

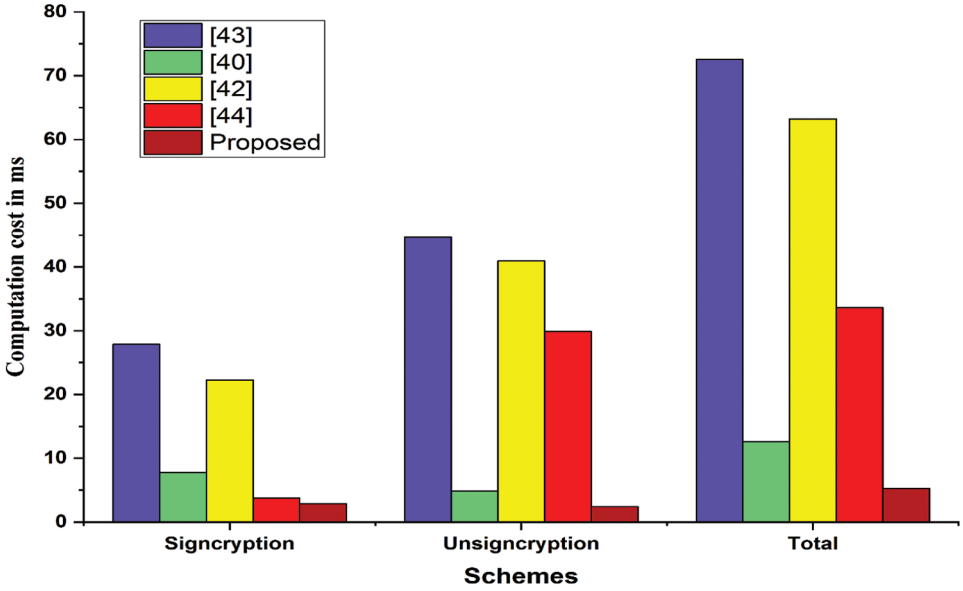

Figure 3: Computation cost analysis in terms of milliseconds

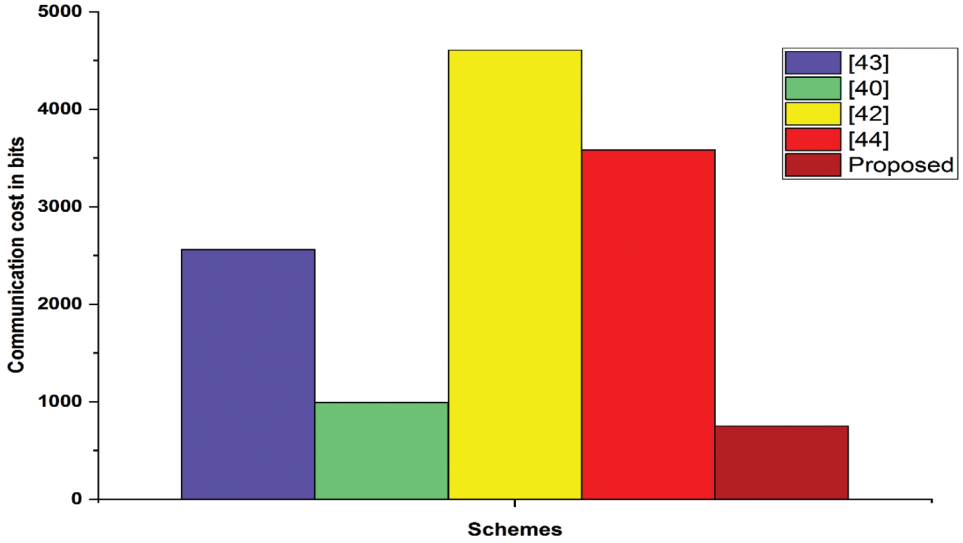

Figure 4: Communication cost analysis in terms of bits

Table 6: Comparative analysis in ciphertext in bits

Schemes	[43]	[40]	[42]	[44]	Proposed
Communication cost	$2\|G\|+\|m\|$	$3\|q\|+\|m\|$	$4\|G\|+\|m\|$	$3\|G\|+\|m\|$	$3\|n\|+\|m\|$
Ciphertext size	2560	992	4608	3584	752

Table 7: Percentage communication cost reduction

Schemes	[43]	[40]	[42]	[44]
Total communication cost (α)	2560	992	4608	3584
Total communication cost (β)	752	752	752	752
Cost reduction in % (γ)	70.62	24.19	83.68	79.01

Improvement in percentage (γ): $\left(\frac{\alpha-\beta}{\beta}\right)*100$

7 Deployment of Proposed Scheme

In this section, we deployed our scheme on IoTEH in the NDN network. We consider several IoT devices that can sense and share healthcare-related information among the hospital, patient, doctor, and IoT devices through the NDN router. The information can be shared from the city to the city as well as from country to country. Moreover, the devices in healthcare are connected based on the NDN policy.

Here, every NDN router maintains three kinds of data structures, such as Pending Interest Table (PIT), Forwarding Information Base (FIB), and Content Store (CS) [33]. The data attainment process begins by sending an Interest with a particular name from the client's side. The routers rely on FIBs for transferring the interest to a potential provider and generate a PIT entry list on each router to establish an opposite path. Based on the opposite path, the provider of any interest returns the data to the client with the target data. The CS stores the targeted data are passing through it for future use [48].

Assume consumers require healthcare-related information from the producer, and the communication includes the participants such as client, private key generator (PKG), NDN routers, and provider. The consumers are those who need the information. The providers are those who distribute the information to the consumers, and the PKG is a trusted authority that is responsible for establishing secure communication between the consumer and producer. Communication among consumers and producers is discussed below.

Registration Phase: In this stage, the consumer and producer registered themselves with the PKG by providing their Identities (ID_c, ID_p) to PKG. The PKG gets their Identities $(\mathcal{I}\lceil_u)$, and generate consumer private key (ϱ_c): $\varrho_c = \nu \cdot \hbar_0(ID_c)\ mod\ n$, consumer public key (ς_c): $\varsigma_c = \varrho_c \cdot D$, private producer key (ϱ_p): $\varrho_p = \nu \cdot \hbar_0(ID_p)\ mod\ n$ and producer public key (ς_p): $\varsigma_p = \varrho_p \cdot D$ by using their identity (ID_c, ID_p) Then the PKG sends the $(\varrho_c\ , \varsigma_c, \varrho_p, \varsigma_p)$ to consumer and producer, as shown in Fig. 5.

Signcryption Phase: When the consumer shows interest in information m, upon receiving interest, the producer will signcrypt m. For this purpose, the producer takes information (m), fresh nonce (Λ), $ID_c, ID_p\ \varsigma_c$, D, ϱ_p as input. First, take a random number $r\ \varepsilon\ (0,1,2,3,4\ldots(n-1))$, compute a private number $(\mathcal{b})$ where $\mathcal{b} = r \cdot D$. After that, the producer computes an encryption

key ($\mathfrak{J}$) where $\mathfrak{J} = \mathrm{ID_c} \cdot \mathscr{r} \cdot \varsigma_c$. Then perform the encryption process on information ($\mathfrak{w}$) where $\mathfrak{w} = \mathfrak{w}_{\mathfrak{J}}(\mathrm{m})$. The producer then computes information digest ($\mathscr{Z}$) where $\mathscr{Z} = \mathscr{h}_1(\mathrm{m}||\Lambda|\,|\mathrm{ID_p}|\,|\mathrm{ID_c}||\varsigma_c)$. After that, the producer generates signature (∇) where $\nabla = \mathrm{ID_c} \cdot \mathscr{r} - \mathrm{ID_p} \cdot \mathscr{Z} \cdot \varrho_p \cdot \mathscr{b}\ mod\ \mathscr{n}$. Finally, producers generate the signcrypted information ($\mathscr{s}$) where $\mathscr{s} = (\mathfrak{w}, \mathscr{Z}, \nabla, \mathscr{b})$ and send it to the consumer, as shown in Fig. 6.

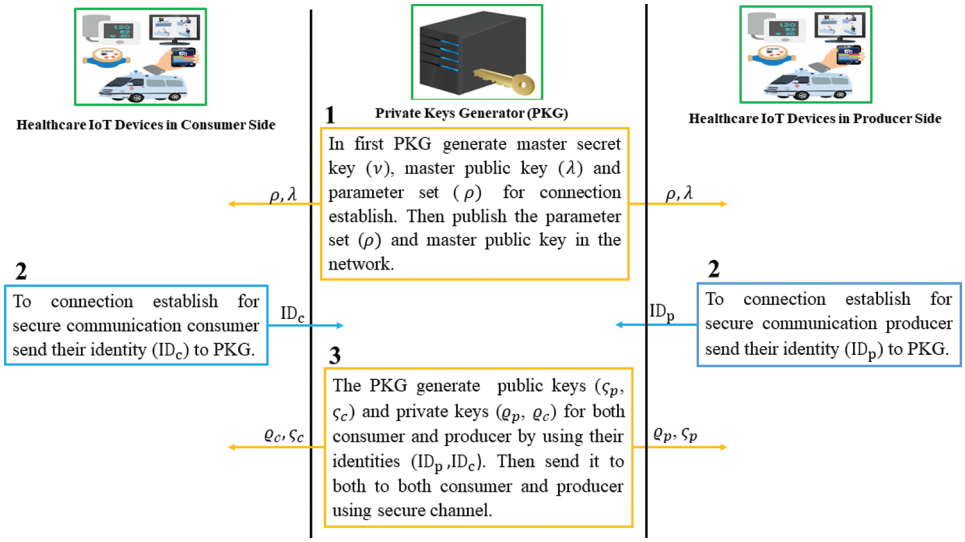

Figure 5: Registration of consumer and producer with PKG

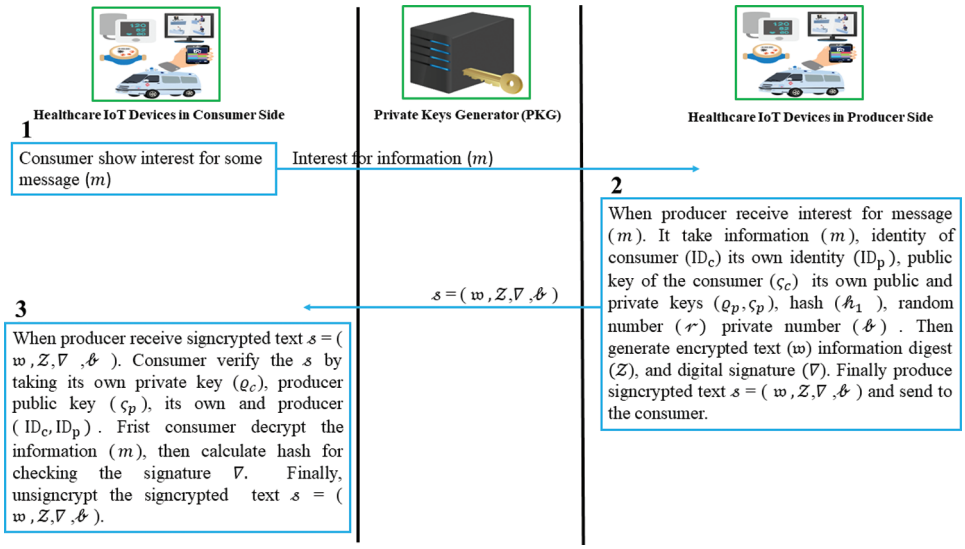

Figure 6: Communication between consumer and producer

Unsigncryption Phase: After receiving the signcrypted information $\mathscr{s} = (\mathfrak{w}, \mathscr{Z}, \nabla, \mathscr{b})$, the consumer unsigncrypt the $\mathscr{s}$. For unsigncryption, the consumer takes $\mathscr{s} = (\mathfrak{w}, \mathscr{Z}, \nabla, \mathscr{b})$, $\mathrm{ID_c}, \mathrm{ID_p}\varrho_C$, and ς_p as input. First, the consumer computes the decryption key ($\mathfrak{J}$) from

$\mathfrak{J} = \nabla \cdot \varsigma_c + \mathrm{ID}_p \cdot \mathcal{Z} \cdot \mathscr{b} \cdot \varsigma_p \cdot \varrho_{\mathcal{C}}$. Then decrypt the information (m') where $\mathrm{m}' = d_{\mathfrak{J}}(\mathfrak{w})$. Finally, compute information digest $(\mathcal{Z}')$ where $\mathcal{Z}' = \hbar_1(\mathrm{m}'||\Lambda|\left|\mathrm{ID_p}\right||\mathrm{ID_c}||\varsigma_c)$. If $\mathcal{Z} = \mathcal{Z}'$ valid otherwise invalid, as shown in Fig. 6.

8 Conclusion

In this paper, we proposed a secure NDN framework for the Internet of Things Enabled Healthcare (IoTEH) using a lightweight Identity-Based Signcryption (IBS) cryptography to secure the information of IoT enabled healthcare in NDN infrastructure. To minimize the cost consumption, we used a Hyperelliptic Curve Cryptosystem (HCC) which provides the corresponding level of security as compared to bilinear pairing and Elliptic Curve Cryptosystem (ECC). To show the efficiency of our newly proposed scheme we compared the proposed scheme with recently presented identity-based signcryption schemes in terms of computation and communication overheads. The final results show the superiority of our scheme in terms of computation and communication costs. For further security, we simulate the security of our scheme using Automated Validation of Internet Security Protocols and Applications (AVISPA). Finally, we deployed our proposed scheme on NDN enabled healthcare.

Acknowledgement: The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

Funding Statement: The authors received no financial support for the research, authorship, and/or publication of this article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Khan, J. P. Li, B. Ahamad, S. Parveen, A. U. Haq *et al.,* "SMSH: Secure surveillance mechanism on smart healthcare iot system with probabilistic image encryption," *IEEE Access*, vol. 8, pp. 15747–15767, 2020.

[2] X. Guo, H. Lin, Y. Wu and M. Peng, "A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems," *Future Generation Computing Systems*, vol. 3, no. 8, pp. 1–5, 2020.

[3] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computing Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] A. S. M. S. Arefin, K. M. T. Nahiyan and M. Rabbani, "The basics of healthcare IoT: Data acquisition, medical devices, instrumentations and measurements," in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*, Cham, Switzerland: Springer, pp. 1–37, 2020.

[5] E. M. A. Nassar, A. M. Iliyasu, P. M. El Kafrawy, O. Y. Song, A. K. Bashir *et al.,* "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[6] G. Srivastava, R. M. Parizi and A. Dehghantanha, "The future of blockchain technology in healthcare Internet of Things security," in *Blockchain Cybersecurity, Trust and Privacy*, Cham, Switzerland: Springer, pp. 161–184, 2020.

[7] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. Thornton *et al.,* "Named Data Networking (NDN) project, relatório técnico NDN-0001, xerox palo alto res," *Center-PARC*, vol. 157, pp. 158, 2010.

[8] K. Ahed, M. Benamar and R. E. Ouazzani, "Content delivery in named data networking based Internet of Things," in *2019 15th Int. Wireless Communications & Mobile Computing Conf.*, Tangier, Morocco, pp. 1397–1402, 2019.

[9] B. Nour, H. Ibn-Khedher, H. Moungla, H. Afifi, F. Li *et al.,* "Internet of Things mobility over information-centric/named-data networking," *IEEE Internet Computing*, vol. 24, no. 1, pp. 14–24, 2019.
[10] D. Saxena, V. Raychoudhury and N. SriMahathi, "SmartHealth-NDNoT: Named data network of things for healthcare services," in *Proc. of the 2015 Workshop on Pervasive Wireless Healthcare*, Hangzhou, China, MobileHealth 15, pp. 45–50, 2015.
[11] 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.
[12] X. Wang and S. Cai, "Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud," *Future Generation Computing Systems*, vol. 112, pp. 320–329, 2020.
[13] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons *et al.,* "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustainable Energy Grids and Networks*, vol. 15, pp. 14–25, 2018.
[14] M. Kumar, H. K. Verma and G. Sikka, "A secure lightweight signature based authentication for Cloud-IoT crowdsensing environments," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 4, pp. e3292, 2019.
[15] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari *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.
[16] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption)," in *Annual Int. Cryptology Conf.*, Santa Barbara, California, USA, pp. 165–179, 1997.
[17] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things," *Electronics*, vol. 8, no. 10, pp. 1171, 2019.
[18] L. Pang, M. Kou, M. Wei and H. Li, "Anonymous certificateless multi-receiver signcryption scheme without secure channel," *IEEE Access*, vol. 7, pp. 84091–84106, 2019.
[19] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi *et al.,* "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[20] W. Cui, Z. Jia, M. Hu and L. Wang, "A new signcryption scheme based on elliptic curves," in *Int. Conf. on Security and Privacy in New Computing Environments*, Tianjin, China, pp. 538–544, 2019.
[21] A. Shamir, *Identity-Based Cryptosystems and Signature System*. Santa Barbara, CA, USA: SpringerLink, pp. 47–53, 1985.
[22] Y. Huang and J. Yang, "A novel identity-based signcryption scheme in the standard model," *Information*, vol. 8, no. 2, pp. 58, 2017.
[23] J. Malone-Lee, "Identity-based signcryption," *International Association for Cryptologic Research (IACR)*, vol. 2002, pp. 98, 2002.
[24] M. Suárez-Albela, P. Fraga-Lamas and T. M. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, pp. 3868, 2018.
[25] M. Yu, J. Zhang, J. Wang, J. Gao, T. Xu *et al.,* "Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, 2018.
[26] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry (Basel)*, vol. 10, no. 8, pp. 352, 2018.
[27] C. Zhou, Z. Zhao, W. Zhou and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, no. 3, pp. 1–17, 2017.
[28] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu *et al.,* "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[29] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, no. 6, pp. 108, 2018.

[30] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *International Journal of Advanced Studies and Science Research*, vol. 3, no. 8, pp. 1–5, 2018.

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

[32] A. U. Rahman, I. Ullah, M. Naeem, R. Anwar, H. Khattak *et al.,* "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve," *International Journal of Advanced Computer Science & Applications*, vol. 9, no. 5, pp. 160–167, 2018.

[33] M. Amadeo, G. Ruggeri, C. Campolo and A. Molinaro, "IoT services allocation at the edge via named data networking: From optimal bounds to practical design," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 661–674, 2019.

[34] Z. Rezaeifar, J. Wang, H. Oh, S. B. Lee and J. Hur, "A reliable adaptive forwarding approach in named data networking," *Future Generation Computing Systems*, vol. 96, pp. 538–551, 2019.

[35] B. Nour, K. Sharif, F. Li, H. Moungla, A. E. Kamal *et al.,* "NCP: A near ICN cache placement scheme for IoT-based traffic class," in *2018 IEEE Global Communications Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirate, pp. 1–6, 2018.

[36] K. K. R. Choo, J. Nam and D. Won, "A mechanical approach to derive identity-based protocols from diffie-hellman-based protocols," *Information Sciences*, vol. 281, pp. 182–200, 2014.

[37] S. Duan and Z. Cao, "Efficient and provably secure multi-receiver identity-based signcryption," in *Australasian Conf. on Information Security and Privacy*, Melbourne, VIC, Australia, pp. 195–206, 2006.

[38] F. Li, X. Xin and Y. Hu, "Indentity-based broadcast signcryption," *Computer Standards & Interfaces*, vol. 30, no. 1–2, pp. 89–94, 2008.

[39] B. Libert and J. J. Quisquater, "A new identity based signcryption scheme from pairings," in *Proc. 2003 IEEE Information Theory Workshop (Cat. No. 03EX674)*, Paris, France, pp. 155–158, 2003.

[40] B. Nayak, "A secure ID-based signcryption scheme based on elliptic curve cryptography," *International Journal of Computational Intelligence Studies*, vol. 6, no. 2–3, pp. 150–156, 2017.

[41] S. Reddi and S. Borra, "Identity-based signcryption groupkey agreement protocol using bilinear pairing," *Informatica*, vol. 41, no. 1, pp. 31–37, 2017.

[42] A. Karati, S. K. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar *et al.,* "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet of Things*, vol. 5, no. 4, pp. 2904–2914, 2017.

[43] G. Swapna and P. V. Reddy, "Efficient identity based aggregate signcryption scheme using bilinear pairings over elliptic curves," *Journal of Physics: Conference Series*, vol. 1344, no. 1, 12010, 2019.

[44] D. Dharminder, D. Mishra, J. J. P. C. Rodrigues, R. de AL Rabelo and K. Saleem, "PSSCC: Provably secure communication framework for crowdsourced industrial Internet of Things environments," *Software: Practice and Experience*, vol. 14, no. 6, pp. 1, 2020.

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

[46] Y. Ashibani and Q. H. Mahmoud, "An efficient and secure scheme for smart home communication using identity-based signcryption," in *2017 IEEE 36th Int. Performance Computing and Communications Conference*, San Diego, CA, pp. 1–7, 2017.

[47] S. S. Ullah, H. Khattak, M. A. Khan, M. Adnan, S. Hussain *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.

[48] X. Hu, J. Gong, G. Cheng, G. Zhang and C. Fan, "Mitigating content poisoning with name-key based forwarding and multipath forwarding based inband probe for energy management in smart cities," *IEEE Access*, vol. 6, pp. 39692–39704, 2018.

[49] M. Abadi, B. Blanchet and H. Comon-Lundh, "Models and proofs of protocol security: A progress report," in *Int. Con. on Computer Aided Verification*, Grenoble, France, pp. 35–49, 2009.
[50] S. Malani, J. Srinivas, A. K. Das, K. Srinathan and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet of Things*, vol. 6, no. 6, pp. 9762–9773, 2019.
[51] C. J. F. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Int. Conf. on Computer Aided Verification*, Princeton, NJ, USA, pp. 414–418, 2008.
[52] I. Ullah, N. U. Amin, M. Naeem, H. Khattak, S. J. Khattak *et al.,* "A novel provable secured signcryption scheme: A hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, pp. 686, 2019.

Appendix A. Simulation and Validation

There are several formal security verification tools, such as ProVerif [49], AVISPA (Internet Security Protocol and Automatic Verification of Application) [50], and Scyther [51]. In our proposed work, we use AVISPA as it is popular in the security community. Specifically, we encode our proposed scheme using the "role-oriented language" of High-Level Protocol Specification Language (HLPSL) [50], which has a variety of basic roles (the roles for consumer, the role for the producer). Defined the proposed scheme two mandatory roles (session, goal and environment). The HLPSL2IF Translator helps to convert the HLPSL code to "Intermediate Format (IF)," and the IF is then sent to one of AVISPA's four available backends: "On-the-Fly Model-Checker (OFMC)," "Automatic Approval for Analysis of Tree Automata, Security Protocol (TA4SP)," "Structure Logic Based Attack Search (CL-AtSe)" and "SAT-based Model-Checker (SATMC)" [52]. The basic top-down illustration of AVISPA is shown in Fig. 7.

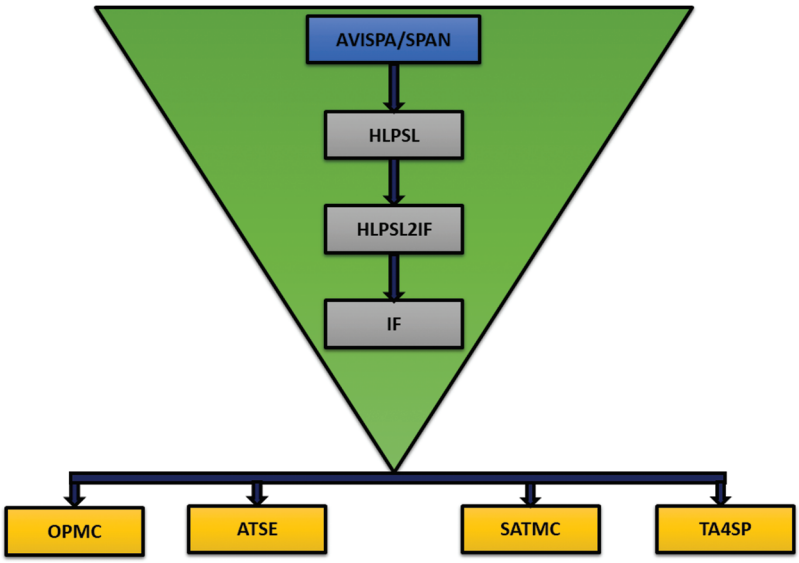

Figure 7: Top-down illustration of AVISPA

A.1 Simulation and Validation Results

Here we validate our scheme according to the backend tools of AVISPA tool such as ATSE and OFMC.

A.1.1 Results of OFMC Protocol

In Fig. 8 below, we provide the simulation result of the proposed scheme under the back-end checkers of AVISPA called OFMC. The simulation result under OFMC shows that our scheme is perfectly safe.

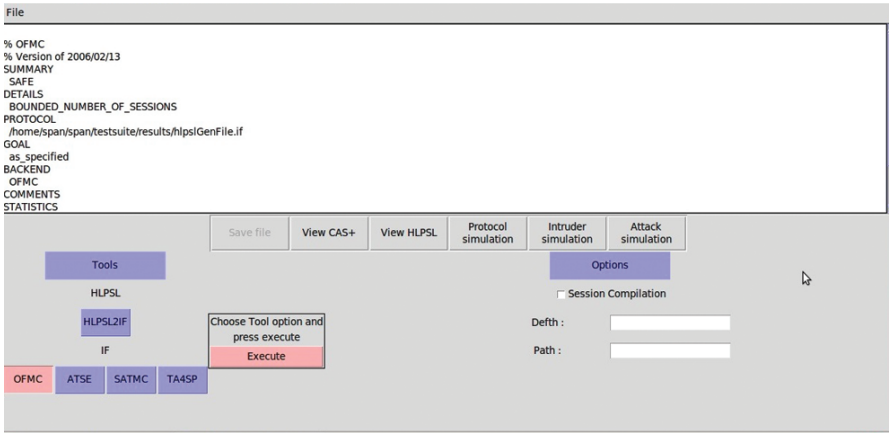

Figure 8: OFMC protocol result of our scheme

A.1.2 Results of ATSE Protocol

In Fig. 9, we also provide the simulation result of our scheme under the function of the another AVISPA back end checker called CL-AtSe. The result shows that the given scheme is safe under CL-AtSe. The CL-AtSe supports a type-imperfection discovery that is responsible for the associativity message concatenation.

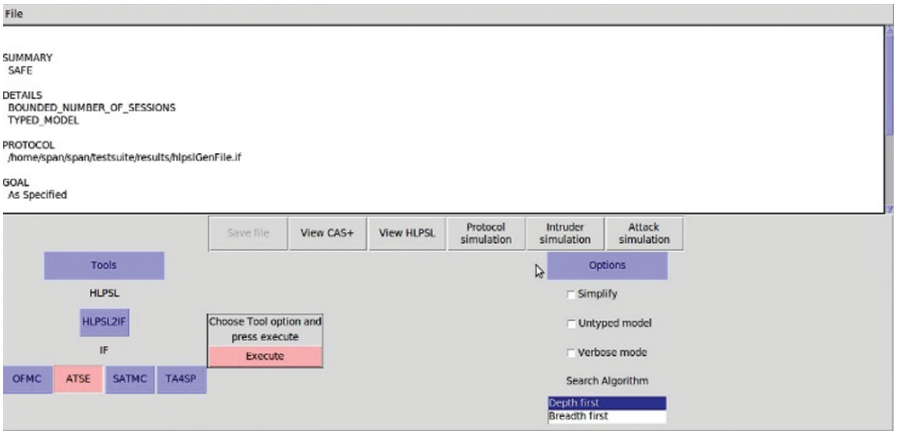

Figure 9: ATSE protocol result of our scheme