Computers, Materials & Continua
DOI: 10.32604/cmc.2022.023769
Article

Tech Science Press

A Secure and Efficient Signature Scheme for IoT in Healthcare

Latika Kakkar[1], Deepali Gupta[1], Sarvesh Tanwar[2], Sapna Saxena[3], Khalid Alsubhi[4], Divya Anand[5], Irene Delgado Noya[6,7] and Nitin Goyal[1,*]

[1]Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, 140401, India
[2]AIIT, Amity University, Noida, 201313, India
[3]Chitkara School of Engineering & Technology, Chitkara University, HP, 174103, India
[4]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 37848, Saudi Arabia
[5]Lovely Professional University, Jalandhar, Punjab, 144411, India
[6]Universidad Europea Del Atlántico, C/ Isabel Torres 21, 39011, Santander, Spain
[7]Universidad Internacional Iberoamericana, Campeche, C.P., 24560, Mexico
*Corresponding Author: Nitin Goyal. Email: dr.nitingoyal30@gmail.com
Received: 21 September 2021; Accepted: 25 October 2021

Abstract: To provide faster access to the treatment of patients, healthcare system can be integrated with Internet of Things to provide prior and timely health services to the patient. There is a huge limitation in the sensing layer as the IoT devices here have low computational power, limited storage and less battery life. So, this huge amount of data needs to be stored on the cloud. The information and the data sensed by these devices is made accessible on the internet from where medical staff, doctors, relatives and family members can access this information. This helps in improving the treatment as well as getting faster medical assistance, tracking of routine activities and health focus of elderly people on frequent basis. However, the data transmission from IoT devices to the cloud faces many security challenges and is vulnerable to different security and privacy threats during the transmission path. The purpose of this research is to design a Certificateless Secured Signature Scheme that will provide a magnificent amount of security during the transmission of data. Certificateless signature, that removes the intricate certificate management and key escrow problem, is one of the practical methods to provide data integrity and identity authentication for the IoT. Experimental result shows that the proposed scheme performs better than the existing certificateless signature schemes in terms of computational cost, encryption and decryption time. This scheme is the best combination of high security and cost efficiency and is further suitable for the resource constrained IoT environment.

Keywords: CSSS; digital signature; ECC; IoT; security; signcryption; smart healthcare system

1 Introduction

The Internet has given birth to a new technology named Internet of things (IoT). IoT is the collection of smart devices that are connected to each other that are able to collect and share the data among each other. These smart devices have the capability of sensing, storing and processing the data and there is no need for any human interaction for doing this task [1]. The base idea about IoT is to automatically sense, collect, compile and complete the tasks that are being utilized by people in their day to day lives. It is basically used for collecting and processing the data for human assistance and without human intervention [2,3]. However, IoT devices have limited storage capacities, limited computational power and minimized battery life. Hence the tremendous data fetched from IoT devices needs some good storage medium where data can be kept securely. Cloud proves to be a secure medium for data storage and processing [4–6]. This mapping of the real world and virtual world is necessary for storing and maintaining a large capacity of data [7]. The data transferred to cloud for further storage, security and processing of data is then used to design various applications of IoT that includes smart home, smart city, smart grid, smart healthcare, smart transportation etc. [8–11]. The data generated by these smart applications are sensitive and thus this data needs to be protected and safeguard from any kind of illegal attacks and tempering. The sensed data from IoT devices is vulnerable to various attacks such as routing attacks, DoS attacks, cloning attacks, Man in the Middle attacks, eavesdropping attacks [12].

To sustain the legitimacy and integrity of the data from the sensor devices, a secured medium needs to be established between sensors and cloud storage [13]. Security and privacy of sensed data are imperative concerns in the development of IoT [14,15]. Therefore, the proposed study aims to design a secured scheme in this IoT-Cloud environment that provides an efficient authentication procedure for secure communication. The proposed work will be focusing on the data of healthcare application of IoT [16]. Large amounts of patient data accessed from the sensor devices known as wireless body area network is collected and implanted on the security mechanism in this research. A smart healthcare system without the security parameter will give attackers a privilege to access the data and thus hamper the integrity, confidentiality and authenticity of data [17,18].

Healthcare is one the smart application of IoT where IoT enhances the quality of services and provides cost-effective solutions. The wearable medical sensors are embedded with the health-related equipment that is used for patients' health monitoring. Different health parameters are monitored by these healthcare sensors that can be body temperature, blood pressure, sugar level etc. [19,20]. Patient body activities and various health parameters are analyzed and collected from the Wireless Body Area Network (WBNs) [21,22]. The information and the data sensed by these devices is made accessible on the internet from where medical staff, doctors, relatives and family members can access this information. This helps in improving the treatment as well as getting faster medical assistance, tracking of routine activities and health focus of elderly people on a frequent basis [23–27]. As patients do not have to wait for doctors to reach their place or vice versa, patients can be treated without a delay [28–30]. High quality healthcare is provided by constant monitoring and speedup response for chronically ill people.

The data from these smart healthcare devices is sensitive and has the requirement of being protected from any unauthorized access, tempering and various types of security attacks. Fig. 1 explains a general scenario where sensors are able to continuously monitor the complete health related information about the patient and this information is stored in the cloud server. From the cloud only authentic users like doctor, family members can access their medical reports for diagnosis and treatment.

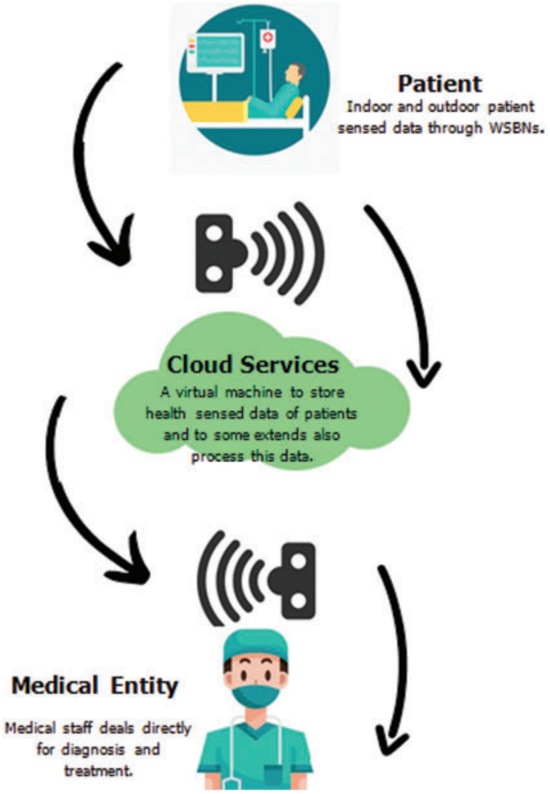
Patient
Indoor and outdoor patient sensed data through WSBNs.
Cloud Services
A virtual machine to store health sensed data of patients and to some extends also process this data.
Medical Entity
Medical staff deals directly for diagnosis and treatment.

Figure 1: Smart healthcare

The authors are motivated by above-mentioned limitations and thus proposed a novel Certificateless Secured Signature Scheme (CSSS) that does not undergo problems of extra consumption of bandwidth and the issues of secret key distribution. The salient features specifying the research contributions are:

1. Authors proposed a novel CSSS that performs combined digital signature and encryption with efficient key generation technique for IoT in Healthcare.
2. A comparative analysis of computation cost is performed with the existing schemes and the experimental results show that the proposed scheme is more efficient than the existing state of art.
3. By using the proposed scheme, various security parameters such as confidentiality, authentication, integrity, unforgeability, forward secrecy and non-repudiation are achieved.

2 Related Works

An overview of IoT, its applications and the various challenges encountered in different fields were discussed [1–3]. IoT technology and the security problems that arise when IoT devices are connected to the internet were widened by the researcher [4]. The researcher focuses on the integration of two foremost technologies i.e., IoT and cloud and also discusses advantages and disadvantages of their integration [5,6]. The authors also focused the attention on the security issues that arise as a result of their amalgamation. IoT works on different types of architectures and security issues arises in various layers of these architectures. Security and privacy issues in different layers were discussed [7]. A survey was made on cloud computing in which its various main concepts were discussed. The motive of the paper was to focus research areas based on different design challenges of cloud computing [8]. Issues and difficulties arise when IoT is used with cloud services. Challenges and benefits of amalgamation of these two techniques were focused upon. The paper defines that cloud computing improves the overall functionality of IoT [9,10]. The author focuses on the hardware's that are utilized in IoT layers such as sensors, cloud, processors etc. Also, various applications of IoT were described here [11]. A distributed algorithm was implemented on the IoT devices that perform resources allocation [12]. The author focuses on the concepts of cyber-physical systems and Industry 4.0.

A framework was designed that focuses on analysis that can compute Industrial IoT (IIoT) devices and the various security threats [13]. Various security attacks on IoT were analyzed, classified and their impact was examined [14]. A heterogeneous ring signcryption scheme was proposed that was capable of providing a trusted and authentic IoT to server communication. The proposed scheme achieves various security parameters [15]. Existing threats and vulnerabilities in IoT were focused and the preventive measures were analyzed [16]. A risk based security model was proposed that can withstand various threats and vulnerabilities and is capable of evaluating various layers of IoT against various security risks [17]. A multi-valued and ambiguous scheme is designed that works in wireless body area network in cloud based environment. The scheme achieved confidentiality [19]. A scheme was proposed that is capable of transmitting the data from sensor effectively [20]. Patient privacy and data security was focused in sensor to cloud environment [21]. IoT and its research challenges were described in [22–24]. Wireless body area network (WBAN) has witnessed significant attentions in the healthcare domain using biomedical sensor-based monitoring of heterogeneous nature of vital signs of a patient's body [25–27]. WBAN are used in healthcare applications of IoT where real time monitoring of health related data of patients like their body temperature, Sugar level, Blood pressure is done. This information is directly sent to doctors and thus helps in the early diagnosis [28]. A novel architecture was designed that was based on cloud and implemented for WSN for providing security in medical data fetched using WSN [29]. An ISA based scheme was proposed in the healthcare domain and data was stored onto the cloud [30].

A novel architecture was proposed that can accumulate and admit huge amounts of medical sensor network data [31,32]. An intelligent system based on IoT was designed that was capable of detecting allergies and effects of drugs on the human body [33,34]. An approach was introduced where patients and doctors can connect globally and thus helps in early diagnosis [35]. A framework was implemented that was based on a signature scheme where there is no need of managing the certificates and have no key escrow issues. This scheme is known as certificateless signature scheme [36]. A certificateless signature based scheme was implemented that worked efficiently than the existing schemes [37]. A certificateless public key signature scheme was proposed and implemented that provides high level security as it could withstand various attacks [38]. Certificateless signature scheme in the IoT environment was implemented that provides efficiency and less computational overheads [39,40]. ECC and RSA were compared on the basis of various parameters like key size, energy consumption etc. The result showed that ECC outperforms RSA [41,42]. The time taken in generating keys in RSA is much slower than that in ECC [43,44]. The ECC point multiplication has advantage over RSA modular exponentiation as the key size increases and the processor word reduces [45]. The encryption time and the decryption time of ECC and RSA were analyzed by performing experimental analysis [46]. Certificateless signature schemes were proposed and implemented to provide data security. The time taken for signature generation and verification were computed in certificateless signature scheme [47–51].

3 Proposed Design and Security Architecture

3.1 General Signcryption Algorithm

In this section, a formal model of Certificateless Signature Scheme (CLSC) is defined. These algorithms carry steps for key generation, key management, to signcrypt and to unsigncrypt [37–40]. Algorithm 1 defines the basic steps of CLSC. Fig. 2 defines the phases involved in the signcryption algorithm.

Algorithm 1: General Signcryption Algorithm

Step 1 (Setup phase): A trusted KGC (key generation center) generates a master secret key s $\in Z_n*$. Also, KGC generates master secret key's analogous master public key PK_{KGC} and a set of public parameters, i.e., params.

KGC → master secret key s + master public key PK_{KGC} + *params*

Step 2 (Partial-Private-Key-Extract phase): With the master secret key s, params and the user b's identity ID_i, KGC generates a partial secret key D_i for the user b.

Master secret key *s* +params + User identity,Id_I → a partial secret key D_i

Step 3: KGC sends partial secret key D_i to the user b.

Step 4 (Set-Secret-Value phase): When D_i is established, the user b examines the correctness of D_i. If D_i is accurate then only the user b arbitrarily picks a value $x_i \in Z_n*$ as his/her secret. Else, the session is dismissed.

Step 5 (Set-Public-Key phase): Using *params* and x_i, the user b generates and outputs his/her public key PK_i.

Step 6 (Sign phase): This phase generates a signature σ_i with the message 'msg'. This σ_i is based on msg, *s* and x_i.

Step 7: The user b sends signature σ_i to the verifier.

Step 8 (Verify phase): With the signature σ_i of the message 'msg', the verifier scrutinizes the correctness of σ_i. If the value of the signature is accurate, the signature is valid. Otherwise, the session will be terminated.

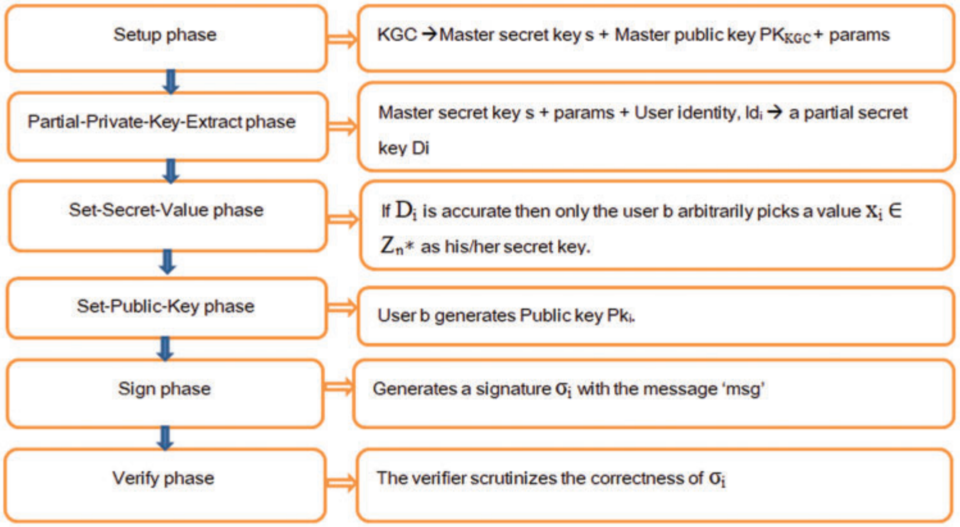
Setup phase
KGC → Master secret key s + Master public key PK_{KGC} + params
Partial-Private-Key-Extract phase
Master secret key s + params + User identity, Id_i → a partial secret key Di
Set-Secret-Value phase
If D_i is accurate then only the user b arbitrarily picks a value $x_i \in Z_n*$ as his/her secret key.
Set-Public-Key phase
User b generates Public key Pk_i.
Sign phase
Generates a signature σ_i with the message 'msg'
Verify phase
The verifier scrutinizes the correctness of σ_i

Figure 2: General signcryption algorithm

The entire process of using signcryption and unsigncryption algorithm has been defined with the help of data flow diagram in Fig. 3. The procedure starts when the user input the data after the pre-processing phase that includes initial parameter setup. After this a master secret key is generated using complex conjugates. Then the random partial private key is generated with the help of key generation center. Thereafter, user keys are generated that generates partial private key using complex mathematical calculations. Then signature generation phase is completed that provides a valid cypher text.

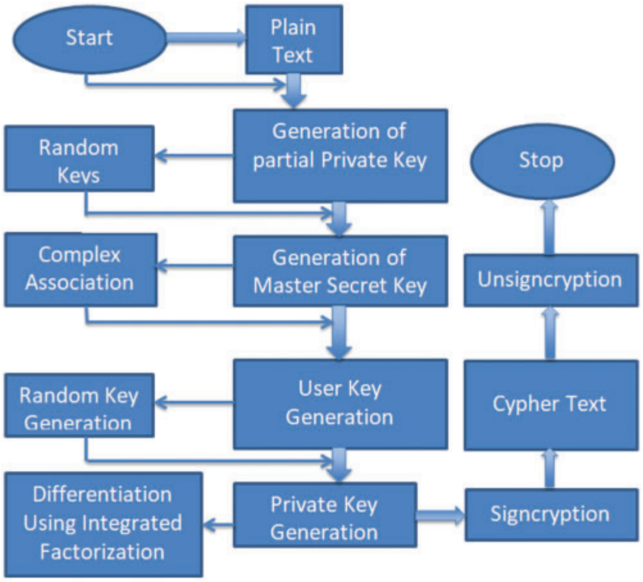

Figure 3: Data flow diagram

Now this generated signature is verified by decrypting the cyphertext with a valid private key. This process is known as unsigncryption. This completes the entire procedure of data encryption and decryption.

3.2 Proposed Framework

Al-Riyami and Paterson in 2003, proposed a new scheme for public key encryption that removes the disadvantages of both public key encryption and IBE keeping in mind the end goal to determine the key escrow issue. The new scheme is known as Certificateless Signcryption (CLSC). This algorithm successfully resolves the problem of certificate management that was in traditional PKI and key escrow problem in IBSC. From IBSC it takes over the solution to certificate management issues and also eradicates the requirement of trusted authority in between. In Identity based signcryption encryption, private key is generated by trusted private key generator (PKG). But it is likely that PKG can misuse its powers (Key escrow problem) so to overcome this CLSC was developed. KGC is used to provide partial private key and thus does not have access to sender's private keys. This partial private key is computed from the sender's identity and a master key. Today IoT gadgets having constrained computational resources and communication bandwidth discover Certificateless public key cryptography extremely appealing and imperative to reduce stack on the system. It also achieves the basic security requirements such as message secrecy and non-repudiation [35–38]. Certificateless cryptography is a public key scheme that gives security without the validation of public key. In this section, an efficient Certificateless Secured Signature Scheme (CSSS) based on ECC is proposed.

The framework is designed to provide security to the healthcare data sensed from IoT devices (Fig. 4). Sender will be present in the IoT environment and the data sensed from the sensor will be transmitted through the gateway node towards cloud servers. During the transmission path a CSSS algorithm will be implemented that is capable of performing encryption and signing in one logical step. The ECC algorithm will be used for generating strong private and public keys. Simultaneously data hashing function will be applied on the transmitted data. Advanced Encryption Standard (AES) is an encryption algorithm that is capable of providing data security and also has high speed. NIST has recommended AES as fastest algorithm than existing algorithms in terms hardware and software implementation. AES is replaced by DES algorithm under the standards defined by NIST. In the proposed scheme, AES algorithm will be implemented for encryption and decryption. The encrypted data is stored in the cloud environment and is further used for processing and analyzing after implementation of the decryption algorithm. This CSSS is capable of providing security to the data being transmitted from the IoT device. In this research the data has been taken from the healthcare WBN sensor. The verification of the signature generated is shown in Fig. 5. This process takes cipher text that is then decrypted using unsigncryption algorithm. Simultaneously digital signature is verified to ensure the integrity of the data received. Here sender public key is used for verification.

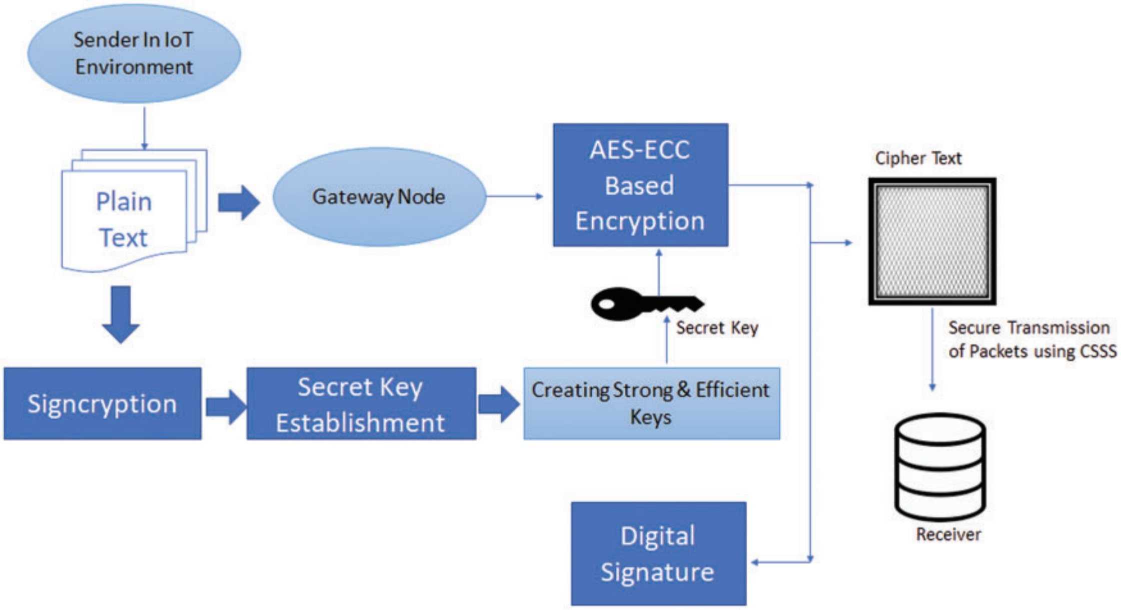

Figure 4: CSSS-signature generation

3.3 *Implementation of CSSS*

Different algorithms that work under signcryption algorithm are defined in the points below. It includes setup, key generation, generate secret key, partial-private-key-Extract, generate private key and generate public key. Tab. 1 represents the basic notations used in above proposed scheme.

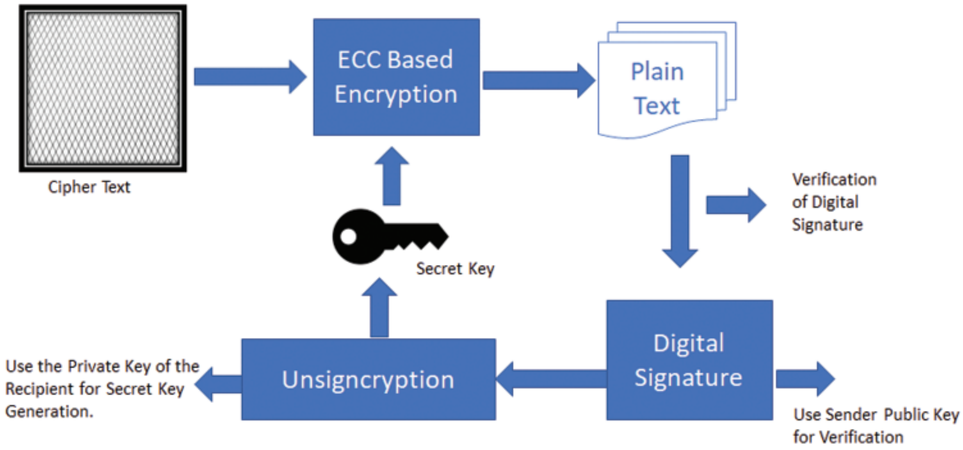
Cipher Text
ECC Based Encryption
Plain Text
Verification of Digital Signature
Secret Key
Use the Private Key of the Recipient for Secret Key Generation.
Unsigncryption
Digital Signature
Use Sender Public Key for Verification

Figure 5: CSSS-signature verification

Table 1: Basic notations used in proposed scheme

Notation	Meaning	Notation	Meaning
UID_a	User ID	(d_a, Q_a)	Private/public key
AID_b	Authentication server ID	D	Encrypted time stamp
X_a	User secret key	sk_a	Private key
x_a	Secure random number	pk_a	Public key
R_a	Partial public key	σ	Signature
AS	Authentication server	r_a	Random number

Algorithm 2: CSSS

Setup: For given security parameters *params*, Authentication Server (AS) engenders various parameters for the system using the defined steps:

- AS selects a k bit prime number q in order to find out the tuple $\{F_q,\ E/F_q, G_q,\ P\}$
- Protected arbitrary number $s \in RZ_q^*$ as the master private key and a master public key is generated using Eq. (1).

$$P_{pub} = sP \tag{1}$$

- Then a one way hash functions is selected i.e., $H_0, H_1, H_2, H_3\ : \{0, 1\}^* \to \{0, 1\}^k$.
- Publish system parameters $= \{F_q,\ E/F_q, G_q,\ P,\ P_{pub},\ \ H_0, H_1, H_2,\ H_3\}$

Key Generation: AS executes the Setup algorithm to generate system parameters and master key. It extracts the partial private key by running a private key extract algorithm for each user. Each user selects a secret value and computes its own private and public key.

(Continued)

Algorithm 2: Continued

Generate Secret Key: Let User U_a is the sender. AS computes private and public key pairs for each user U_a with identities of $UID_a \in \{0, 1\}^*$.

The U_a with UID_a select a protected arbitrary number $x_a \in R\ Z_q^*$ as their secret key and then the scalar multiplication is computed for mathematical related public key as shown in Eq. (2)

$$X_a = x_a P \tag{2}$$

Partial-Private-Key Extract: After computing X_a, U_a send $(UID_a,\ X_a)$ to the AS.

AS chooses a random number $r_a \in RZ_q^*$ and computes

$$R_a = r_a P \tag{3}$$

AS also computes secret key as shown in Eq. (4) and q_a is defined in Eq. (5) using Eq. (3)

$$d_a = r_a + sq_a \ mod \ q \tag{4}$$

where,

$$q_a = H_0(UID_a \parallel R_a \parallel X_a) \tag{5}$$

Through a secure and authentic channel the private key d_a and R_a are transmitted to the user with UID_a by AS. The corresponding ID based public key of user Q_a is computed using the formula as shown in Eq. (6)

$$Q_a = R_a + q_a P_{Pub} \tag{6}$$

Now the private/public key (d_a, Q_a) pair can be verified by checking the Eq. (7). This equation relates the value of private key with correspondence to the public key.

$$Q_a = R_a + q_a P_{Pub} = d_a P. \tag{7}$$

Generate-Private-Key: The private key is generated as shown in Eq. (8) for user with UID_a.

$$sk_a = (d_a, x_a) \tag{8}$$

Generate-Public-Key: The public key is generated in Eq. (9) for user with UID_a.

$$pk_a = (X_a, R_a) \tag{9}$$

3.4 CSSS Signature Generation

When message m request for the signature Sign $(\mathrm{m}, \mathrm{X_a}, \mathrm{UID_a}, \mathrm{AID_b}, \mathrm{d_a}, \mathrm{t})$, then the user performs the following steps:

Algorithm 3: CSSS Signature Generation

- User generates encrypted time stamp in Eq. (9) and sends it to the receiver along with the message.

$$D = E_{PK_{AS}}(t) \tag{10}$$

- User selects a random number $y \in RZ_q^*$ and computes $Y = yP$ and computes hash values as shown in Eqs. (11)–(13)

$$h_1 = H_1(Y) \tag{11}$$

$$h_2 = H_2(UID_a, X_a, Y, AID_b, h_1) \tag{12}$$

$$h_3 = H_3(m, UID_a, X_a, Y, AID_b, t, h_2) \qquad (12)$$

Here t is the time when the request was sent.

- Then Computes V as shown in Eq. (14)

$$V = (y + h_2x_a + h_3d_a) \ mod \ \ q \tag{14}$$

- Alice Computes C as shown in Eq. (15)

$$C = (m \parallel V) \oplus h_2 \tag{15}$$

$$Z = VP$$

- And returns signature σ on message m as shown in Eq. (16)

$$\sigma = (C, Y, Z) \tag{16}$$

3.5 CSSS Signature Verification

The signature σ is (C, Y, Z) generated upon the request of message m, is verified by the verifier AS by performing the following steps:

Algorithm 4: CSSS Signature Verification

- AS Computes $h_1 = H_1(Y)$
- Then XOR operation is performed $C \oplus h_1 = (m \parallel V)$
- AS is verified using Eqs. (6), (12) and (13),

$$h_2 = H_2(UID_a, X_a, Y, AID_b, h_1)$$

$$h_3 = H_3(m, UID_a, X_a, Y, AID_b, h_2, t, h_2)$$

$$Q_a = R_a + q_aP_{Pub}$$

(Continued)

Algorithm 4: Continued

where q_a is computed in Eq. (17)

$$q_a = H_0(ID_a \parallel R_a \parallel X_a) \tag{17}$$

And then verifies the following equation as shown in Eq. (18),

$$Z = Y + h_2X_a + h_3Q_a \tag{18}$$

Check whether the equation $Z = VP$. If it verifies the verifier accepts the signature

$$\sigma = (C, Y, Z) \tag{19}$$

As Eqs. (16) and (19) are equal so signatures are verified.
Otherwise rejects it.

4 Performance Evaluation and Analysis

The effects of implementing Secured Signature Scheme (CSSS) are discussed. Their accuracy in generating the secret key, pre-processing, Encryption and Decryption, computational cost and graph generation were examined and compared with previous papers. The comparison shows that this scheme proves to be better than the previous schemes. All of our algorithms are implemented using Python, used the given hardware and software resources of AMD A6-9225 RADEON R4, 5 COMPUTE CORES 2C + 3G @ 2.60 GHZ processor Windows 10-bit machine with 4GB RAM. ECC is asymmetric public key cryptography that makes use of elliptic curves for the generation of secret keys. These keys are defined by cubical functions,

$$\mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}, \tag{20}$$

Here, a & b are constants.

It is very difficult to find these points on the curve thus higher security is provided using ECC. It provides equal security with smaller key size as compared to other asymmetric algorithms like RSA [41]. Fig. 6 defines the key length of ECC based security framework and RSA based security framework. By reviewing the existing work and focusing on their implementation results it has been analyzed that the size of the keys generated by ECC is much lesser than that of RSA to provide an equivalent level of security. The proposed CSSS performs encryption and decryption of the data using Certificateless signcryption. This scheme is capable of providing security to the data in between the IoT devices. The various security parameters such as confidentiality, authentication, integrity, unforgeability and forward secrecy and non-repudiation are achieved with the proposed scheme.

In case of *Confidentiality*, the data transmitted from IoT to cloud need to be secured from any unauthorized access. In the proposed security model if an unauthorized person tries to access the original message from the encrypted text, then he should have access to private key $\mathrm{SK_a}$, but it is not possible in the proposed algorithm as for deriving $\mathrm{SK_a}$, the attacker requires $\mathrm{x_a}$ that is secured random number that can be generated randomly and can be utilized only once. Through the proposed scheme it can be validated if the data received have not been altered in between transmission paths. If the attacker changes the message m to m’ then the message digest of the original data can be compared with the message digest of received data. Message digest will be different if the data has been altered. Thus, the proposed CSSS provides *message integrity*.

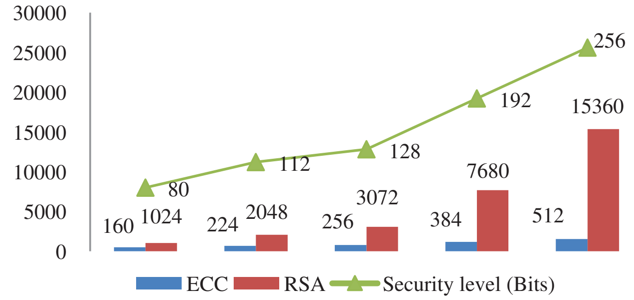

Figure 6: Comparison of ECC and RSA key size with respect to security level in bits [38–43]

In case of *Unforgeability* if an attacker cannot generate valid ciphertext and thus message cannot be forged in proposed scheme because for that attacker requires the SK_a of the sender. Depending upon the condition if the message is forged then it has to satisfy SK_a that is not possible. Through the proposed scheme, *authentication* can be assured at both user level and data level. For user level authentication, the receiver utilizes the user Id UID_a and public key and thus digital signature is obtained that validates user identity. For data level authentication the message m received at the receiver side is validated using the signature σ received at the receiver side.

Forward secrecy is achieved because in CSSS even if an attacker gets the private key PK_a of the sender, then also he cannot get access to the actual message m from the encrypted text. For getting access to the message, the attacker requires secret key SK_a, the random value X_a or through the secret key of the receiver. In CSSS scheme the receiver will be able to ensure that the message was sent by the original user because the digital signature algorithm is implemented under signcryption. Thus, sender signs the encrypted text and thus *non-repudiation* is achieved. Tab. 2 shows the time taken (in ms) for Signature-generation/Encryption, Signature verification/decryption and graph data plotting and is compared with the existing work.

Table 2: Result comparison

Phase	Previous results [40]	Proposed CSSS
Signature-generation/encryption	0.422 ms	0.29747676849365234 ms
Signature-verification/decryption	1.7716 ms	0.3303670883178711 ms

By implementing the proposed CSSS, the pre-processing of the initial parameter setup and signature generation takes lesser time than previous paper [40] (Fig. 7). Also, the decryption time/Signature verification time taken on the transmitted data is significantly less in the proposed scheme (Fig. 8). In [40] the authors have not encrypted the health Id's of the patients.

Tab. 3 shows the comparison of efficiencies of the proposed scheme with previous scheme. The efficiencies of the proposed scheme are compared with the existing signcryption schemes compared in terms of signature generation, signature verification, computational cost and the size of the signature generated during the process.

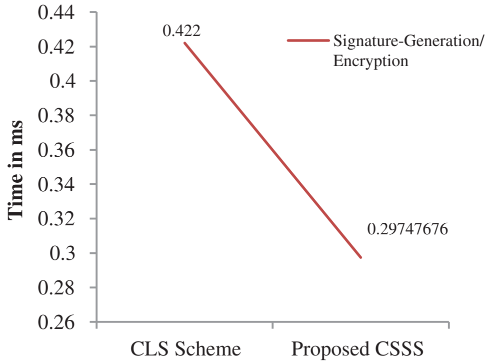

Figure 7: Time required for signature generation

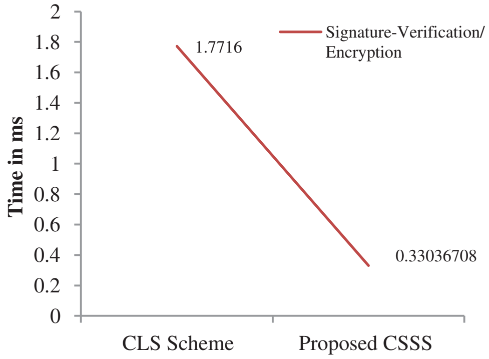

Figure 8: Time required for signature verification

Table 3: Comparison of efficiency

Reference	Signature-generation	Signature-verification	Computational cost	Signature size
Choi et al. [47]	5.127 ms	16.051 ms	21.178 ms	64 byte
Chen et al. [48]	3.418 ms	14.342 ms	17.76 ms	64 byte
Wang et al. [49]	0.422 ms	1.3314 ms	1.7534 ms	61 byte
Yeh et al. [50]	0.422 ms	1.3296 ms	1.7516 ms	41 byte
Karati et al. [51]	0.422 ms	1.3314 ms	1.7534 ms	41 byte
Du et al. [40]	0.422 ms	1.7716 ms	2.1936 ms	41 byte
Proposed CSSS	0.297 ms	0.3303 ms	0.6273 ms	41 byte

As shown in Tab. 3, the efficiency of the proposed scheme is higher than that of the existing schemes. Proposed scheme is compared with relevant existing signcryption schemes such as Choi et al. [47], Chen et al. [48], Wang et al. [49], Yeh et al. [50], Karati et al. [51] and Du et al. [40]. Efficiency is measured in terms of computational cost. CSSS scheme is the best combination of high security and efficiency so far and is more appropriate for the IoT environment. Computational cost is calculated in terms of processing time of signature generation and signature verification. Fig. 9 represents the comparison of proposed scheme with the corresponding state of art schemes in terms of Signature Generation. Signature generation represents the time taken to generate signature and encrypt the message to be transmitted from sender to receiver. Fig. 10 represents the comparison of proposed scheme with the corresponding state of art schemes in terms of Signature Verification. Signature verification represents the time taken to verify the signature by decrypting the cipher text received.

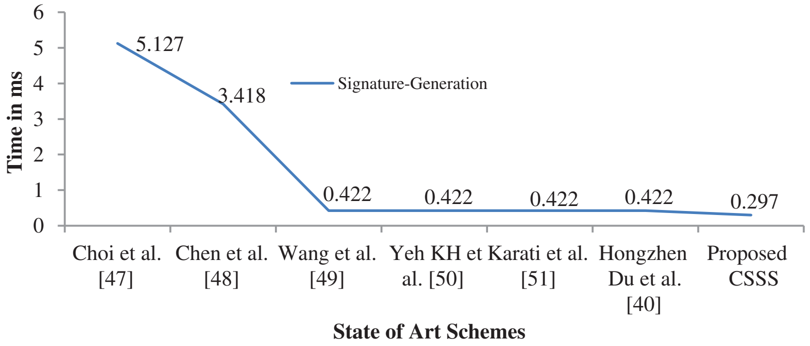

Figure 9: Analysis of time taken for signature generation with state of art

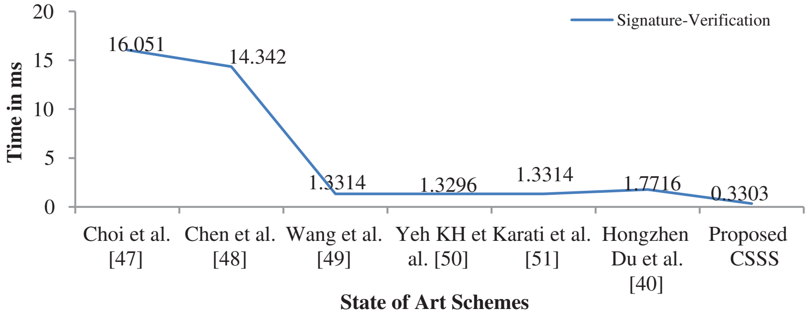

Figure 10: Analysis of time taken for signature verification with state of art

The proposed scheme provides better results as signcryption algorithm is used for the implementation along with ECC for key generation. Computational cost involved in the entire process is computed as total of time taken for signature generation and signature verification. Fig. 11 shows a clear computational cost comparison of the proposed scheme with existing signcryption schemes.

Computational cost =(Signature generation + Signature verification)

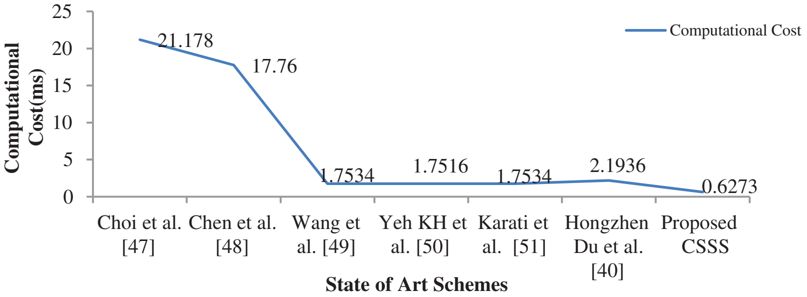

Figure 11: Analysis of computational cost with state of art

5 Conclusion and Future Work

In this paper, a competent and protected joint Key generation, data encryption, digitally signing signcryption scheme for IoT based on healthcare data is presented. A certificateless signcryption algorithm will be implemented to provide a high level of security to data being transmitted from IoT to cloud. CLSC performs signing and encryption in one logical step making it more efficient and secure. The designed scheme is capable of achieving various security parameters such as confidentiality, authentication, integrity, unforgeability and forward secrecy and non-repudiation. Efficiency of the scheme is compared with other schemes in terms of signature generation, signature verification, computational cost and signature size. This scheme performs better than the existing CLS schemes and is more proper for the resource-constrained environment of the IoT. The proposed scheme improves computational cost and provides high level of security for the data being transmitted from low power IoT devices to cloud. Consequently, this CSSS scheme is better and efficient in terms of security and efficiency for an IoT environment. Future work can be done to further minimize the complexity of the proposed scheme and research can also be forwarded to improve energy efficiency parameter while transmission of data from IoT devices. It is expected that this proposed scheme will be enhanced and used as a means of providing security when the proposed research is implemented in real sensor environment. Also the research can be forwarded towards improving the signature size generated during the encryption phase. It is therefore; hope to extensively investigate these issues in the near future.

Funding Statement: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant No. (D14-611-1443). The authors, therefore, gratefully acknowledge DSR technical and financial support.

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

References

[1] P. Singh, M. Masud, M. S. Hossain and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial iot," *Journal of Parallel and Distributed Computing*, vol. 156, pp. 176–184, 2021.

[2] P. V. Dudhe, N. V. Kadam, R. M. Hushangabade and M. S. Deshmukh, "Internet of things (IOT): An overview and its applications," in *Int. Conf. on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, pp. 2650–2653, 2017, IEEE.

[3] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng *et al.,* "Secure and energy-efficient smart building architecture with emerging technology IoT," *Computer Communications*, vol. 176, no. 3, pp. 207–217, 2021.

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[5] A. Botta, W. Donato, V. Persico and A. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[6] L. Kakkar, D. Gupta, S. Saxena and S. Tanwar, "An analysis of integration of internet of things and cloud computing," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 10, pp. 4345–4349, 2019.

[7] L. Kakkar, D. Gupta, S. Saxena and S. Tanwar, "IoT architectures and its security: A review," in *Proc. of the Second Int. Conf. on Information Management and Machine Intelligence*, Jaipur, Rajasthan, vol. 166, pp. 87–94, 2021.

[8] P. Singh, A. Kaur, P. Gupta, S. S. Gill and K. Jyoti, "RHAS: Robust hybrid auto-scaling for web applications in cloud computing," *Cluster Computing*, vol. 24, no. 2, pp. 717–737, 2021.

[9] T. Bhattasali, R. Chaki and N. Chaki, "Secure and trusted cloud of things," in *Annual IEEE India Conf. (INDICON)*, Mumbai, India, IEEE, pp. 1–6, 2013, December.

[10] M. Krichen, S. Mechti, R. Alroobaea, E. Said, P. Singh *et al.,* "A formal testing model for operating room control system using iot," *Computers, Materials & Continua*, vol. 66, no. 3, pp. 2997–3011, 2021.

[11] K. Yelamarthi, M. S. Aman and A. Abdelgawad, "An application-driven modular IoT architecture," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–16, 2017.

[12] V. Pilloni, L. Atzori and M. Mallus, "Dynamic involvement of real world objects in the IoT: A consensus-based cooperation approach," *Sensors*, vol. 17, no. 3, pp. 484, 2017.

[13] H. Boyes, B. Hallaq, J. Cunningham and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1–12, 2018.

[14] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, IEEE, pp. 32–37, 2017.

[15] F. Li, Z. Zheng and C. Jin, "Secure and efficient data transmission in the internet of things," *Telecommunication Systems*, vol. 62, no. 1, pp. 111–122, 2016.

[16] I. Cvitić and M. Vujić, "Classification of security risks in the IoT environment," *Annals of DAAAM & Proceedings*, vol. 26, no. 1, pp. 731–740, 2015.

[17] P. Singh, A. Kaur and N. Kumar, "A reliable and cost-efficient code dissemination scheme for smart sensing devices with mobile vehicles in smart cities," *Sustainable Cities and Society*, vol. 62, pp. 102374, 2020.

[18] R. Negra, I. Jemili and A. Belghith, "Wireless body area networks: Applications and technologies," *Procedia Computer Science*, vol. 83, pp. 1274–1281, 2016.

[19] N. D. Han, L. Han, D. M. Tuan, H. P. In and M. Jo, "A scheme for data confidentiality in cloud-assisted wireless body area networks," *Information Sciences*, vol. 284, pp. 157–166, 2014.

[20] H. P. Chiang, C. F. Lai and Y. M. Huang, "A green cloud-assisted health monitoring service on wireless body area networks," *Information Sciences*, vol. 284, pp. 118–129, 2014.

[21] I. Masood, Y. Wang, A. Daud, N. R. Aljohani and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 23–46, 2018.

[22] A. Whitmore, A. Agarwal and L. Da Xu, "The internet of things—a survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[23] D. Miorandi, S. Sicari, F. De Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[24] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn and G. Schreier, "The internet of things for ambient assisted living," in *Seventh Int. Conf. on Information Technology: New Generations*, Las Vegas, Nevada, USA, pp. 804–809, 2010.

[25] F. Ullah, A. H. Abdullah, O. Kaiwartya, J. Lloret and M. M. Arshad, "EETP-MAC: Energy efficient traffic prioritization for medium access control in wireless body area networks," *Telecommunication Systems*, vol. 75, no. 2, pp. 181–203, 2020.

[26] F. Ullah, Z. Ullah, S. Ahmad, I. U. Islam, S. U. Rehman *et al.,* "Traffic priority based delay-aware and energy efficient path allocation routing protocol for wireless body area network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 3775–3794, 2019.

[27] F. Ullah, A. H. Abdullah, O. Kaiwartya, S. Kumar and M. M. Arshad, "Medium access control (MAC) for wireless body area network (WBAN): Superframe structure, multiple access technique, taxonomy, and challenges," *Human-centric Computing and Information Sciences*, vol. 7, no. 1, pp. 1–39, 2017.

[28] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[29] A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks," *Future Generation Computer Systems*, vol. 55, pp. 266–277, 2016.

[30] A. A. V. Rani and E. Baburaj, "An efficient secure authentication on cloud based e-health care system in WBAN," *Biomedical Research-India*, vol. 27, pp. 53–59, 2016.

[31] A. Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Secure and scalable cloud-based architecture for e-health wireless sensor networks," in *Int. Conf. on Computer Communications and Networks (ICCCN)*, Germany, IEEE, pp. 1–7, 2012.

[32] J. Lee, S. Kang and S. Kim, "Study on the smart speaker security evaluations and countermeasures," *Advanced Multimedia and Ubiquitous Engineering*, Las Vegas, Nevada, USA, pp. 50–70, 2019.

[33] C. C. Aggarwal, N. Ashish and A. Sheth, "The internet of things: A survey from the data-centric perspective," *Managing and Mining Sensor Data*, pp. 383–428, 2013.

[34] A. Jara, F. Belchi, A. Alcolea, J. Santa, M. Zamora-Izquierdo *et al.,* "A pharmaceutical intelligent information system to detect allergies and adverse drugs reactions based on internet of things," in *2010 8th IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, Germany, pp. 809–812, 2010.

[35] A. J. J. Valera, M. A. Zamora and A. F. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in *IEEE Consumer Communications and Networking Conf.*, Las Vegas, USA, IEEE, pp. 1–5, 2010.

[36] Z. Xu, M. Luo, M. K. Khan, K. K. R. Choo and D. He, "Analysis and improvement of a certificateless signature scheme for resource-constrained scenarios," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1074–1078, 2020.

[37] M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Int. Conf. on Computational and Information Science*, Georgia, USA, vol. 5576, pp. 110–116, 2005.

[38] Z. Zhang, D. S. Wong, J. Xu and D. Feng, "Certificateless public-key signature: Security model and efficient construction," *International Conference on Applied Cryptography and Network Security*, vol. 3989, pp. 293–308, 2006.

[39] K. H. Yeh, C. Su, K. K. R. Choo and W. Chiu, "A novel certificateless signature scheme for smart objects in the internet-of-things," *Sensors*, vol. 17, no. 5, pp. 1001, 2017.

[40] H. Du, Q. Wen, S. Zhang and M. Gao, "A new provably secure certificateless signature scheme for internet of things," *Ad Hoc Networks*, vol. 100, pp. 102074, 2020.

[41] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas and L. Castedo, "A practical performance comparison of ecc and rsa for resource-constrained iot devices," *Global Internet of Things Summit (GioTS)*, vol. 14, pp. 1–6, 2018.

[42] V. B. Kute, P. B. Paradhi and G. R. Bamnote, "A software comparison of rsa and ecc," *International Journal of Computer Science and Applications*, vol. 2, no. 1, pp. 43–59, 2009.

[43] N. Jansma and B. Arrendondo, "Performance comparison of elliptic curve and rsa digital signatures," in *Technical Report*, Ann Arbor, MI, USA: University of Michigan, 2004.

[44] V. Gopinath and R. S. Bhuvaneswaran, "Design of ECC based secured cloud storage mechanism for transaction rich applications," *Computers, Materials & Continua*, vol. 57, no. 2, pp. 341–352, 2018.

[45] N. Gura, A. Patel, A. Wander, H. Eberle and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems*, vol. 14, pp. 119–132, 2004.

[46] D. Mahto, D. A. Khan and D. K. Yadav, "Security analysis of elliptic curve cryptography and RSA," *Proceedings of the World Congress on Engineering*, vol. 1, pp. 419–422, 2016.

[47] K. Y. Choi, J. H. Park and D. H. Lee, "A new provably secure certificateless short signature scheme," *Comput. Math. Appl.*, vol. 61, no. 7, pp. 1760–1768, 2011.

[48] Y. C. Chen, R. Tso, G. Horng, C. I. Fan and R. H. Hsu, "Strongly secure certificateless signature: Cryptanalysis and improvement of two schemes," *Journal of Information Science and Engineering*, vol. 31, no. 1, pp. 297–314, 2015.

[49] L. Wang, K. Chen, Y. Long and X. Mao, "A modified efficient certificateless signature scheme without bilinear pairings," in *Int. Conf. on Intelligent Networking Systems*, Taipei, Taiwan, pp. 82–85, 2015.

[50] K. H. Yeh, C. Su, K. -K. R. Choo and W. Chiu, "A novel certificateless signature scheme for smart objects in the internet-of-things," *Sensors*, vol. 17, no. 5, pp. 1–17, 2017.

[51] A. Karati, S. H. Islam and G. P. Biswas, "A Pairing-free and provably secure certificateless signature scheme," *Information Sciences*, vol. 450, pp. 378–391, 2018.