Bilinear Paired Boneh–Lynn–Shacham Certificateless Signcryption for Secured Healthcare Data Transmission in IoT Environment

K. Hemalatha[1], P. Vijayakumar[2]

{ hemalathacbe2010@gmail.com[1], viajayvigash@gmail.com[2]}

Assistant Professor[1], Associate Professor[2], KG College of Arts and Science, Coimbatore[1,2]

Abstract. Healthcare data is the information collected during the patient care. Information about patient health is gathered, processed, stored, examined and distributed. Secure communication is the method of transmitting the information between cloud user and cloud server. The patient transmits their collected information with different degrees of certainty. The data security is an important one for guaranteeing large number of cloud users. Performance of safe healthcare data communication was achieved by using many cryptographic techniques was introduced. However, data secrecy and integrity rate was not improved by conventional methods. IoT based Bilinear Paired Boneh–Lynn–Shacham Certificateless Signcrypted Data Communication (IoT-BPBLSCSDC) Method is introduced. The main aim of IoT-BPBLSCSDC Method is to perform secured healthcare data transmission for IoT environment with lesser storage cost. IoT-BPBLSCSDC Method comprises three processes, namely registration, signcryption and unsigncryption for secured healthcare data transmission. Initially, the number of sensor devices are registered and placed for monitoring the body motion and vital signs. Boneh–Lynn–Shacham Certificateless Signcryption is carried out in IoT-BPBLSCSDC Method for encrypting the collected data from patients from different location. Finally, Boneh–Lynn–Shacham Certificateless Unsigncryption process is performed in IoT-BPBLSCSDC Method based on successful validation and corresponding medical information is given to the receiver. Existing and IoT-BPBLSCSDC is compared to estimate experimental analysis. Result reveals of IoT-BPBLSCSDC achieves superior data confidentiality as well as data integrity when compared to other three existing cryptographic methods.

Keywords: Healthcare data, medical information, data transmission, IoT environment, signcryption, unsigncryption.

1 Introduction

Healthcare systems have witnessed huge growth with different technologies. CGST-FCM was designed in [1] to encrypt data using GM as well as transferred for confirmation. But, it failed to consider storage cost during group signcryption. The patient authentication is carried [2] with

IACIDS 2023, November 23-25, Lavasa, India
Copyright © 2024 EAI
DOI 10.4108/eai.23-11-2023.2343178

Improved Elliptical Curve Cryptography (IECC). But, the accuracy rate was not focused. CBCSES was introduced by [3] to perform encryption and signcryption. But, storage cost was not reduced. An encryption scheme was introduced in [4] through elliptic curve cryptography for protecting data. Designed scheme guaranteed data reliability.

Secure as well as scalable healthcare data transmission was designed by [5] with IoT depending on routing protocol. Data cleaning algorithms were utilized to perform preprocess. PCA was used for decreasing weight. A heterogeneous ring signcryption scheme was introduced in [6] for secure communication from the sensor to the server. But, the data rate was not improved by the heterogeneous ring signcryption scheme. A robust multi-level security method was designed in [7] to avoid adversaries and guaranteed data confidentiality. Hybrid IoT was designed in [8] for device verification. However, the computational cost was not reduced. A healthcare system was introduced in [9] with a high degree of public verification in the reliable and cost-effective cloud platform. But, the computational cost was not reduced. A new cryptography-based authentication was designed in [10] to confirm device validation in communication. But, storage cost was not minimized. The main contribution of the IoT BPBLSCSDC Method is given as,

- IoT-BPBLSCSDC Method performs the secured healthcare data transmission in an IoT environment with a lesser storage cost. IoT-BPBLSCSDC Method comprises a registration process, signcryption process, and unsigncryption process for secured healthcare data transmission. The number of sensor devices is registered and positioned for monitoring body motion and vital signs.
- Boneh–Lynn–Shacham certificate less Signcryption is performed in IoT-BPBLSCSDC Method for converting the collected data from patients at the different locations into encrypted form.
- Boneh–Lynn–Shacham Certificateless Unsigncryption process is used in IoT-BPBLSCSDC Method depending on the successful validation and corresponding medical information given to the receiver with a higher security level.

The research objective of IoT BPBLSCSDC Method is followed by,

- To obtain secured healthcare data transmission in IoT, IoT-BPBLSCSDC is

developed for minimizing storage cost.

- To execute data encryption for finding authorized user, Boneh–Lynn–Shacham Certificateless Signcryption is utilized for improving data integrity.
- To perform signature and validation process, Boneh–Lynn–Shacham Certificateless Unsigncryption process is employed with higher confidentiality.

The rest of the paper is organized into Section 2 reviews the survey on literature for secured data transmission. Section 3 explains the methodology of analysis. Section 4 presents the experimental setup. The obtained results and related analysis are represented in Section 5. Finally, Section 6 concludes the paper.

2 Related Works

An intelligent healthcare system was introduced in [11] with IoT. The designed method sense and processes the patient data. A new high payload, as well as a reversible EHR embedding method, was designed in [12] for protecting data. But the security level was not improved. An anonymous certificateless signcryption scheme was introduced in [13] for IoHT applications with HEC for addressing-protection necessities. Designed method guaranteed privacy level. A new certificateless hybrid signcryption scheme was designed in [14] for data transmission with IoT resource devices. The designed scheme addressed confidentiality and unforgeability with higher computational efficiency and lesser transmission overhead. A lightweight authentication technique was designed with homomorphic encryption. The designed technique was employed for protecting data in an encrypted format.

3 Methodology

Healthcare data is any kind of data related to health conditions, outcomes, death causes, and quality of life for individuals. However, existing secure transmission methods were time-consuming processes and not attained improved security. In order to address these issues, IoT based Bilinear Paired Boneh–Lynn– Shacham Certificateless Signcrypted Data Communication (IoT-BPBLSCSDC) Method is introduced in healthcare applications.MHEALTH dataset from kaggle, body movement and vital signs recordings from ten cloud users 'CU_i' with sensor devices 'D_i' are collected. The data are registered in User Registration with help of Hub 'H' and Trusted Third Party 'TTP'. Data encryption is carried out using Boneh–Lynn–Shacham Certificateless Signcryption process. Lastly, to guarantee secure transmission, data gets decrypted using Boneh–Lynn–Shacham Certificateless Unsigncryption process. With these three distinct processes, security was ensured via data integrity and confidentiality.

3.1. IoT based Bilinear Paired Boneh–Lynn–Shacham Certificateless Signcrypted Data Communication

Registration as well as key generation is carried in IoT-BPBLSCSDC. In the registration procedure, user registers personal information o server. Information's stored on the server. The MHEALTH dataset is used for safe healthcare data communication. When patients are at any hospital, they fill registration form CSP. It comprised data. cloud service provider transmits theme-based Time One Time Pin (TOTP) to enter a mobile number. Consequently, user enters TOTP inside specific time. When pin not entered at specific time period via user, user is toward log in once more as well as enters information. The generated time-based OTP applies to a particular time. Behind entering time-based OTP, the cloud server transmits the registered message to the equivalent user. With all registered cloud user, cloud server generates two keys.

$$Cloud\ User \quad Enter\ User\ Details \rightarrow Cloud\ Server \tag{1}$$

From (1), cloud user enters their details to server. Cloud server sends TOTP to entered mobile number.

$$Cloud\ Server \quad TOTP \rightarrow Cloud\ user \tag{2}$$

Cloud user provides TOTP within particular time given by cloud server. Cloud server stored their information well as produce key pairs. Consider secret signature key 'PI' is considered a positive integer and produced with Bilinear Paired Boneh–Lynn–Shacham Key Generation.

$$Pv_k = PI \tag{3}$$

From (3), 'Pv_k' represents the private key and 'PI' is chosen arbitrarily. After private key generation, it is attained by

$$Pb_k = owf(PI) \tag{4}$$

From (4), '$owf(PI)$' represents the one-way function as,

$$owf(PI) = PI + 1 \; mod \; 16 \tag{5}$$

From (5), 'Pb_k' indicates public verification key attained as 'PI'. Public verification keys are denoted by 'ID'. Public key is sent to registered user in cloud environment.

- **Signcryption**

IoT-BPBLSCSDC Method performed the signcryption for data sharing.When the registered cloud needs to access data on the server, the cloud penetrate'ID' in the login window. During registration, cloud server confirms that entered IDs are matched using'ID' stored. CS allows entrée right to users. Then, user access uses 'if' and '$then$' rules. When entered 'ID' is matched by 'ID' stored on the server, after that user is an authorized user, as well as the server, authorized access. Or else, the cloud user was considered an unauthorized user. When the server authenticates the user, then patient data is shared in ciphertext form. The server transmits encrypted data to the approved user.

Let us consider cloud user data are '$cud_1, cud_2, cud_3, \ldots . cud_n$'. Ciphertext of patient data is accessed with cloud server is,

$$C(cud) \leftarrow En \langle Pb_k, cud \rangle \tag{6}$$

From (6), '$C(cud)$'represents ciphertext of cloud user data 'cud'. 'En' represents the encryption using'(Pb_k)'. A digital signature is produced with the private key. Digital signature presents data produced with the server and data is not varied by any intruders. Boneh–Lynn–ShachamCertificatelessSignature Generation algorithm is carried out using the private key. Consider patient data and signature generation is illustrated as

$$Signature_{cud} = \left(R_{ijcud}\right) \tag{7}$$

From (7), '$Signature_{cud}$'represents the signature of cloud data 'cud'.'PK_{ij}'symbolizes the private key position of the sender. 'pi' symbolizes the positive integer. After signature generation, the cloud server sends the ciphertext and signature.

- **Unsigncryption**

IoT-BPBLSCSDC Method executes unsigncryption for attaining patient data. Through performing Boneh–Lynn–Shacham Certificateless Signature Verification algorithm, the signature verification is carried out.

$$Signature_{cud}'' = owf(S_{cud}) \tag{8}$$

$$owf(Signature_{cud}) = Signature_{cud} + 1 \; mod \; 16 \quad (9)$$

From (9),'$Signature_{cud}{}''$'represents signature generated at the receiver side.'$owf(Signature_{cud})$' symbolizes the one-way function of signature. '$S_{cd}{}''$' is verified with public key 'Pb_k'. When both signatures get matched, it is valid and the user decrypts encrypted data. When the signature is not matched and is invalid, it did not decrypt ciphertext. The authorized user decrypts ciphertexts well as attains original data by,

$$cud \leftarrow Dec\,\langle Pv_k, C(cud)\rangle \quad (10)$$

From (10),'cud' symbolizes original data. 'Dec' denotes the decryption.'Pv_k' symbolizes private key.'$C(cud)$'represent ciphertext. Original data is attained by protected healthcare data transmission in IoT environment. IoT-BPBLSCSDC Method to access data with higher data confidentiality. The algorithmic process of IoT-BPBLSCSDC is given as

// Algorithm 1 IoT based Bilinear Paired Boneh–Lynn–Shacham Certificateless Signcrypted Data Communication
Input: Number of cloud data '$cud_1, cud_2, cud_{3,\ldots} cud_m$'   **Output:** Increase data confidentiality level

Begin
 Number of cloud users taken as input at input layer
 For each user u_i // **Registration and key generation**
 Register the details to server
 Cloud server sends the time based one-time password '$TOTP$'
 User enters '$TOTP$' at particular time 't'
 Cloud server generates a private and public key
 End for
 Login to server with valid identity **//Signcryption**
 If (identity matched with server database) **then**
 User is considered as an authorized user
 Cloud server permits the access
 else
 User is considered as an unauthorized user
 Cloud server denied the access
 End if
 Perform data encryption using public key

Perform digital signature generation

Send to the authorized user

If signature is valid **then // Unsigncryption**

Perform data decryption using private key

Obtain the original data

End if End

4 Experimental Setup

IoT-BPBLSCSDC Method and existing CGST-FCM [1], IECC [2], CBCSES[3] and Anonymous certificateless signcryption scheme [4] are implemented using MATLAB-SIMULINK tool with help of the MHEALTH datataset from https://www.kaggle.com/datasets/gaurav2022/mobile-health.

5 Result and Discussion

5.1 Storage Cost

Storage cost 'SC' is defined as memory consumed while storing the public key, private key and secret key of the corresponding cloud user respectively. Storage cost is formulated as,

$$SC = \sum_{i=1}^{n} Cloud\ user_i * Mem\left[Pb_{k_i} + Pv_{k_i} + S_{k_i}\right] \quad (11)$$

From above equation (11), the memory is taken to store with the public key 'Pb_{k_i}', private key 'Pv_{k_i}' and secret key 'S_{k_i}'. Table 1 discusses the storage cost of the proposed method and four different existing methods.

Table 1 illustrates the storage cost. The different number of samples ranging between 500 and 5000 are considered from different physical activities. From above table representation, when sample instances get increased, storage cost gets increased using all four different methods. This is evident from the simulation results where 15 KB of results were arrived using the IoT-BPBLSCSDC, 22 KB, 31 KB, 43 KB using [1] [2] [3] for 500 samples. The reason for lesser storage cost is to apply Boneh–Lynn–Shacham Certificateless Signcryption and Unsigncryption process in IoT-BPBLSCSDC Method. Contrary to [1], [2] [3], storage cost using IoT-BPBLSCSDC is reduced as 34%, 45%, 60%.

Table 1 Tabulation for Storage Cost

Samples	Storage Cost (KB)			
	IoT-BPBLSCSDC Method	CGST-FCM	IECC	CBCSES Scheme
500	15	22	31	43
1000	17	25	35	50
1500	21	32	41	56
2000	25	36	46	62
2500	28	45	52	74
3000	32	52	56	82
3500	41	68	75	95
4000	49	74	86	106
4500	56	82	93	119
5000	65	90	105	128

5.2 Data Confidentiality Rate

Ratio of number of sample data preserved to whole number of samples sent computed as data confidentiality.

$$DCR = \sum_{i=1}^{n} \frac{S_{Prot}}{S_i} * 100 \quad (12)$$

From (12), data confidentiality rate 'DCR' is calculated on samples 'S_i' and number of sample data protected 'S_{Prot}'. It is expressed by percentage (%).

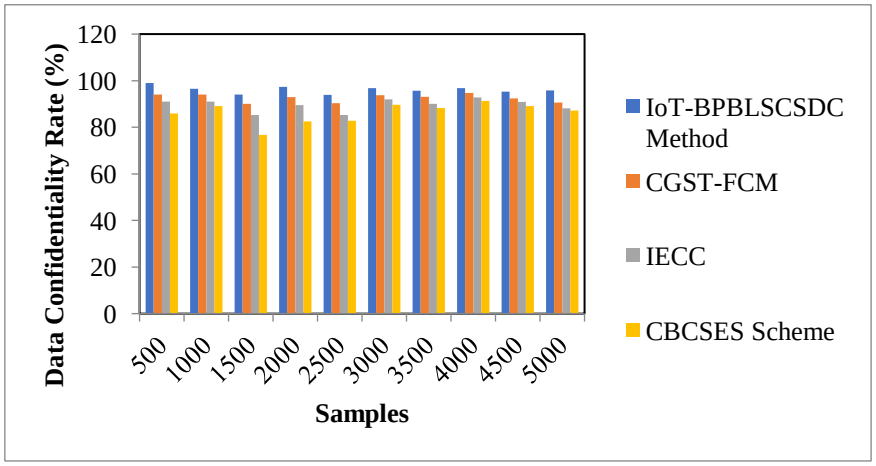

Fig 1 Measurement of Data Confidentiality Rate

Fig 1 describes graphical representation of DCR versus number of samples. The blue, brown, green, violet color column denotes the data confidentiality rate of IoT-BPBLSCSDC, CGST-FCM [1], IECC [2] and CBCSES scheme [3]. The reason is owing to application of Boneh–Lynn–Shacham Certificateless Signcryption and Unsigncryption process for secured healthcare data communication. Assume 500 samples, performance of DCR is 99%, 94%, 91% and 86% using IoT-BPBLSCSDC, [1] [2] respectively. Ten different results are observed with each method. The performance of the proposed LFSR-CROL is compared to results of other existing methods. Data confidentiality rate using IoT-BPBLSCSDC increased by 4%,7% 12%, compared to [1],[2],[3].

5.3 Data Integrity Rate

It has estimated as percentage of number of samples that are not changed by any malicious cloud user to the number of samples. The data integrity rate is formulated as,

$$DIR = \sum_{i=1}^{n} \left(\frac{S_{na}}{S_i}\right) * 100 \quad (13)$$

From (13), data integrity rate 'DIR' is determined based on the number of samples that are not altered by malicious users 'S_{na}''. Table 2 shows a comparison between data integrity rates for proposed and existing methods.

Table 2 Tabulation for Data Integrity Rate

Samples	Data Integrity Rate (%)			
	IoT-BPBLSCSDC Method	CGST-FCM	IECC	CBCSES Scheme
500	95	92	90	80
1000	98	93	90	87
1500	94	86.7	80	73.3
2000	98.8	88	85	77.5
2500	88	86.4	81.2	80
3000	91.7	90.5	90	86.3
3500	90	85.7	84.2	82.9
4000	90	87.5	87.8	88.8
4500	92.2	91.1	88.7	86.7
5000	94	89.2	86	85.2

Table 2 demonstrates data integrity rate. Let us consider the 1000 data samples as input for calculating the DIR, the performance of the IoT-BPBLSCSDC technique is 95%. Similarly, the performance of DIR using [1] and [2] are 92%, 90%, and 80% respectively. Likewise, different results are observed for all four methods. Then, percentages of the DIR using the proposed

technique are compared to existing results. This is due to the application of way cryptography hash function applied to Burrows–Abadi–Needham logic–based Signcryption algorithm. $DIR$is increased by5%, 8%, 13%, compared to [1] [2],[3].

6 Conclusion

This paper presents a new method called IoT-BPBLSCSDC Method for protecting personal health information and secured healthcare data transmission for IoT environment. At first, number of sensor devices is registered to monitor body motion and vital signs of patient at diverse places. Next, Boneh–Lynn–Shacham Certificateless Signcryption encrypts gathered data from patients. Then, Boneh–Lynn–Shacham Certificateless Unsigncryption process executes successful validation. Lastly, respective medical information is transmitted to receiver. We performed in depth experiments using a MHEALTH dataset to evaluate outcomes of the proposed method. During secured healthcare data communication, IoT-BPBLSCSDC Method has yielded superior results, with highest confidentiality (8%), integrity (13%), and storage cost (46KB) in cloud platform. In future work, the proposed technique is further implemented to obtain security by using a novel signcryption and unsigncryption technique for the healthcare system. We also plan to test the proposed method on different data sets along with increasing the network samples.

References

[1] Chandrashekar Meshram, Agbotiname Lucky Imoize, Sajjad Shaukat Jamal, Adel R. Alharbi, Sarita Gajbhiye Meshram and Iqtadar Hussain, "CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps", IEEE Access, Vol 10, pp. 39853 – 39863. April 2022.

[2] Mohammad Ayoub Khan, Mohammad Tabrez Quasim, Norah Saleh Alghamdi and Mohammad Yahiya Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data", IEEE Access, Vol 8, pp. 52018 – 52027. March 2020.

[3] Insaf Ullah, Noor Ul Amin, Muhammad Asghar Khan, Hizbullah Khattak, Saru Kumari, "An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System", Journal of Medical Systems, Springer, Sep 2020

[4] Sangjukta Das and Suyel Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure", Computers and Electrical Engineering, ACM, Vol 101, Issue C, pp. 1-15. July 2022.

[5] Eshrag Refaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, and Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Hindawi Publishing Corporation, Wireless Communications and Mobile Computing, Vol 2022, pp. 1-12.2022.

[6] Fagen Li, Zhaohui Zheng and Chunhua Jin, "Secure and efficient data transmission in the Internet of Things", Telecommunication Systems, Springer, Vol 62, 2016, pp.111–122.

[7] Nasir N. Hurrah, Shabir A. Parah, Javaid A. Sheikh, Fadi Al-Turjman and Khan Muhammad, "Secure data transmission framework for confidentiality in IoTs", Ad Hoc Networks, Elsevier, Vol 95, pp. 1-18, December 2019.

[8] Ming-Shen Jian and Jimmy Ming-Tai Wu, “Hybrid Internet of Things (IoT) data transmission security corresponding to device verification”, Journal of Ambient Intelligence and Humanized Computing, Springer, pp. 1-18.2021.
[9] Mahmood Shahul Hamid, S. Babu and R. Pitchai, “Secure identity-based proxy re-encryption techniques for healthcare system”, Materials Today: Proceedings, Elsevier, pp. 1-5. April 2021.
[10] G. Manikandan and R. Perumal, “Symmetric cryptography for secure communication in IoT”, Materials Today: Proceedings, Elsevier, pp 1-15. November 2020.
[11] Kashif Hameed, Imran Sarwar Bajwa, Shabana Ramzan, Waheed Anwar and Akmal Khan, “An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks”, Scientific Programming, Hindawi Publishing Corporation, Vol 2020, Pages 1-15,2020.
12] Shabir A. Parah, Javaid A. Kaw, Paolo Bellavista, Nazir A. Loan, G. M. Bhat, Khan Muhammad and Victor Hugo C. de Albuquerque, “Efficient Security and Authentication for Edge-Based Internet of Medical Things”, IEEE Internet of Things Journal, Vol 8, Issue 21, pp. 15652 – 15662. November 2021.
[13] Insaf Ullah, Ali Alkhalifah, Sajjad Ur Rehman, Neeraj Kumar and Muhammad Asghar Khan, “An Anonymous Certificateless Signcryption Scheme for Internet of Health Things”, IEEE Access, Vol 9, pp. 101207 – 101216. July 2021.
[14] Yong Wu, Bei Gong and Yu Zhang, “An Improved Efficient Certificateless Hybrid Signcryption Scheme for Internet of Things”, Wireless Communications and Mobile Computing, Hindawi Publishing Corporation, Vol 2022, pp. 1-15.2022.