Indexed Steep Descent Fish Optimization with Modified Certificateless Signcryption for Secured IoT Healthcare Data Transmission

K. Hemalatha[1] and Dr. P. Vijayakumar [2]

[1]Ph.D. Scholar, Department of Computer Science, Sri Jayendra Saraswathy Maha Vidyalaya College of Arts and Science, Coimbatore, India. [1]Assistant Professor, Department of Computer Science, KG College of Arts and Science, Coimbatore, India
[2]Associate Professor, Department of Computer Applications, KG College of Arts and Science Coimbatore, India

***Correspondence:** K. Hemalatha; Email: hemalathacbe2010@gmail.com

ABSTRACT- IoMT is a healthcare strategy and utilization connected with online computer networks for IoT. During data communication from machine to machine, Security is one of essential barriers. In order to improve security, Jaccardized Czekanowski Indexive, Steepest Descent Fish Optimization Based Kupyna Schmidt-Samoa Certificateless Signcryption (JCISDFO-KSSCS) is introduced. JCISDFO-KSSCS is used for enhancing authentication and secure Data Transmission. JCISDFO-KSSCS comprises two major processes, namely authentication, and secured data transmission. The discussed results indicate that proposed JCISDFO-KSSCS increases the performance results than the conventional approaches.

Keywords: IoMT, Jaccardized Czekanowski Index-based Authentication, Steepest Descent Fish Swarm Optimization, Kupyna Schmidt- Samoa Certificateless Signcryption, Tversky Similarity Coefficient.

ARTICLE INFORMATION

Author(s): K. Hemalatha and Dr. P. Vijayakumar

Special Issue Editor: Dr. S. Gopalakrishnan ;
Received: 01/05/2022; **Accepted**: 03/06/2022 **Published**: 30/06/2022;
e-ISSN: 2347-470X;
Paper Id:0422SI-IJEER-2022-17;
Citation: 10.37391/IJEER.100249
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100249.html

This article belongs to the Special Issue on **Intervention of Electrical, Electronics & Communication Engineering in Sustainable Development**

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

A new smart secure authentication (SSA) model was introduced in [1] for healthcare applications to increase the security of data transmission from patients to physicians. The designed SSA model uses the crypto-primitives such as bilinear pairing, ECC, and bio-hash to perform the signature generation resulting in minimizing the computation cost. However, the performance of accurate authentication and confidentiality rate was not improved. An improved Elliptical Curve Cryptography (IECC) scheme was introduced in [2] for authentication and encryption of IoT-based medical data. Though the designed scheme minimizes the computational cost, the higher confidentiality with minimum storage cost was not obtained during the secure data transmission.

2. RELATED WORKS

Heterogeneous integrated network resource management scheme was developed and analyzed in to secure transmission. But the authentication was not focused. CP-HABE was introduced by to enhance data security. But the performance of confidentiality level was not improved. A cloud-based cryptographic and non-cryptographic techniques were developed in for eHealth to ensure the confidentiality and security of digital data. CB-PRES was introduced in for e-health data distribution. However, it was unsuccessful to discuss privacy as well as security within Electronic Health Records (EHRs).

3. PROPOSAL METHODOLOGY

Smart healthcare sensors as well as IoT enabled medical devices to transmit data as well as combine with smart devices for protecting broadcast collected sensitive data. Therefore, efficient encryption schemes are needed to ensure secure transmission from any other security threats. Moreover, authentication is another major criterion of each communication system, especially in healthcare applications. JCISDFO-KSSCS is developed to protect data transmission and prevent authorized access in cloud-based applications to protect eHealth record data.

3.1 Authentication

In authentication step, proposed JCISDFO-KSSCS begins for achieving registration process by storing the data. Let us consider two different large prime numbers m and n the public key of the patient is generated as follows

$$\alpha_p = m^2 * n \qquad (1)$$

From (1), α_p indicates public key. Based on public key, private key of the patient is generated as follows,

$$_r = \frac{1}{\alpha_p} * \ mod\ K \qquad (2)$$

Where,

$$\varphi\ (m-1, n-1) \qquad (3)$$

From (2), (3) β_r indicates private key, α_p indicates public key, φ denotes a least common multiple factors. Once the keys are generated, the registration process is completed. After the registration, the server stores the patient details in the form of a hash code using Kupyna single-block-length compression function. The patient data (D_i) are divided with number of blocks.

$$D_i = z_1, z_2, z_3, \dots z_k \qquad (4)$$

Where, $z_1, z_2, z_3, \dots z_k$ denotes the number of blocks. Then the input block is gien to the Kupyna single-block-length compression function which takes an input block (z_1) and previous hash and finally generating the hash value (h).

$$h = [F_z(\mathrm{h}_{i-1}) \oplus \mathrm{h}_{i-1}] \qquad (5)$$

Where h denotes a final hash value generated from the compression function feeds block 'F_z'. It feeds previous hash 'h_{i-1}'. When there is no previous hash value and it was located to constant pre-specified value in binary. The output of ciphertext is XORed ($\oplus$) with previous hash value (h_{i-1}) to hash 'h'. Then hash value is stored in server. Therefore, the newly generated hash value '$h_n{}'$' is given below,

$$h_n = [F_z(h_{i-1}) \oplus h_{i-1}] \qquad (6)$$

Using the h and h_n, the genuine patients are identified. When h and h_n are the same, the hash value verification is done by using the Jaccardized Czekanowski index. The verification process is performed as follows,

$$\delta = \frac{h \cap h_n}{\sum h + \sum h_n - h \cap h_n} \qquad (7)$$

Where δ symbolizes Jaccardized Czekanowski index, h denotes a hash generated at registration, h_n denotes a hash generated at login phase. $h \cap h_n$ denotes a mutual dependence between the two hash, $\sum h$ is the sum of$h$ score, $\sum h_n$ is the sum of h_n score.

$$\delta = \begin{cases} 1 \ ; patient\ is\ authorized \\ 0 \ ; patient\ is\ unauthorized \end{cases} \qquad (8)$$

3.1.1 Secured Data Transmission

In this process, the two entities are considered such as sender and receiver. The sender transmits the data in ciphertext to receiver. Let us consider the number of data $D_1, D_2, D_3, \dots . D_m$. Then the encryption of data is obtained as follows,

$$C(D) = D^{\alpha_{p\,(r)}} \ mod\ \alpha_{p\,(r)} \qquad (9)$$

Where, $C(D)$indicates ciphertext which is obtained based on receiver public key '$\alpha_{p\,(r)}$' and original data 'D'. Subsequently, the digital signature is generated by sender's private key. Consider the input data are converted into a message bit $V_i \in [0, 1]$. The digital signature is generated as given below,

$$S_i(s) = H \ \langle \beta_{r\,(s)} | V_i \rangle \qquad (10)$$

From (10), signature '$S_i\ (s)$ 'is generated by '$\beta_{r\,(s)}$', hash H and message bit 'V_i'. The ciphertext of data with the signature is transferred to receiver.

3.1.2 Unsigncryption

Unsigncryption process is performed for achieving original patient data at receiver (i.e. physician). It comprises two major processes as signature verification and decryption. The signature of the received data is generated with same hash function at time of signcryption

$$S_i(r) = H \ \langle \alpha_{p\,(s)} | V_i \rangle \qquad (11)$$

Where, $S_i(r)$ indicates a signature generated at the receiver with senders public key '$\alpha_{p\,(s)}$'. Finally, generated signature is matched by Tversky similarity coefficient. The coefficient is used to measure the association between the two variables (i.e. signatures). The correlation between the two signatures is verified as a given blow,

$$\omega = \frac{S_i(s) \cap S_i(r)}{A(\,S_i(s) \,\Delta\, S_i(r)) + \ B(\,S_i(s) \cap S_i(r))} \qquad (12)$$

From (12), ω indicates a similarity coefficient, $S_i(s)$ signifies the signature generated at the sender side, $S_i(r)$ indicates signature, $S_i(s) \cap S_i(r)$ indicates a mutual dependence between the two signatures, $and\ S_i(s) \,\Delta\, S_i(r)$ indicates a variance between the signatures. From (12), A and B indicate parameters of the Tversky index ($A, B \geq 0$). Similarity coefficient (ω) gives value of [0, 1]. High similarity indicates two signatures were correctly matched and signature is valid. Thus, signatures are verified. Otherwise, the signature is not valid and the receiver did not decrypt the ciphertext. The decryption is achieved using receiver's private key $\left(\beta_{r\,(r)}\right)$ by

$$D = C(D)^{\beta_{r\,(r)}} \ mod\ mn \qquad (13)$$

Where 'D' indicates an original data, $C(D)$ indicates a ciphertext, $\beta_{r\,(r)}$ indicates a receiver's private key, m, and n indicate large prime numbers.Secured communication between the patient and the cloud server is performed. If the entered receiver's private key is incorrect, proposed JCISDFO-KSSCS generates an additional key (i.e. secret key). A secondary secret key is many security questions that are generated at the time of registration. It helps to increase the security and storage costs of the key generation. In order to minimize the storage costs, an optimal number of security keys are selected. Based on fitness, an optimal question is selected among population to minimize the storage cost. Initialize population of 'n' artificial fish swarms (i.e. number of security questions) $Q = q_1, q_2, q_3, \dots . q_w$ randomly. Fitness is calculated on storage space. It is defined as amount of storage space required to store the keys. Storage space is calculated as follows

$$M_c = M_t - M_u \qquad (14)$$

Where, M_c represents the storage cost, $M_t$represents a total memory space and $M_u$denotes a consumed memory space. The fitness is measured based on the storage cost. In the fitness measure, the proposed optimization technique employs gradient descent function for analyzing fittest among population based on minimum storage cost.

$$F = arg\ min(M_c) \qquad (15)$$

Where F denotes a fitness, $arg\ min$ denotes a gradient descent function. Based on the fitness value, three behaviors of the artificial fish positions such as search or prey, swarm, and follow are carried out as follows,

3.1.3 Follow behavior of fish

Follow behavior is executed that neighborhood X_j state has a higher food concentration than the position X_i . Follow behaviors of artificial fishes are formulated as follows.

$$X_i(t+1) = X_i(t) + c * d * \left(\frac{(X_{max}-X_i)}{\|X_{max}-X_i\|}\right) \quad (16)$$

Where, $X_i(t+1)$ denotes an updated position of fish, $X_i(t)$ is the current position, X_{max} denotes a position having best fitness function, $c$indicates a random number varied from zero to one $(0 < c < 1), d$ denotes a step of the fish moving which is a random positive number, $\|X_{max} - X_i\|$ indicates visual distance among position of 'i' fish and central position of fish having maximum fitness 'X_{max}' function. Security of patient data transmission was performed with minimum computation cost. Algorithmic process of JCISDFO-KSSCS is described as given below,

```
// Algorithm 1: Jaccardized Czekanowski Indexive Steepest Descent Fish Optimization Based Kupyna Schmidt-Samoa Certificateless Signcryption
Input: patients $p_1, p_2, p_3, \dots . p_n$ and healthcare data $D_1, D_2, D_3, \dots . D_m$
Output: Secured Data Transmission
Begin
For each patient '$p$'
    Enter the patient details and send to '$server$'
The server generates the pair of keys
end for
    For each patient details
Generate hash using Kupyna single-block-length compression function
End for
 User login into the system with keys
Server verifies hash using a Jaccardized Czekanowski index
if $(\delta = 1)$ then
The patient is said to be an authorized
      Grant the access
    else
The patient is said to be an unauthorized
      Access denied
end if
```

4. EXPERIMENTAL SCENARIO

Simulation of JCISDFO-KSSCS and SSA model [1], IECC [2] are implemented using MATLAB-SIMULINK tool using heart disease dataset collected from https://www.kaggle.com/sulianova/cardiovascular-disease-dataset

5. RESULTS AND DISCUSSION

The performance outcomes are compared using different parameter as authentication accuracy, confidentiality rate, computational cost, and storage cost.

5.1 Performance Analysis of Authentication Accuracy

It is measured as ratios of a number of patients are correctly verified by authorized or unauthorized to entire number of patients. It is measured using following equation,

$$A_{Acc} = \left[\frac{Numberof\ patients\ correctlyauthenticated}{Number\ of\ patients}\right] * 100 \quad (17)$$

In (*17*), A_{Acc} denotes authentication accuracy, 'n' indicates number of patients. It is calculated by percentages (%).

Table 1: Authentication accuracy versus number of patients

Number of patients	Authentication Accuracy (%)		
	JCISDFO-KSSCS	SSA model	IECC
5000	95	90	88
10000	94	89	87
15000	95.33	90	88
20000	93.5	89	86.5
25000	94.4	90	87.2
30000	95	88.33	85.33
35000	96	89.14	86.28
40000	94.5	88.75	86.25
45000	96	89.33	85.77
50000	95.2	90.4	87.6

Table 1 reports the performance analysis of authentication accuracy versus number of patients. Authentication accuracy using JCISDFO-KSSCS is enhanced as 6% and 9 % compared to [1] and [2].

5.2 Performance Results of Confidentiality Rate

It is defined by number of patient data that are protected by unauthorized access to entire number of patient data. It is calculated as given below,

$$C_{DR} = \left(\frac{NDP}{n}\right) * 100 \quad (18)$$

In (20) C_{DR} symbolize the data confidentiality rate, NDP represents the number of data protected, n indicate total number of data. It is calculated by percentage (%).

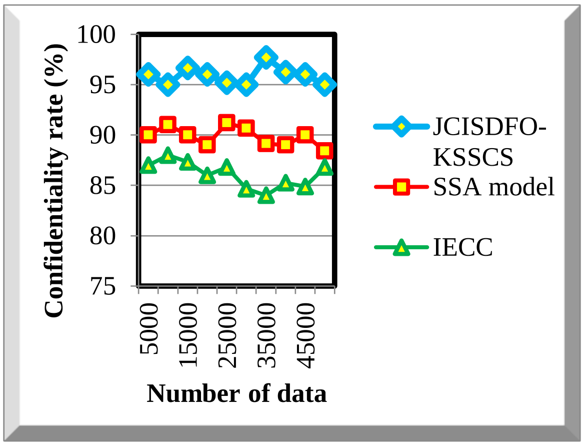

Figure 1: Graphical illustration of the data confidentiality rate

Figure 2 portrays data confidentiality rate versus numbers of patient data. Data confidentiality rate of JCISDFO-KSSCS was improved as 7% and 11% compared with SSA model [1], IECC [2]

5.3 Performance Results of Computational Cost

Computational cost is referred by number of time consumed for achieving secure communication. Computational cost is measured as follows,

$$CC = n * ti[ST_o] \quad (19)$$

From *(19)*,CC denotes computational cost, 'n' indicates number of patient data, and '$ti[ST_o]$' indicates time consumed for secure transmission of one patient data. It is calculated by milliseconds (ms).

Table 2. Computational cost versus number of patients

Number of data	Computational Cost (ms)		
	JCISDFO-KSSCS	SSA model	IECC
5000	19	22.5	25
10000	25	28	31
15000	30	34.5	39
20000	34	40	46
25000	40	45	50
30000	45	51	54
35000	50.75	56	63
40000	55.2	60	68
45000	61.2	66.6	69.75
50000	66	70	75

Table 2 reports the performance of computation cost using proposed JCISDFO-KSSCS, existing SSA model [1], IECC [2]. Computation cost is significantly reduced as 11% and 19% compared with [1] and [2] respectively.

5.4 Performance Results of Storage Cost

Storage cost is measured by number of space taken to store keys such as private, public, and secret keys. Storage cost calculated in terms of kilobytes (KB) Storage cost is given

$$Cost_{St} = Number\ of\ patients * space\ (\beta_r + \alpha_p + S_{key})\ (20)$$

By using (20), $Cost_{St}$ denotes a Storage cost. β_r indicates private key, α_p indicates public key, S_{key} indicates secret key.

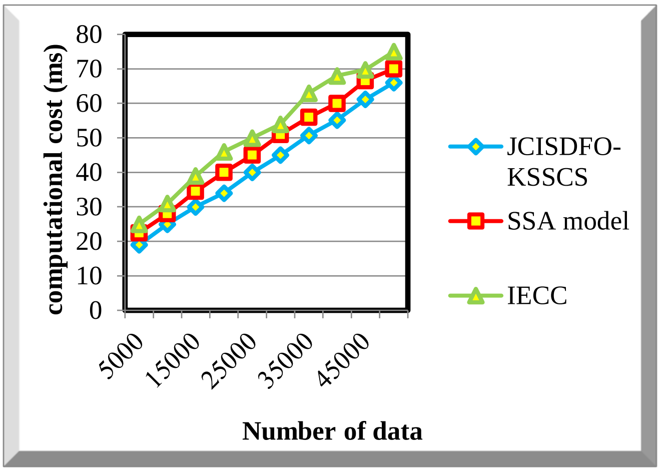

Figure 2. Graphical illustration of the computation cost

Figure 2 gives storage cost versus number of patients. Storage cost is minimized using JCISDFO-KSSCS by 8% and 15% than the conventional methods.

6. CONCLUSION

Security of IoT plays a vital role to multi-application nature. JCISDFO-KSSCS of security assessment is utilized to IoT devices in healthcare environment. Proposed methodology provides higher level of authentication accuracy, confidentiality rate, and minimum computation cost, storage cost than the conventional approaches.

REFERENCES

[1] B.D. Deebak and Fadi Al-Turjman, "Smart Mutual Authentication Protocol for Cloud-Based Medical Healthcare Systems Using Internet of Medical Things", IEEE Journal on Selected Areas in Communications, Vol. 39, Issue 2, 2021.

[2] Sarath Sabu, H.M. Ramalingam, M Vishaka, H.R. Swapna, Swaraj Hegde, "Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain", Global Transitions Proceedings, Elsevier, Volume 2, Issue 2, November 2021, Pages 429-433.

[3] Muhammad Azeem, Ata Ullah, Humaira Ashraf, NzJhanjhi Mamoona Humayun, Sultan Aljahdali, And Thamer A. Tabbakh, "FoG-Oriented Secure and Lightweight Data Aggregation in IoMT", IEEE Access, Volume 9, 2021, Pages 111072 – 111082.

[4] Rui Guo, Geng Yang, Huixian Shi, Yinghui Zhang, and Dong Zheng, "O3-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System", IEEE Internet of Things Journal, Volume 8, Issue 11, 2021, Pages 8949 – 8963.

[5] Junaid Hassan,Danish Shehzad Insaf Ullah, Fahad Algarni, Muhammad Umar Aftab, Muhammad Asghar Khan, and M. Irfan Uddin, "A Lightweight Proxy Re-Encryption Approach with Certificate-Based and Incremental Cryptography for Fog-Enabled E-Healthcare", Security and Communication Networks, Hindawi, Volume 2021, November 2021, Pages 1-17.

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

[7] Mahender Kumar and Satish Chand, "A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System with Public Verifiability", IEEE Internet of Things Journal, Volume 7, Issue 10, 2020, pp. 10650 – 10659.

[8] Lanjing Wang; Yasir Ali; Shah Nazir; Mahmood Niazi, "ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods", IEEE Access, Volume 8, 2020.

[9] Samira Akhbarifar, Hamid Haj SeyyedJavadi, Amir Masoud Rahmani& Mehdi Hosseinzadeh, "A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment", Personal and Ubiquitous Computing, Springer, 2020, Pages 1-17.

[10] Lanjing Wang; Yasir Ali; Shah Nazir; Mahmood Niazi, "ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods", IEEE Access, Vol. 8, 2020, pp. 152316 – 152332.

[11] Ding Li, Wang Zhongsheng, Wang Xiaodong, Wu Dong, "Security information transmission algorithms for IoT based on cloud computing", Computer Communications, Elsevier, Volume 155, 2020, Pages 32-39.

[12] Dankan Gowda V, K. R. Swetha, Namitha A R, Manu Y M, Rashmi G R and Veera Sivakumar Chinamuttevi (2022), IOT Based Smart Health Care System to Monitor Covid-19 Patients. IJEER 10(1), 36-40. DOI: 10.37391/IJEER.100105.