Management of Public Health: A Study on Novel Strategy for Securing Health Data

Sandeep Soni[1], Rajvir Saini[2]

[1]*Assistant Professor, Department of Management, Kalinga University, Raipur, India. Email: ku.sandeepsoni@kalingauniversity.ac.in ORCID:0009-0000-3692-6874*

[2]*Assistant Professor, Department of Management, Kalinga University, Raipur, India. Email: ku.rajvirsaini@kalingauniversity.ac.in ORCID: 0009-0000-6644-0795*

KEYWORDS

Public Health, Internet Of Medical Things (Iomt), War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC), Health Management Systems, Smart Healthcare

ABSTRACT

The effective management and security of sensitive health data is becoming exponentially important to public health administration. This research examines and evaluates innovative ways to improve health data security in public health management systems to provide accessibility for authorized stakeholders. The study introduces the War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC) encryption method for improving the security of primary healthcare medical records. The WSO-ECC technique, based on a war strategy framework, optimizes encryption and decryption processes by balancing exploration and exploitation phases, enhancing security while maintaining efficiency. It significantly reduces encryption and decryption times compared to traditional methods.The proposed method offers a robust solution for safeguarding medical information in public health management systems, demonstrating superior performance of 24.6 in encryption time, 23 decryption times, execution efficiency, and delay.

1. Introduction

Community and township health centers provide traditional public health services, involving the administration of medical information [1], public health situations of emergency, transmissible diseases, learning, chronic illness people, maternal and child health, geriatric health, and healthcare monitoring. Essential healthcare establishments must have a public health database of information [2] to integrate health records and service records, ensuring a unique, lifelong health record for each resident. Information technology can significantly improve the efficiency and completeness of essential public health services for residents or migrants [3]. The Internet of Things (IoT) is crucial in various fields like healthcare, mining, and agriculture, necessitating a green solution to tackle challenges in IoT-based [14] smart healthcare. An environmental approach is required to solve issues in IoT-based smart healthcare initiatives [5] as it transforms physical care by gathering and transferring data to a cloud repository [7]. Cyber-physical systems (CPS) are utilized in public services, particularly in healthcare, to improve medical care quality and reduce healthcare costs [6]. IoMT medical technologies include wearable, in-home, and point-of-care (POC)devices for real-time health monitoring, enabling real-time processing and analysis of [15] patients' health data. Digital healthcare is revolutionizing standard monitoring by enabling cloud products and automated detection technologies, [8] similar to POC devices providing cloud storage and internet access. Figure 1 represents the overview of public health management.The goal of the research is to better understand War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC), a revolutionary approach to improving security and efficiency while protecting health data in public health management systems [4].

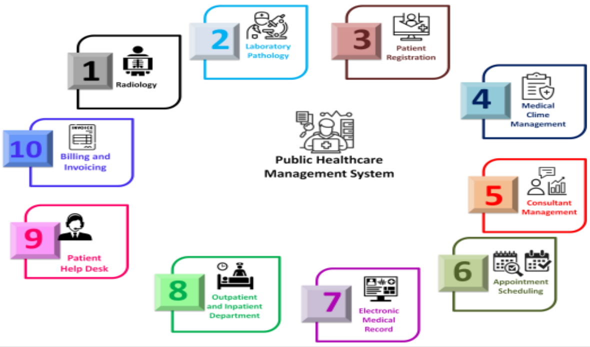

Figure 1. Overview of public health management

2. Literature Review

Thilagam et al. [9] proposed IoT-based Deep learning (DL) algorithms for data analytics and privacy protection. For IoT medical institutions, they created a secure authentication module by evaluating fitness related data stored in the cloud. The solution was deemed credible and productive, as seen by 98% accuracy rating. Seh et al.[16] investigated healthcare data breaches and found that the most frequent types of attacks are IT incidents and hacking. Simplified moving average forecasting is more accurate than exponential soothing forecasting when it pertains to analyzing expenses and trends in the research. Using a hybrid deep neural network (DNN) system and binary spring search approach, Ali et al. [11] established an innovative group theory (GT). For safe monitoring and keyword-based dataset access, the block chain served as a distributed database [10]. In addition to modified rules, the technique offered a secure crucial revocation method. IoT and cloud computing were the main tools employed by Anuradha et al. [12] to construct a cancer prediction system. Doctors and nurses can easily access the extracted, encrypted, and cloud-stored blood results. The solution gave cancer patients security and authentication while streamlining healthcare computations and processing.

3. Methodology

The purpose of this study is to develop and assess a novel encryption approach that strengthens the security of healthcare data while maintaining high efficiency in IoT based healthcare software networks.

Data Collection

10,000 records from the primary IoT application were gathered based on healthcare dataset for this investigation, each of which represents an authentic patient healthcare record. It includes details regarding the patient's condition, demographics, and enrollments, among other things. The dataset is meant to be used for private, instructional uses. It is completely artificial and does not include actual patient information.

War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC)

The study evaluates War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC), an advanced cryptographic method that leverages strategic planning to improve performance and attack resistance while enhancing the security of IoT-based healthcare datasets by combining manipulation, flexibility, and unpredictability.

War Strategy Optimization

In war strategy, there are three main groups: King node performance is the decision making and security control of the entire network. Commander node, manage the security and ensure balance between the security of efficiency and soldiers performance is influenced by the quality of encryption keys, which balance exploration and exploitation for optimal key discovery. Both commanders and monarchs are in charge of managing their armies according to their fighting prowess. Every soldier has the potential to rise to the position of commander or king at, any given time. Leaders may face powerful rivals, but they are supervised on collective motion strategies and guided by the commander or king's situation to prevent potential traps.

Attack Tactic: The commander and the king's circumstances influence the places of the troops in the first strategy, where the king is the one with the strongest offensive force. As they use the technique, their rank rises, and if they are effective, their positions are renewed. The locations of the troops, commander, and king get closer as the fight continues on.

Renewing weight and rank: The ranking of soldiers in their prosperous past has affected their trajectory of conflict, overshadowing the $X_j$factor, are determined in equation (1). The encryption key of each soldier indicates their closeness to the goal. The offered optimizer experiences exponential variation in weight, with soldiers taking the previous situation if it's greater.

$$X_j = X_j \times (1 - \frac{Qb_j}{Max\_iter})^{\beta} \qquad (1)$$

Strategy of defense: The King, anerratically selected warrior, and the commandant scenario form the basis of the second strategy for restarting the scenario. In order to include warriors in greater quantities, the war policy broadens its search regions, and $z_j$in smaller amounts, the opposite is true, are shown in equation (2).

$$z_j(s+1) = z_j(s) + 2o(z_L - z_{ran}(s)) + rand \times X_j(z_d - z_j(s))(2)$$

Replacing the weak soldier: The weak soldier with the worst cost function value is identified and replaced using various strategies, with the easiest being a random replacement. Equation (3) determined the second strategy involves replacing weak soldiers with the standardentire army in the ground, resulting in improved optimizer convergence.

$$z_x(s+1) = z_L - (1 - rand) \times (z_X(s) - median(z)) \qquad (3)$$

Salient characters of the obtainable optimizer: Balances security exploration and efficiency phases, each soldier's weight is based on encryption key.Weight renewal is based on cost-value improvement over the renewal stage. Weight variation is nonlinear, with large variations in early epochs and small variations in last epochs.The renewing process includes two steps, improving exploration capability. The optimizer is simple and requires less calculation.

The phases of development and investigation: The proposed optimizer combines utilizationin network development and communication phases, focusing on attack and security tactics, with other factors influencing its effectiveness and performance.The $rand$ parameter determines thesoldier's exploration or exploration-oriented movements. The $'pr'$ parameter allows flexibility in choosing values based on thecost function. The search individual's direction and weight are adaptive, with small values adapted for low cost soldiers and high values for high cost soldiers.

Elliptic Curve Cryptography

The method uses a competitive imperialist approach to generate an ideal key, enhancing medical records security and reducing data loss through hybrid encryption and decryption. The ECC algorithm, which is comparable to asymmetric key cryptography, is used to accomplish public key cryptography. Based on the initial points and the maximum limit of the prime factorization function, an equation of ECC is obtained. This is followed by the evaluation of an encryption function;J and I are constants in this equation (4) of the ECC, and the value of$J = I = 2$.

$$F = [PRIMER(L)]^3 + J \times PRIMER(L) + I \qquad (4)$$

Generation of key: An important part of the encryption procedure, depending on the cryptographic function, is key generation. The public key, which is acquired from the recipient side, is created as the initial stage in the encryption process as represented in equation (5). The receiver side's private or secret key generation for the decoding procedure comes next. When A_{en} represents in equation (6) the initial position of the curves, $G_{opt}$is the chosen random integer to $m - 1$ in the range of 1, and O is the general key. $G_{opt}$is also designated as the optimum private key.

$$O = G_{opt} \times A_{en} \qquad (5)$$

$$A_{en}\ and\ G_{opt} \qquad (6)$$

Encryption Process: The encryption procedure is used to encrypt each block, and the total number of blocks is indicated by the notation$M(i, and\ j)$, where i and j stand for the row and column of image blocks. The following equations (7) and (8) express the pixels ($Q_h(i,j)$ and$Q_g(j+1,i)$, as well as their associated points.

$$F_1 = G_{opt} \times A_{en} \quad (7)$$

$$F_2 = (Q_h, (Q_g) + F_1 \quad (8)$$

Decryption Process: The receiver side of the message's decryption operation uses the secret passwordG_{opt}. Pixel points are decrypted by pointF_3, and the following equations (9) and (10) provide the final outcomes of the decryption procedure$F_{j,i}$.

$$F_3 = (G_{opt} \times F_1 \quad (9)$$

$$F_{j,i} = (F_2 - F_3) \quad (10)$$

$$A_y = A1\ XOR\ A_2 XOR\ A_3 XOR\ A_4 XOR\ key \quad (11)$$

Subsequently, the output decrypted picture is simultaneously stored to get the original medical consideration which is calculated using equation (11).

An adapted encrypting technique called WSO-ECC intends to increase the effectiveness and security of managing public health data. It makes use of ECC's strong security with reduced key sizes, enhancing performance, management and encryption algorithms to safeguard private health information, conform to privacy regulations, and guarantee data integrity.

4. Results And Discussion

In this section, this section compares the proposed method with various traditional approaches, including Advanced Encryption Standard (AES) [13], group theory (GT)-based binary spring search (BSS) (GT-BSS) [13], and Lionized remora optimization-based serpent (LRO-S) [13], based on factors including decryption time and encryption time, execution time, and delay.

Encryption Time

The recommended approach determines the conservative methods for data of varying dimensions, with anefficient faster encryption time than the present representation, demonstrating that the method receives longer as the data size increases. Table 1 depicts the evaluation of encryption time.The estimated time essential to encryption is contrasted with the existing models in Figure 2.

$$Encryption\ time = \frac{overall\ \ encrypted\ plain\ data}{Time} \quad (12)$$

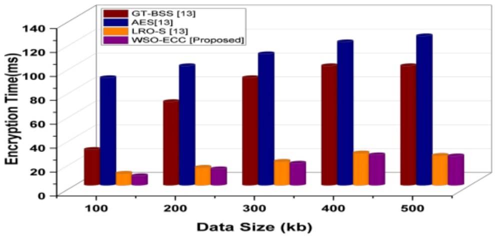

Figure 2. Comparsion of encryption time

Table 1. Numerical evalution of encryption time

Data size(kb)	**GT-BSS [13]**	**AES[13]**	**LRO-S [13]**	**WSO-ECC [Proposed]**
100	30	90	10	8
200	70	100	15	13.8

300	90	110	20	18.5
400	100	120	27	25.5
500	100	125	25	24.6

Decryption Time

Figure 3 corresponded with the recommended decryption time for the encryption data, indicating that the data size increases, so does the decryption time. The recommendation for strategy outperforms traditional methods for a variety of dimensions of record and offers several advantages, including faster data decoding time compared to prior approaches. Table 2 depicts the evaluation of decryption time.

$$Decryption\ time = \frac{Overall\ decrypted\ cipher\ data}{Time} \qquad (13)$$

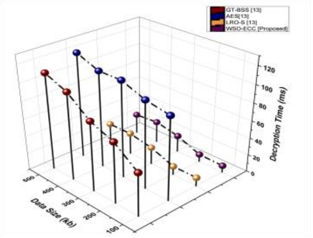

Figure 3. Comparsion of decryption time

Table 2. Numerical evalution of decryption time

Data size(kb)	GT-BSS [13]	AES[13]	LRO-S [13]	WSO-ECC [Proposed]
100	50	95	10	7.9
200	70	100	10	8.7
300	80	110	20	19.4
400	100	110	25	25
500	110	120	25	23

Execution Time and Delay

The suggested data security paradigm for smart healthcare management is extremely scalable and offers secure storage and accessibility for scattered medical information. Figures 4 (a) and 4 (b) illustrate how the model outperforms earlier approaches as a result of execution time and average delay.

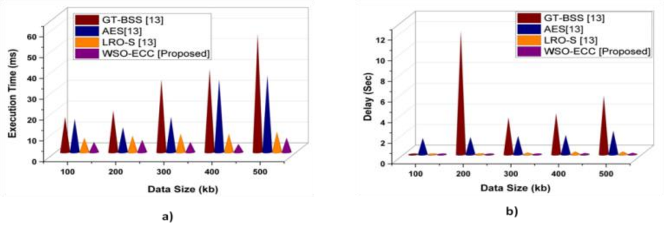

Figure 4. Comparison of execution time b) Comparison of delay

5. Conclusion

The work presents a state-of-the-art encryption technique for protecting health data in public health management systems called War Strategy Optimized Elliptic Curve Cryptography (WSO-ECC). WSO-ECC improves efficiency and strengthens the security of medical records by using the primary healthcare dataset. Its creative strategy enhances encryption and decryption procedures by striking a balance between the exploration and exploitation stages. WSO-ECC is a potential option for contemporary public health data management as it offers better safety for health data and significantly reduces down on encryption and decryption times when compared to conventional cryptographic techniques.

Reference

[1] Y. Zhao, L. Liu, Y. Qi, F. Lou, J. Zhang, and W. Ma, "Evaluation and design of public health information management system for primary health care units based on medical and health information," Journal of infection and public health, 13(4), pp.491-496, 2020. https://doi.org/10.1016/j.jiph.2019.11.004

[2] S. Wolf-Fordham, "Integrating government silos: Local emergency management and public health department collaboration for emergency planning and response,"The American Review of Public Administration, 50(6-7), pp.560-567,2020. https://doi.org/10.34172%2Fhpp.2020.30

[3] I. Keshta, and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges", Egyptian Informatics Journal, 22(2), pp.177-183, 2021.

[4] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[5] K.K. Baseer, K. Sivakumar, D. Veeraiah, G. Chhabra, P.K. Lakineni, M.J. Pasha, R. Gandikota, and G. Harikrishnan, "Healthcare diagnostics with an adaptive deep learning model integrated with the Internet of medical Things (IoMT) for predicting heart disease," Biomedical Signal Processing and Control, 92, p.105988, 2024.

[6] F. Chen, Y. Tang, C. Wang, J. Huang, C. Huang, D. Xie, T. Wang, and C. Zhao, "Medical cyber–physical systems: A solution to smart health and the state of the art," IEEE Transactions on Computational Social Systems, 9(5), pp.1359-1386, 2024.

[7] Sonya, A., & Kavitha, G. (2022). A Data Integrity and Security Approach for Health Care Data in Cloud Environment. Journal of Internet Services and Information Security, 12(4), 246-256.

[8] M. Sekar, R. Sriramprabha, P.K. Sekhar, S. Bhansali, N. Ponpandian, M. Pandiaraj, and C. Viswanathan, "Towards wearable sensor platforms for the electrochemical detection of cortisol," Journal of The Electrochemical Society, 167(6), p.067508.

[9] K. Thilagam, A. Beno, M.V Lakshmi, C.B. Wilfred, S.M. George, M. Karthikeyan, V. Peroumal, C. Ramesh, and P. Karunakaran, "Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System," Journal of Nanomaterials, (1), p.2638613,2022.

[10] Mohamed, K.N.R., Nijaguna, G.S., Pushpa, Dayanand, L.N., Naga, R.M., & Zameer, AA. (2024). A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15(2), 94-108. https://doi.org/10.58346/JOWUA.2024.I2.007

[11] A. Ali, M.A Almaiah, F. Hajjej, M.F. Pasha, O.H. Fang, R. Khan, J. Teo and M. Zakarya, "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network,"Sensors, 22(2), p.572, 2022.

[12] M. Anuradha, T. Jayasankar, N.B. Prakash, M.Y. Sikkandar, G.R. Hemalakshmi, C. Bharatiraja, and A.S.F. Britto, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," Microprocessors and Microsystems, 80, p.103301, 2021.

[13] A. Almalawi, A., A.I. Khan, F.Alsolami, Y.B . Abushark and A.S. Alfakeeh "Managing security of healthcare data for a modern healthcare system," Sensors, 23(7), p.3612, 2023.

[14] Ishrat Zahan Mukti, Ebadur Rahman Khan, and Koushik Kumar Biswas, "1.8-V Low Power, High-Resolution, High-Speed Comparator With Low Offset Voltage Implemented in 45nm CMOS Technology", JVCS, vol. 6, no. 1, pp. 19–24, Dec. 2023.

[15] Z.N. Aghdam, A.M. Rahmani, and Hosseinzadeh, "The role of the Internet of Things in healthcare: Future trends and challenges," Computer methods and programs in biomedicine, 199, p.105903, 2021.

[16] P. Manickam, S.A. Mariappan, S.M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S.P. Thipperudraswamy, "Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare," Biosensors, 12(8), p.562, 2022.

[17] A.H. Seh, M. Zarour, M. Alenezi, A.K. Sarkar, A. Agrawal, R. Kumar, and R. Ahmad Khan," Healthcare data breaches: insights and implications, "In Healthcare (Vol. 8, No. 2, p. 133). MDPI. 2020, May.https://doi.org/10.3390/healthcare8020133