Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1723–1731
DOI : 10.47974/JDMSC-2172

Design and implementation of secure cryptographic algorithms for wireless sensor networks in healthcare applications

Rohini Kale [†]
Department of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Ajjay S. Gaadhe *
Department of Electronics and Telecommunication
PCET's Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Navnath B. Pokale [§]
Department of Computer Engineering
TSSM's Bhivarabai Sawant College of Engineering and Research
Pune 411044
Maharashtra
India

Prashant Ashok Patil [‡]
Department of Mechanical Engineering
Dr. D. Y Patil Institute of Technology
Pune 411018
Maharashtra
India

[†] *E-mail:* rohini.kale@mitwpu.edu.in
* *E-mail:* ajay.gadhe@pccoepune.org (Corresponding Author)
[§] *E-mail:* nbpokale@gmail.com
[‡] *E-mail:* prashant.p@dypvp.edu.in

Pradnya Borkar [@]
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Pune 440008
Maharashtra
India

Satyajit Sidheshwar Uparkar [#]
Department of Computer Science and Applications
Ramdeobaba University
Nagpur 440013
Maharashtra
India

Abstract

Wireless sensor systems (WSNs) are exceptionally vital for collecting information and following in genuine time in healthcare employments that are changing rapidly. But since healthcare information is private, solid security steps are required to ensure persistent security and make beyond any doubt information exactness. This ponder talks approximately how to form secure cryptographic strategies that work with WSNs in healthcare settings and how to put them into activity. We recommend a light encryption strategy that strikes a adjust between security and the constrained computing control and vitality that are common in WSNs. Our arrange incorporates a good key administration framework that produces beyond any doubt that contact between sensor hubs and with central information servers is secure. We moreover utilize a two-layer encryption framework that employments symmetric and deviated cryptography to secure against numerous sorts of assaults, such as information robbery and tuning in in on discussions. Broad models and real-world utilize in a healthcare setting are used to test the proposed strategies. Execution measures just like the speed of encryption and interpreting, the sum of vitality utilized, and the sum of memory utilized are looked at to appear that our approach works and is effective. The comes about appear that our cryptographic strategies offer a tall level of security whereas still being able to work rapidly and effectively sufficient for real-world healthcare employments. Since of this work, secured WSNs are getting superior, which suggests healthcare frameworks will be more secure and more viable.

Subject Classification: *68M10.*

Keywords: *Cryptographic algorithms, Wireless sensor networks (WSNs), Healthcare applications, Data security, Encryption techniques, Authentication protocols, Secure data transmission.*

[@] *E-mail:* **pradnyaborkar2@gmail.com**
[#] *E-mail:* **uparkarss@rknec.edu**

1. Introduction

Wireless sensor systems (WSNs) have changed healthcare by permitting real-time information collection and consistent following [1]. This has made it simpler to care for and control patients. Sensor hubs spread out totally different regions of the body collect imperative information like heart rate, blood weight, and body temperature and send it to central computers to be analyzed [2]. Since WSNs are utilized in healthcare, modern apps have been made for things like following patients from a far distance, overseeing unremitting illnesses, and setting up crisis reaction frameworks [3], [4]. But the delicate nature of the information being assembled and the reality that screen hubs do not have a part of assets make security exceptionally difficult. Unauthorized get to, changing information, and tuning in in on discussions can all cause protection breaches and put patients at hazard [5], [6]. Solid cryptographic strategies are required to secure the security, security, and legitimacy of information in these networks. This article looks at how to make and utilize secure security strategies that are made to work with WSNs in healthcare settings [7]. Since sensor hubs do not have a part of computing control or vitality, the recommended strategies are little and solid sufficient to ensure against a wide extend of security dangers [8]. We illuminate the special issues of overseeing keys and communicating safely in WSNs by making a speedy and secure framework that lets hubs swap cryptography keys. Our two-layer encryption method too employments the finest parts of both symmetric and halter kilter cryptography to donate you a total security reply. Through cautious testing of their execution, we appear that our recommended calculations meet the strict security needs of healthcare applications whereas still being able to run productively.

2. System Architecture Design

Making a total stage for the Wireless sensor organize (WSN) in healthcare employments is portion of the framework design plan [9]. There are monitor nodes, transmission strategies, and central computers within the figure 1. These hubs communicate wirelessly with each other and the central server, shaping a organize topology that can be modelled as a chart G = (V, E), where V speaks to the set of sensor hubs and E indicates the set of communication joins.

The plan incorporates numerous parts, such as information accumulation, secure directing, and blame resilience, to keep information secure and communication running easily. Differential conditions can be utilized to demonstrate the communication prepare and appear how information exchange and gathering alter over time [10].

$$\frac{dD_i(t)}{dt} = -\sum_{j \in N(i)} R_{ij}(t) + I_i(t)$$

where D_i (t) is the information at hub i at time t, R_ij (t) speaks to the information rate from hub i to hub j, and I_i (t) signifies the input information rate from outside sources. The vitality utilization demonstrate is additionally clarified by including up the control utilize over time:

$$E_i = \int_0^T P_i(t)dt$$

- where E_i is the entire sum of vitality that hub i utilized amid the time period T and P_i (t) is the sum of control that hub i utilized at time t.

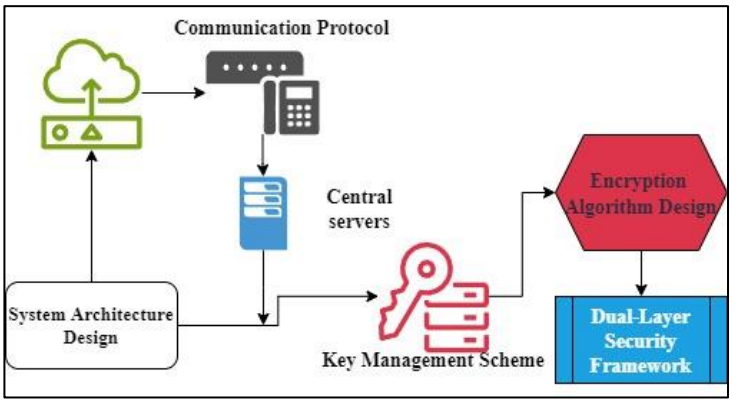

Figure 1
Overview of system Architectural Block Diagram of proposed system

2.1 Key Management Scheme

For healthcare employments, the key administration strategy is exceptionally imperative for keeping discussions secure and secure in a Wireless sensor arrange (WSN) [11]. The demonstrate makes beyond any doubt that key exchanges are secure whereas utilizing as small computing control and vitality as conceivable. A work ($f: S \times R \rightarrow K$) is utilized to begin secure communication. In this work, S may be a shared secret between endorsed hubs, R may be an arbitrary number, and K is the encryption key that's made. The following expression can be utilized to portray the method:

$$K = f(S, R)$$

$$K_{ij} = p_i \cdot P_j = p_i \cdot (p_j \cdot G)$$

Since WSNs are continuously changing, the method of re-establishing keys is depicted by a time-dependent work (R(t)) that upgrades keys on a normal premise:

$$R(t) = R_0 + \int_0^t \frac{dR}{dt} dt$$

where R_0 is the arbitrary number that begins out and $\frac{dR}{dt}$ is the rate of alter. After that, the modern key K' is made as

$$K'(t) = f(S, R(t))$$

2.2 *Encryption Algorithm Design*

A key portion of making beyond any doubt that information is kept private and redress in a Wireless sensor arrange (WSN) for healthcare employments is

the encryption strategy [12]. For speed and security, the program employments a blended strategy that combines symmetric and deviated cryptography. The Progressed Encryption Standard (AES) with a square estimate of 128 bits is utilized for symmetric encryption. The encryption handle can be spoken to by the work ($E: K\_s \times M \rightarrow C$),where (K_s) is the symmetric key, M is the plaintext message, and C is the ciphertext:

$$C = E_{K_s}(M)$$

Elliptic curve cryptography (ECC) is used for asymmetric encryption, which makes it safe for nodes to share the symmetric key K_s. As shown in the symbol (P, p), a node's public and private keys are written as (P, p). Here, P = p.G and G is a generator point on the elliptic curve. The public key of the receiver P_j is used to encrypt the session key K_s:

$$K_s' = E_{P_j}(K_s) = K_s \cdot P_j$$

In order to make the encryption process safer, we add a time-based component. The key that changes over time, K_t, is made by: $K_t = f(K_s, t)$ where t is the time right now.

$$HMAC = H(K_s | M)$$

- where H stands for a safe hash function and (|) means to join two or more things together.

3. Dual-Layer Security Framework

Key administration and encryption strategies are both portion of the dual-layer security structure, which ensures all information sent over WSNs for healthcare apps. Within the to begin with layer, symmetric encryption is utilized to keep data secure, and within the moment layer, deviated cryptography is utilized to securely share keys and confirm characters. Differential conditions and integration can be utilized together to depict the security show and appear how secure information streams. Let D(t) speak to the information transmitted at time t, and (E_(K_s) D(t)) signify the scrambled information employing a symmetric key K_s. The scrambled information stream rate is modelled as:

$$\frac{dD_e(t)}{dt} = \frac{\alpha\, dD(t)}{dt}$$

where α is the factor that measures how well the encryption works. To prove who sent the message, the ECC-based digital signature method uses the sender's private key (p) to create a signature (S) for it (M):

$$S = Sign_p(M)$$

For this signature to be valid, the receiver must use the sender's public key (P), which is shown by the verification function (V):

$$V(M,S) = \begin{cases} Valid, & if\ S = Sign_p(M) \\ Invalid, & otherwise \end{cases}$$

This multi-layered method protects both the privacy and integrity of the data, making it a strong security option for healthcare WSNs.

4. Result and Discussion

By comparing the suggested encryption algorithms to RSA, normal AES, and ECC, the compared study shows their pros and cons which is illustrated in table 1. The suggested method is more computer-friendly, requiring less energy and time to secure and decrypt data. The use of ECC and dual-layer encryption gives it a high level of security of its own. But the methods for managing keys and renewing them are a little more complicated.

Table 1

Comparative Analysis of Cryptographic Solutions

Metric	Proposed Algorithm	RSA	Standard AES	ECC
Encryption Speed (ms)	3.5	7.8	4.1	3.7
Decryption Speed (ms)	3.2	7.4	4.0	3.5
Energy Consumption (mJ)	2.8	5.6	3.2	2.9
Memory Usage (KB)	12	24	18	15
Security Strength	High	Medium	Medium	High
Key Size (bits)	256	2048	128	256
Key Renewal Frequency (min)	15	60	30	20

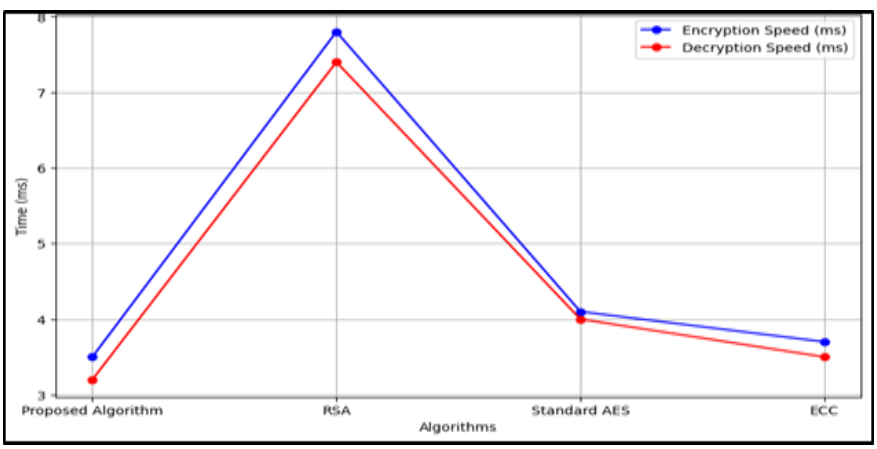

Figure 2

Representation of Encryption and Decryption speed comparison

The figure 2 appears how quick diverse security strategies can secure and translate information. Compared to RSA, typical AES, and ECC, the proposed strategy has the speediest encryption and interpreting times. This implies it works more proficiently. RSA has the speediest speeds, whereas ECC is almost the same as the proposed strategy in terms of execution but takes a small longer. This image appears how the recommended strategy would make cryptographic forms more proficient.

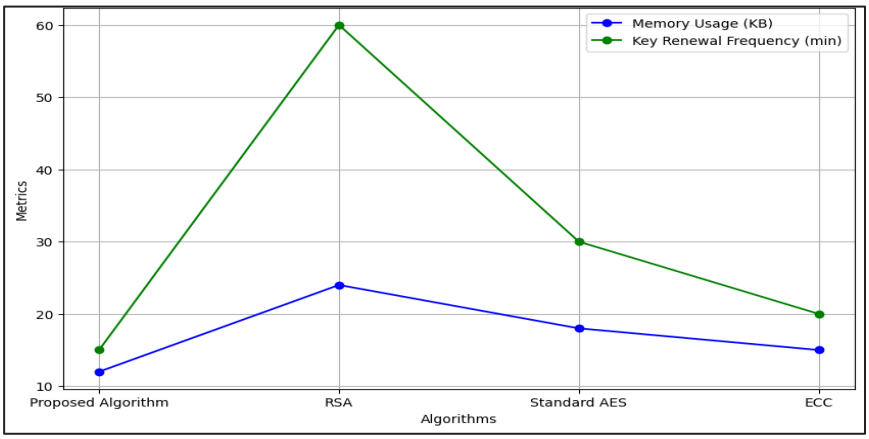

Figure 3
Representation of Memory Usage and Key Renewal Frequency Comparison

The figure 3 appears how much memory diverse encryption strategies utilize and how regularly their keys have to be re-established. The recommended strategy has the foremost visit key revive and the slightest sum of memory usage.

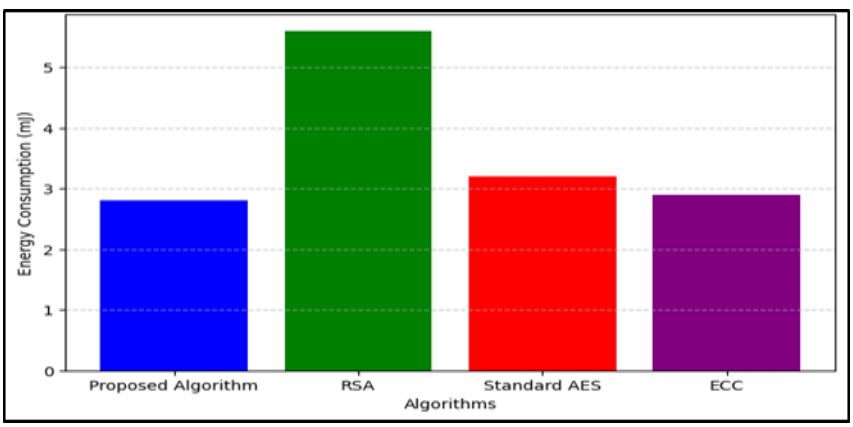

Figure 4
Representation of Energy consumption comparison

This makes way better utilize of assets and makes strides security. RSA needs the foremost memory and its key revive plan is the longest, which implies it employments more assets and changes more gradually. In terms of memory and rehash recurrence, ECC works way better than RSA but not as well as the recommended strategy. The figure 4 appears how much vitality each cryptographic strategy employments. The recommended strategy employments

the slightest sum of control, which makes it way better for WSNs. The foremost vitality is utilized by RSA. Standard AES and ECC are within the center, with ECC being a small way better than AES. This draws consideration to how energy-efficient the recommended strategy is.

5. Conclusion

Utilizing discrete arithmetic to make strides data security measures in cloud computing makes a solid system for securing information and making frameworks more flexible. Organizations can make way better encryption strategies, secure key administration conventions, and solid arrange plans by utilizing discrete scientific thoughts like chart hypothesis, combinatory, and algorithmic complexity. These scientific tools make it simpler to form models that accurately appear and secure against possible assault ways and security gaps. Discrete science is moreover valuable for making versatile security frameworks that can alter with modern dangers while keeping execution tall. As cloud settings get more complicated, discrete mathematics will have to be a huge portion of security plans to keep private information secure and make beyond any doubt that securities are solid and adaptable. Generally, this multidisciplinary strategy not as it were makes security measures more grounded, but it too empowers modern thoughts for building secure cloud computer situations.

References

[1] V. S. P. CH, S. Ranjith, R. V. Krishna and G. Balachandran, "Enhancing Wireless Sensor Network Security using Modified ECC Algorithm," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, pp. 1-6 (2023).

[2] A. Sudarsono, M. U. H. A. Rasyid and H. Hermawan, "An implementation of secure wireless sensor network for e-healthcare system," 2014 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), Bandung, Indonesia, pp. 69-74 (2014)

[3] A. B. Evangeline, R. Jegan and N. W. Subathra, "Implementing Digital Signature with RSA algorithm to enhance the data protection in cloud," 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), Tiruchengode, India, pp. 1-6 (2023).

[4] Y. Zheng, W. Liu and C. H. Chang, "A Lightweight PUF-based Secure Group Key Agreement Protocol for Wireless Sensor Networks," 2023

IEEE International Symposium on Circuits and Systems (ISCAS), Monterey, CA, USA, pp. 1-5 (2023).

[5] Z. Tariq, N. Batool, I. Nadir and T. Bakhshi, "Towards Dynamic Hash-Based Key Establishment in Mobile Wireless Sensor Networking Nodes," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, pp. 1-6 (2020).

[6] G. N. Manoj Chowdary, M. P. Sri Rama lakshmi, Y. Nylu, B. Deepthi, K. Prasad and S. K. Kannaiah, "Elliptic Curve Cryptography for Network Security", 2023 International Conference on Inventive Computation Technologies (ICICT), pp. 1500-1503 (2023).

[7] U Gulen and S Baktir, "Elliptic Curve Cryptography for Wireless Sensor Networks Using the Number Theoretic Transform", *Sensors* (Basel), vol. 20, no. 5, pp. 1507 (Mar 2020).

[8] Arpit Chaudhari and Prachi Jaini, "Stealthier attack on zone routing protocol in wireless sensor network", 2014 Fourth International Conference on Communication Systems and Network Technologies, pp-734-738

[9] D. Dhabliya, S. Kunche, S. Dingankar, S. S. Dari, R. Dhabliya, and V. Khetani, "Blockchain technology as a paradigm for enhancing cyber security in distributed systems," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 729–740 (2024), doi: 10.47974/JDMSC-1923.

[10] Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H. A. Al-Ahdal and Sudhir Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing", *Global Transitions Proceedings,* vol. 2, pp. 91-99 (2021).

[11] A. Mohan and P. Vamshikrishna, "Accounting and Privacy Preserving of Data Owner in Cloud Storage", *International Journal of Innovative Technology and Exploring Engineering* (IJITEE), vol. 10, no. 6 (April 2021), ISSN 2278-3075.

[12] Yahia Alemami, Ali M. Al-Ghonmein, Khaldun G. Al-Moghrabi and Mohamad Afendee Mohamed, "Cloud data security and various cryptographic algorithms", *International Journal of Electrical and Computer Engineering* (IJECE), vol. 13, no. 2, pp. 1867-1879 (April 2023).

Received November, 2024