Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1599–1609
DOI : 10.47974/JDMSC-2159

Implementing secure end-to-end data transmission in wireless sensor networks for healthcare monitoring

Nivedita Ghodke [†]
Department of Artificial Intelligence & Data Science
Dr. D Y Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Rajesh Phursule *
Department of Information Technology
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Revati M. Wahul [§]
Department of Computer Engineering
Modern Education Society's Wadia College of Engineering
Pune 411001
Maharashtra
India

Kirti Bikram [‡]
Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)
Symbiosis Law School Pune (SLS-P)
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

[†] *E-mail:* **Nivedita.Shimbre@gmail.com**
* *E-mail:* **rphursule@gmail.com (Corresponding Author)**
[§] *E-mail:* **rmwahul@mescoepune.org**
[‡] *E-mail:* **kirti.bikram@symlaw.ac.in**

Vikas Nandgaonkar [@]
Department of Computer Engineering
Indira College of Engineering and Management
Pune 410506
Maharashtra
India

Tanya Singh [#]
Department of School of Engineering & Technology
Noida International University
Uttar Pradesh 203201
India

Abstract

Remote sensor systems (WSNs) are basic to healthcare observing frameworks since they give real-time quiet information. Healthcare information is sensitive and requires solid security approaches that account for sensor hub asset limits. This ponder ensures WSN end-to-end information stream with a cross breed cryptographic framework utilizing Elliptic Bend Cryptography (ECC). The strategy combines symmetric encryption for information transmission with ECC for key trade and advanced marks. This crossover strategy optimizes asset utilize and secures information protection, judgment, and genuineness. We compared the proposed convention to RSA with AES, lightweight symmetric encryption, and immaculate ECC encryption to demonstrate its viability. Our cross-breed strategy outflanks choices in numerous key zones. In specific, the proposed approach accomplishes 15 ms encryption and 14 ms unscrambling times, which are much lower than current methods. Since its employments as it were 10 mJ of vitality and 8 KB of memory, it is perfect for resource-constrained situations. Comes about appear that the crossover ECC framework can progress healthcare WSN security and effectiveness, guaranteeing dependable and secure persistent information transmission. This convention meets the require for solid security without relinquishing execution, making it appropriate for healthcare checking frameworks.

Subject Classification: *68M18.*

Keywords: *Wireless sensor networks (WSNs), Elliptic curve cryptography (ECC), Healthcare monitoring, Data security, Hybrid cryptographic protocol.*

1. Introduction

Remote sensor systems (WSNs) empower real-time understanding wellbeing information administration and following in healthcare observing. These systems empower precise and convenient restorative

[@] *E-mail:* **vikas.nandgaonkar@indiraicem.ac.in**
[#] *E-mail:* **dean.academics@niu.edu.in**

mediations by collecting, analyzing, and broadcasting wellbeing information from numerous sensor hubs. WSN integration into healthcare postures genuine security dangers. Wellbeing information is delicate, so it needs solid assurance from information breaches and unauthorized get to. Sensor hubs have restricted computational capacity, memory, and vitality, so they require cryptographic arrangements that ensure information without utilizing as well much framework resources [1], [2]. We utilized lightweight symmetric encryption, unadulterated ECC, and RSA with AES to fathom these issues. RSA with AES combines RSA information encryption and AES key administration. RSA's computational concentrated moderates preparing and employments more vitality, making it unacceptable for WSNs with constrained assets. Lightweight symmetric encryption strategies speed handling but need secure key trade instruments, taking off the framework helpless to assaults. Immaculate ECC gives solid security with littler key sizes and less computational request than RSA, but it can still strain sensor nodes' constrained resources [3], [4]. Given these limitations, this work proposes a crossover cryptographic framework that combines symmetric encryption for information exchange with ECC for key trade and computerized fingerprints. The proposed approach progresses healthcare information security in WSNs to optimize asset utilize and keep up solid security. With ECDH's secure key trades, the crossover cryptographic framework started. ECDH lets two parties safely make a shared mystery key over an unreliable channel utilizing the Elliptic Bend Discrete Logarithm Issue (ECDLP). Each sensor hub and base station produces ECC key sets and trades open keys to compute a shared mystery, which is utilized as the symmetric encryption key for information transmission. The quality of ECC guarantees the key trade remains secure indeed in the event that the transmission channel is compromised [5], [6]. Information bundles are approved utilizing the Elliptic Bend Computerized Signature Calculation (ECDSA) to guarantee information keenness and realness. Sensor hubs sign information with private ECC keys, which the base station confirms with open keys. This framework anticipates information control and guarantees lawfulness. The protocol's symmetric encryption employments the Progressed Encryption Standard (AES), known for its security and effectiveness. Sometime recently sending, AES scrambles healthcare information utilizing the ECDH shared mystery for solid security and moo computational overhead. This half breed approach progresses information security and maximizes asset utilize in healthcare WSNs' constrained situations. To assess the crossover cryptographic convention,

RSA with AES, lightweight symmetric encryption, and unadulterated ECC are compared. The proposed strategy altogether diminishes encryption and decoding times, vitality utilization, and memory utilization, beating current arrangements in key execution criteria. This imaginative arrangement addresses the require for secure, productive information transmission in healthcare WSNs by securing private wellbeing information and guaranteeing sensor hub execution. An adjusted arrangement that meets the strict security criteria and asset limitations of present-day healthcare checking frameworks, the half breed cryptographic convention progresses the field.

2. Literature review

Cutting edge healthcare frameworks presently depend for the most part on remote sensor systems (WSNs), which empower real-time checking and information exchange. WSNs display major troubles in ensuring information security and vitality productivity indeed on the off chance that they have numerous points of interest. Emphasizing complete security, an energy-aware steering component expecting for IoT-based healthcare frameworks addresses the request for solid and compelling information exchange conventions in these touchy uses [7]. With frameworks like FC-SEEDA emphasizing secure and energy-efficient information conglomeration to make strides the Web of Healthcare Things (IoHT), haze computing has too appeared guarantee in this field [8]. Additionally, ponders of healthcare checking frameworks highlight the critical ought to move forward information stream interior WSNs, so focusing the imperative adjust between security safety measures and vitality consumption [9]. Too examined is the integration of secure information transmission conventions in IoHT networks, stressing approaches that grant vitality economy beat need in conjunction with security [10]. Combining AES and RSA, crossover cryptographic models have appeared striking increments in self-organizing brilliantly security for WSNs, so advertising a solid premise for information protection [11]. Thinks about on empowering complete secure communication between WSNs and the bigger web framework highlight the require of building secure channels that can stand up to distinctive cyber dangers whereas keeping successful information flow [12]. By giving secure healthcare information conglomeration, fog-assisted frameworks offer assistance to encourage this objective and so move forward the common constancy and security of IoT-enabled WSN [13]. Persistent checking has too made utilize of

lightweight end-to--end secured communication frameworks, so underscoring the plausibility for perfect cryptographic arrangements free of compromise on security or efficiency [14]. Also appearing empowering comes about are advancements in energy-efficient information accumulation and end-to-end security interior reconfigurable 3D WSNs, so protecting information keenness and vitality economy without compromising performance[15]. This inquire about highlight the critical require of imaginative and successful cryptographic frameworks able to illuminate the two issues of security and asset impediments in healthcare WSN.

3. Methodology

3.1 *Dataset*

The MHealth (Versatile Wellbeing) Dataset, which is available through the "UCI Machine Learning Repository," includes movement and physiological data gathered from ten volunteers. It is used because its diverse range of health-related data makes it ideal for simulating healthcare checking scenarios in WSN. These members performed 12 diverse physical exercises, counting strolling, running, and standing. The dataset incorporates estimations from different sensors such as "accelerometers, whirligigs, magnetometers, and electrocardiograms" (ECG), inspected at a rate of 50 Hz.

3.2 *Data Preprocessing*

Normalization: Normalization scales the sensor information to a standard run, regularly [0, 1] or [-1, 1], guaranteeing consistency over distinctive sorts of sensor estimations**.**

Segmentation: Division partitions the nonstop sensor information into littler, fixed-length windows or portions, encouraging simpler investigation and design acknowledgment.

3.3 *Hybrid Cryptographic Protocol Using ECC*

WSN give real-time understanding wellbeing information, making them fundamental in healthcare checking frameworks. Due to the affectability of healthcare information, transmission security is pivotal. gives a secure and compelling arrangement catered for the asset restrictions common of WSN by implies of a half breed cryptographic convention. Guaranteeing both solid security and viable execution, this convention

combines the focal points of ECC for key trade with advanced marks with symmetric encryption for information transmission.

3.3.1. ECC fundamental

The mathematical structure of elliptic bends over constrained areas serves as the foundation for ECC. The ECDLP, which is computationally challenging to understand, is the source of ECC's security. An elliptic curve over a finite field F_p is defined by the following basic equation:

$$y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p)$$

3.3.2. Key Exchange Using Elliptic Curve Diffie-Hellman (ECDH)

- The ECDH convention permits two parties to build a shared mystery across an unclear channel. Each side creates a private key and an equivalent open key. The actions are as follows:
- **Key Generation**: Each party produces a private key d haphazardly chosen from {1,…,n–1}, where n is the arrange of the elliptic bend. The open key Q is at that point computed as:
- Q=d.G
- Where G may be a predefined focus on the elliptic bend known as generator point.

Key Exchange: Each party sends their public key to the other.

- **Shared Secret Computation**: Each party determines the shared secret S using their personal keys and the other party's public key:

$$S_A = d_A . Q_B$$

$$S_B = d_B . Q_A$$

Due to the properties of elliptic curve $S_A = S_B$ able to establish a common shared secret.

3.3.3 Digital Signatures Using Digital Signature Algorithm using Elliptic Curve

ECDSA guarantees the integrity and genuineness of the transmitted data. The signature generation and verification processes are as follows:

- **Signature Generation**

- Select a random integer k from $\{1,2\ldots n-1\}$
- Compute the point $(x_1, y_1) = k.\ G$. The signature component r is:

$$r = x_1 (\mathrm{mod}\, n)$$

- Compute k^{-1} modulo n.
- Computer the hash of the message m, denoted as $z=H(m)$.
- Compute the signature component s as:

$$s = k \ \ -1(z + rd\_A)(\mathrm{mod}\, n)$$

- **Signature Verification**
  - Identify that r and s are within the interval [1, n-1]
  - Computer $w = s^{-1}$ (mod n)
  - Compute $u_1 = z\ .\ w$ (mod n) and $u_2 = r\ .\ w$ (mod n)
  - Computer the point $(x_2, y_2) = u_1\ .\ G + u_2\ .\ Q_A$
  - The signature is valid if: $r \equiv x_2$ (mod n)

3.3.4 Symmetric Encryption for Data Transmission

After a common secret is calculated by ECDH it is used as a key for symmetric encryption methods such as AES. Symmetric encryption costs less in terms of computational resources when compared to asymmetric encryption and can be used for frequent transmission of health data.

Algorithm: Hybrid Cryptographic Protocol for Secure Data Transmission in WSN

1. **Initialization:**
   For each sensor node:
   Generate ECC key pair (private_key, public_key)
   Base Station:
   Generate ECC key pair (BS_private_key, BS_public_key)
2. **Data Collection:**
   For each sensor node:
   Collect physiological and motion data from sensors (MHealth dataset)
   Store collected data in data_buffer
3. **Key Exchange:**
   For each sensor node:

Forward the public key to the base station.

BS_public_key is obtained from Base Station.

Compute shared_secret using ECDH: shared_secret = ECDH(private_key, BS_public_key)

4. **Data Encryption:**

   For each data packet in data_buffer:

   Encrypt data using AES with shared_secret: encrypted_data = AES_encrypt(shared_secret, data_packet)

   Sign data packet with ECDSA: signature = ECDSA_sign(private_key, data_packet)

   Create transmission_packet: transmission_packet = (encrypted_data, signature)

5. **Data Transmission:**

   For each sensor node:

   Transmit transmission_packet to Base Station

6. **Data Reception and Decryption:**

   Base Station:

   For each received transmission_packet:

   Verify signature using ECDSA: is_valid = ECDSA_verify(BS_public_key, encrypted_data, signature)

   If is_valid:

Use shared_secret and AES to decrypt encrypted_data: data_packet = AES_decrypt(shared_secret, encrypted_data)
Keep or handle the decrypted data packet.

3.3.5 Evaluation parameters

Encryption Time (ms): This parameter measures the term required to scramble a information parcel utilizing the half breed cryptographic convention. It is significant to guarantee that the encryption handle is quick, minimizing the delay in information transmission inside resource-constrained WSNs**.**

Unscrambling Time (ms): Comparable to encryption time, this parameter surveys the time taken to unscramble an approaching information parcel at the base station. Proficient decoding is basic for opportune information handling and reaction in healthcare checking frameworks**.**

Vitality Utilization (mJ): This metric assesses the sum of vitality expended by sensor hubs amid encryption, decoding, and information transmission. Lower vitality utilization is crucial for drawing out the battery life of sensor hubs, guaranteeing supported operation of the WSN**.**

Memory Utilization (KB): This parameter measures the memory assets required for putting away cryptographic keys, scrambled information, and related operations. Proficient memory utilization is basic for sensor hubs with constrained memory capacity, permitting them to handle cryptographic forms without compromising execution.

4. Results discussion

The proposed Half breed ECC Convention illustrates prevalent execution with the least encryption (15 ms) and unscrambling times (14 ms), negligible vitality utilization (10 mJ), and the slightest memory utilization (8 KB). In comparison, RSA with AES appears the most elevated times and asset requests, whereas lightweight symmetric encryption and immaculate ECC offer direct enhancements but still drop brief of the proposed half breed approach's productivity and security adjust as appeared in table 1.

Table 1

Evaluation parameter comparison of proposed model vs other models

Methodology	Proposed Hybrid ECC Protocol	RSA with AES	Lightweight Symmetric Encryption	ECC without Hybrid Approach
Encryption Time (ms)	15	25	20	17
Decryption Time (ms)	14	23	18	16
Energy Consumption (mJ)	10	18	12	11
Memory Usage (KB)	8	16	12	10

5. Conclusion and future scope

The usage of the Cross breed ECC Convention in WSN for healthcare checking altogether improves information security and proficiency. With its moo encryption and unscrambling times, negligible vitality utilization, and decreased memory utilization, the convention addresses the basic challenges postured by asset imperatives in sensor hubs. This makes it an

exceedingly successful arrangement for secure information transmission in healthcare applications. Future investigate might investigate coordination progressed machine learning procedures for real-time irregularity location and versatile security instruments to encourage improve the protocol's strength. Too, growing the convention to bolster a more extensive extend of healthcare gadgets and interoperability guidelines seem encourage broader selection and move forward understanding care through more comprehensive observing frameworks.

References

[1] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 400–411 (2009), doi: 10.1109/JSAC.2009.090505.

[2] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, J. Isoaho, and P. Liljeberg, "Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 581–588 (2015), doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.83.

[3] T.-V. Le, "Cross-Server End-to-End Patient Key Agreement Protocol for DNA-Based U-Healthcare in the Internet of Living Things," *Mathematics*, vol. 11, no. 7. (2023), doi: 10.3390/math11071638.

[4] S. R. Moosavi, T. N. Gia, A. M. Rahmani, A. H. Anzanpour, M. A. Pusti, P. Liljeberg, and H. Tenhunen, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 64, pp. 108–124 (2016), doi: https://doi.org/10.1016/j.future.2016.02.020.

[5] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, and D. Toal, "A secure end-to-end IoT solution," *Sensors Actuators A Phys.*, vol. 263, pp. 291–299 (2017), doi: https://doi.org/10.1016/j.sna.2017.06.019.

[6] S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho, "Performance Analysis of End-to-End Security Schemes in Healthcare IoT," *Procedia Comput. Sci.*, vol. 130, pp. 432–439 (2018), doi: https://doi.org/10.1016/j.procs.2018.04.064.

[7] R. Nidhya, S. Karthik, and G. Smilarubavathy, "An End-to-End Secure and Energy-Aware Routing Mechanism for IoT-Based Modern Health Care System BT - Soft Computing and Signal Processing," pp. 379–388 (2019).

[8] C. Chakraborty, S. Ben Othman, F. A. Almalki, and H. Sakli, "FC-SEEDA: fog computing-based secure and energy efficient data aggregation scheme for Internet of healthcare Things," *Neural Comput. Appl.*, vol. 36, no. 1, pp. 241–257 (2024), doi: 10.1007/s00521-023-08270-0.

[9] S. K. Swami Durai, B. Duraisamy, and J. T. Thirukrishna, "Certain Investigation on Healthcare Monitoring for Enhancing Data Transmission in WSN," *Int. J. Wirel. Inf. Networks*, vol. 30, no. 1, pp. 103–110 (2023), doi: 10.1007/s10776-021-00530-x.

[10] A. Duddalwar and P. Khobragade, "A statistical approach for hospital management system using machine learning," *AIP Conference Proceedings*, vol. 3139, no. 1, p. 100007 (Aug. 2024). doi: 10.1063/5.0224460.

[11] V. Anusuya Devi and T. Sampradeepraj, "End-to-End Self-organizing Intelligent Security Model for Wireless Sensor Network based on a Hybrid (AES–RSA) Cryptography," *Wirel. Pers. Commun.*, vol. 136, no. 3, pp. 1675–1703 (2024), doi: 10.1007/s11277-024-11353-3.

[12] H. Yu, J. He, T. Zhang, P. Xiao, and Y. Zhang, "Enabling end-to-end secure communication between wireless sensor networks and the Internet," *World Wide Web*, vol. 16, no. 4, pp. 515–540 (2013), doi: 10.1007/s11280-012-0194-0.

[13] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 1, pp. 163–174 (2020), doi: 10.1007/s12083-019-00745-z.

[14] F. S. Chowdhury, A. Istiaque, A. Mahmud, and M. Miskat, "An implementation of a lightweight end-to-end secured communication system for patient monitoring system," in *2018 Emerging Trends in Electronic Devices and Computational Techniques (EDCT)*, pp. 1–5 (2018), doi: 10.1109/EDCT.2018.8405076.

[15] K. Ramasamy, M. H. Anisi, and A. Jindal, "E2DA: Energy Efficient Data Aggregation and End-to-End Security in 3D Reconfigurable WSN," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 787–798 (2022), doi: 10.1109/TGCN.2021.3126786.

Received November, 2024