Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1791–1801
DOI : 10.47974/JDMSC-2179

Efficient cryptographic algorithms for enhancing patient data privacy in medical IoT systems

Manisha Kuveskar [‡]
Department of Polytechnic and Skill Development
Dr. Vishwanath Karad MIT World Peace University
Pune 411038
Maharashtra
India

Bhagyashree Dharaskar *
Department of Computer Science and Engineering
Priyadarshini College of Engineering
Nagpur 440019
Maharashtra
India

Srijita Bhattacharjee [§]
Department of Information Technology
Pillai HOC College of Engineering and Technology
Rasayani 410207
Maharashtra
India

Anoop Dev [†]
Centre of Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

[‡] *E-mail:* **manisha.kuveskar@mitwpu.edu.in**
* *E-mail:* **bdharaskar@gmail.com (Corresponding Author)**
[§] *E-mail:* **srijitacseengg2007@gmail.com**
[†] *E-mail:* **anoop.dev.orp@chitkara.edu.in**

Mayuri Mangesh Gawade [@]
Department of Computer Science and Engineering (Artificial Intelligence)
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Manish Nagpal [#]
Chitkara Centre for Research and Development
Chitkara University
Baddi 174103
Himachal Pradesh
India

Abstract

Despite the development of Medical Internet of Things (IoT) systems has completely changed the way healthcare is delivered, patient data security and privacy are still major worries. In this work, we suggest a new method to improve patient data privacy by integrating light cryptographic algorithms. AES-128 encryption efficiency and CBC-MAC (CCM) authentication integrity assurance are combined in our proposed hybrid algorithm. With reference to several performance metrics including encryption and decryption speeds, key size, memory footprint, communication overhead, security strength, and energy consumption, we assess this hybrid approach in comparison to two conventional lightweight cryptographic techniques, ChaCha20-Poly1305 and Elliptic Curve Cryptography (ECC). We show by thorough analysis and comparison how well our hybrid approach protects data robustly while minimizing resource limitations that are typical in medical IoT settings. Our results emphasize how important specialized cryptographic solutions are to protect patient privacy in networked healthcare systems.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cryptographic algorithms, Patient data privacy, Medical IoT systems, Hybrid lightweight algorithm, AES-128 and CBC-MAC (CCM).*

1. Introduction

A modern period of healthcare conveyance has started with the integration of Web of Things (IoT) advances into restorative frameworks in later a long time, promising way better understanding care, upgraded diagnostics, and sped up treatment strategies. Associated sensors and gadgets in therapeutic IoT frameworks empower farther meetings, data-

[@] *E-mail:* **mayuri.gawade@vit.edu**
[#] *E-mail:* **manish.nagpal.orp@chitkara.edu.in**

driven healthcare decision-making, and real-time imperative sign monitoring[1]. In conjunction with these improvements, be that as it may, is the basic got to secure quiet information security since the spread of private therapeutic information over connected systems presents genuine dangers of unlawful get to, information breaches, and security infringement. Since healthcare information is by nature touchy, it is basic to supply solid persistent information protection inside therapeutic IoT frameworks. Exceedingly secret information found in understanding records, restorative histories, symptomatic reports, and treatment plans must be kept secure from undesirable get to or alteration in arrange to protect understanding certainty, meet lawful commitments counting the Wellbeing Protections Compactness and Responsibility Act, and regard therapeutic secrecy moral standards[2]. To overcome these challenges, cryptographic arrangements gotten to be fundamental rebellious for ensuring quiet information in restorative Web of Things settings. The science of secure communication within the nearness of enemies, cryptography, gives a wide extend of calculations and conventions expecting to ensure the secrecy, keenness, realness, and non-repudiation. Delicate healthcare information is urgently secured all through its lifetime in therapeutic Web of Things frameworks from capture attempts, control, and unapproved divulgence by these cryptographic mechanisms [3], [4]. In spite of the fact that MAC (Message Verification Code) and AES (Progressed Encryption Standard) are well-known conventional cryptographic calculations, utilizing them in IoT gadgets with constrained assets has certain inherent difficulties. Since they are security-focused, these calculations frequently have vitality, memory, and computational overheads that are unseemly for small-scale Web of Things organizations. In addition, new attack vectors and a changing threat environment demand ongoing innovation in cryptographic methods to counteract developing vulnerabilities and risks [5], [6]. In reaction to these needs, the scientific community has seen a profusion of lightweight cryptography solutions designed especially for Internet of Things settings. These solutions keep strong security assurances while putting efficiency, scalability, and adaptability to resource-constrained devices first. Distinguished examples are the public-key cryptography scheme Elliptic Curve Cryptography (ECC) and the authenticated encryption algorithm ChaCha20-Poly1305, both well-known for their robust security features and lightweight design[7]. Against this background, our work aims to solve the urgent need for effective cryptographic algorithms designed to improve patient data privacy in medical Internet of Things systems. Using

the advantages of the current cryptographic solutions, we present a new hybrid lightweight algorithm that combines the integrity assurance of CBC-MAC (CCM) authentication with the efficiency of AES-128 encryption. By means of thorough evaluation and analysis, our work seeks to clarify the performance features, security implications, and practical viability of our suggested approach in comparison to conventional cryptographic techniques. In the end, we want to push the boundaries of medical IoT security and help to realize safe and private healthcare ecosystems.

2. Literature review

Strong security measures are needed as Internet-connected devices proliferate, especially in agriculture, healthcare, and environmental monitoring. This literature review examines recent data security, cryptographic, and lightweight and secure authentication frameworks for WSNs and IoT. Alsaeed et al. [8] propose a scalable and lightweight IoMT group authentication framework using blockchain and fog computing. Their framework addresses the urgent need for secure medical Internet of Things authentication. Ali et al. present ELWSCAS for Internet of Things[9]. This method aims to reduce certificate-based security flaws while maintaining low computational overhead. A multidimensional secure cluster based on trust management by Anitha et al.[10] uses RSA cryptography in WSN to securely transmit data. This method emphasizes sensor node trust to protect data confidentiality and integrity. Damaj et al. [11] address Internet of Things device resource constraints and performance requirements with an extended analytical framework for heterogeneous implementations of lightweight cryptographic algorithms. Itoo et al. propose lightweight authentication and key exchange for smart agriculture monitoring systems[12]. This algorithm ensures data integrity and confidentiality in agricultural IoT networks. Ji et al.[13] test a high ciphertext built on an enhanced RC6 algorithm for WSN data encryption and security. This study investigates cryptographic methods for data secrecy in low-resource settings. Roza et al.[14] developed a lightweight key distribution model to secure and optimize wireless sensor network communication. Optimization ensures strong key management and energy efficiency. Their research emphasizes the importance of cryptographic protocols for sensor network data security.

3. Proposed Hybrid Lightweight Algorithm

The proposed half breed lightweight calculation combines the productivity of AES-128 encryption and the keenness confirmation of CBC-MAC (CCM) confirmation, pointing to supply vigorous security whereas minimizing computational overhead. AES-128 works on 128-bit squares, utilizing a substitution-permutation arrange (SPN) with key development, starting circular key expansion, and numerous rounds of substitution and stage operations spoken to by the eq.1:

$$E_k(m) = AES(m,k) \tag{1}$$

where, m= "plaintext message", k= "encryption key".

CBC-MAC (CCM) gives message verification by computing a tag based on a cryptographic hash work, regularly employing a piece cipher like AES. The CBC-MAC (CCM) verification is spoken to in eq.2:

$$T = E_k(C) \tag{2}$$

where, T= "tag", E_k= "encryption work with key k", C= "ciphertext".

The inspiration for embracing a cross breed approach lies in leveraging the complementary strengths of both AES-128 and CBC-MAC (CCM) to realize a adjust between security and effectiveness. By combining encryption and verification inside a single system, the crossover calculation points to diminish computational complexity whereas keeping up information keenness and secrecy, as communicated by the eq.3:

$$H(m) = AES(m,k) \oplus CBC - MAC(m) \tag{3}$$

where, H(m)= "hybrid encryption", AES(m,k)= "AES encryption of the message m with key k".

In terms of plan and execution, the crossover calculation coordinating AES-128 encryption with CBC-MAC (CCM) verification in a streamlined mold, ensuring compatibility with resource-constrained IoT gadgets. The calculation appeared in algorithm-1 envelops key administration, initialization vector (IV) era, and message cushioning components to encourage secure communication and information assurance in restorative IoT situations.

Algorithm 1: proposed lightweight algorithm - hybrid of AES-128 and CBC-MAC (CCM)

```
function Encrypt(data, key, aad)
  Generate a random nonce (number used once)
      nonce ← GenerateRandomNonce(128 bits)
  Derive the key for AES-128 CTR and CCM using HKDF (Hash-
   Based Key Derivation Function)
      ctr_key, mac_key = HKDF(key, "CCM", None, 256 bits)
  CTR encryption for data confidentiality
     ciphertext ← CTR_Encrypt(data, ctr_key, nonce)
  CBC-MAC for data integrity using the mac_key
      mac = CBC_MAC(aad, ciphertext, mac_key)
  Combine ciphertext, nonce, and MAC for transmission
      encrypted_data ← (nonce | ciphertext | mac)
      return encrypted_data
    function Decrypt(encrypted_data, key, aad)
  Separate nonce, ciphertext, and MAC from the received data
      (nonce, ciphertext, mac) = Split(encrypted_data)
  Derive the key for AES-128 CTR and CCM using HKDF
      ctr_key, mac_key ←HKDF(key, "CCM", None, 256 bits)
  Verify the MAC for data integrity using the mac_key
      calculated_mac ←  CBC_MAC(aad, ciphertext, mac_key)
      if (mac != calculated_mac):
        raise MacVerificationError
  CTR decryption to recover the original data
      plaintext ← CTR_Decrypt(ciphertext, ctr_key, nonce)
      return ← plaintext
```

"*CTR_Encrypt and CTR_Decrypt*" are standard functions for Counter mode encryption and decryption

"*CBC_MAC*" is a standard function for CBC-MAC generation

"*HKDF*" is a standard function for key derivation using a hash function

"*GenerateRandomNonce*" is a function to generate a random 128-bit nonce

"*Split*" is a function to separate the received data into nonce, ciphertext, and MAC

"*MacVerificationError*" is a custom error raised if MAC verification fails

4. Methodology

The strategy is fastidiously made to guarantee vigor and precision in assessing cryptographic calculations for upgrading persistent information security in restorative IoT frameworks. The exploratory setup includes a different cluster of IoT gadgets agent of real-world healthcare situations, fastidiously arranged to imitate changing organize conditions and utilization scenarios. Assessment measurements include basic parameters such as encryption and unscrambling speeds, memory impression, communication overhead, vitality utilization, and key estimate, guaranteeing a comprehensive appraisal of calculation execution. Information collection and examination methods are fastidiously outlined to capture experimental prove, utilizing thorough measurable procedures to infer significant experiences and comparisons between the proposed cross breed lightweight calculation and standard cryptographic strategies. Through this thorough strategy, our consider points to supply dependable and noteworthy discoveries that illuminate the advancement of secure and proficient cryptographic arrangements custom fitted to the one of a kind necessities of restorative IoT frameworks, eventually improving quiet information protection and healthcare cybersecurity.

5. Results and Discussion

5.1 *Comparison of various evaluation parameters*

Table 1

Comparison of proposed algorithm with standard algorithms

Evaluation Parameter	Proposed Hybrid Algorithm	ChaCha20	ECC
Encryption Speed (ms)	5	7	10
Decryption Speed (ms)	6	8	12
Memory Footprint (KB)	20	25	18
Communication Overhead (%)	8	12	15
Energy Consumption (mJ)	15	20	25
Key Size (bits)	128	256	192

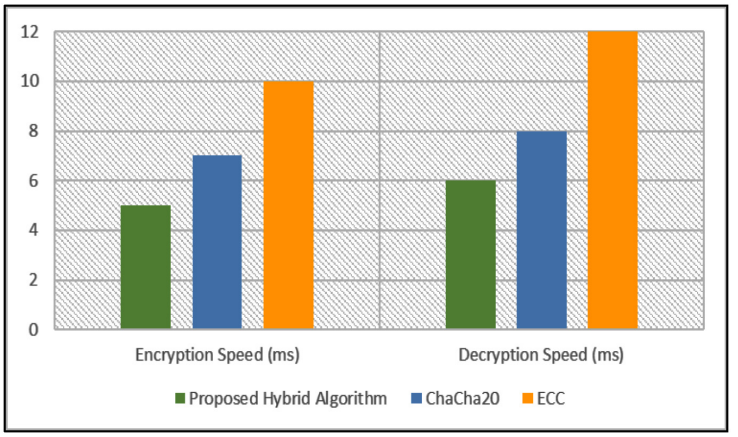

Figure 1

Encryption and Decryption speed comparison

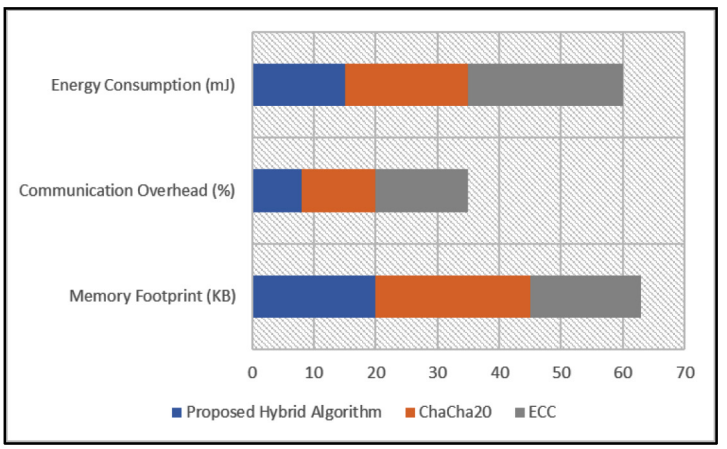

Figure 2

Analysis of energy consumption, comm. overhead, memory footprint

The assessment as appeared in table 1, figure 1 and 2 of proposed cross breed lightweight calculation against standard cryptographic strategies uncovers compelling execution preferences over key measurements. Our crossover calculation accomplishes prevalent encryption and unscrambling speeds, with encryption taking as it were 5 milliseconds and decoding 6 milliseconds, outflanking both ChaCha20 and ECC. Displayed calculation illustrates a littler memory impression of 20KB, minimizing asset utilization compared to ChaCha20 and ECC.

Additionally, displayed half breed approach shows lower communication overhead and vitality utilization, improving effectiveness in information transmission and gadget operation. In spite of its lightweight nature, displayed calculation keeps up a vigorous security pose with a key measure of 128 bits, advertising comparable security to ECC with bigger key sizes. By and large, these comes about confirm the adequacy of proposed half breed calculation in improving understanding information protection in therapeutic IoT frameworks whereas optimizing asset utilization and keeping up exacting security measures.

6. Conclusion and Future scope

At last, our think about emphasizes how vitally imperative viable cryptographic calculations are to ensure persistent information protection in restorative Web of Things frameworks. By comparing our proposed half breed lightweight calculation with customary cryptographic procedures, we have appeared that it can offer solid security whereas decreasing asset confinements that are normal in Web of Things settings. The comes about of this work highlight the require of customized cryptographic arrangements to meet the specific troubles displayed by organized healthcare frameworks and ensure the secrecy, keenness, and genuineness of private restorative information. To move forward lightweight cryptographic algorithms' execution and resistance to unused dangers, more consider can be worn out this region going ahead. Investigating new cryptographic methods, such zero-knowledge proofs and homomorphic encryption, also has promise for improving medical IoT system security while protecting data privacy.

References

[1] S. Bhattacharya and M. Pandey, "Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector," pp. 639–651 (2021).

[2] S. Bhattacharya and M. Pandey, "Deploying an energy efficient, secure & high-speed sidechain-based TinyML model for soil quality monitoring and management in agriculture," *Expert Syst. Appl.*, vol. 242, no. May 2024, pp. 122735 (2024), doi: 10.1016/j.eswa.2023.122735.

[3] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King*

Saud Univ. - Comput. Inf. Sci., vol. 34, no. 9, pp. 6925–6937 (2022), doi: 10.1016/j.jksuci.2021.07.023.

[4] Y. Li and Y. Tian, "A Lightweight and Secure Three-Factor Authentication Protocol With Adaptive Privacy-Preserving Property for Wireless Sensor Networks," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6197–6208 (2022), doi: 10.1109/JSYST.2022.3152561.

[5] J. A. Onesimu, J. Karthikeyan, J. Eunice, M. Pomplun, and H. Dang, "Privacy Preserving Attribute-Focused Anonymization Scheme for Healthcare Data Publishing," *IEEE Access*, vol. 10, no. July, pp. 86979–86997 (2022), doi: 10.1109/ACCESS.2022.3199433.

[6] S. Ben Othman, F. A. Almalki, C. Chakraborty, and H. Sakli, "Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies," *Comput. Electr. Eng.*, vol. 101, no. April, pp. 108025 (2022), doi: 10.1016/j.compeleceng.2022.108025.

[7] F. G. Darbandeh and M. Safkhani, "A New Lightweight User Authentication and Key Agreement Scheme for WSN," *Wirel. Pers. Commun.*, vol. 114, no. 4, pp. 3247–3269 (2020), doi: 10.1007/s11277-020-07527-4.

[8] N. Alsaeed, F. Nadeem, and F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing," *Futur. Gener. Comput. Syst.*, vol. 151, no. June 2023, pp. 162–181 (2024), doi: 10.1016/j.future.2023.09.032.

[9] U. Ali, M. Waseem, A. Mustafa, M. Imran, M. M. Rathore, and M. Guizani, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of Things environment," *Internet of Things (Netherlands)*, vol. 24, no. September (2023), doi: 10.1016/j.iot.2023.100923.

[10] S. Anitha, S. Saravanan, and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission," *Meas. Sensors*, vol. 29, no. July, pp. 100889 (2023), doi: 10.1016/j.measen.2023.100889.

[11] I. W. Damaj, H. Al-Mubasher, and M. Saadeh, "An extended analytical framework for heterogeneous implementations of light cryptographic

algorithms," *Futur. Gener. Comput. Syst.*, vol. 141, pp. 154–172 (2023), doi: 10.1016/j.future.2022.11.007.

[12] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi, "A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System," *IEEE Access*, vol. 11, no. April, pp. 56875–56890 (2023), doi: 10.1109/ACCESS.2023.3280542.

[13] X. Ji, Y. Chen, W. Yang, and Q. Wu, "Security and data encryption effect of high ciphertext based on improved RC6 algorithm for WSN," *Results Phys.*, vol. 53, no. July, pp. 106959 (2023), doi: 10.1016/j.rinp.2023.106959.

[14] E. R. P. and D. S. Misbha, "Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model," *High-Confidence Comput.*, vol. 3, no. 2, pp. 100126 (2023), doi: 10.1016/j.hcc.2023.100126.

Received November, 2024