Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 441–452
DOI : 10.47974/JDMSC-1900

Secure and scalable data aggregation techniques for healthcare monitoring in WSN

Mahendra Alate [‡]
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad
Maharashtra
India

Uma R. Godase [†]
School of Computing
MIT Art, Design and Technology University
Pune
Maharashtra
India

Uddhav T. Kumbhar [§]
Department of Community Medicine, Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed To Be University)
Karad
Maharashtra
India

Sheela Hundekari*
Department of MCA
MIT-COM
MIT Art, Design & Technology University
Loni Kalbhor
Pune
Maharashtra
India

[‡] *E-mail:* mahendra.alate@gmail.com
[†] *E-mail:* urgodase@gmail.com
[§] *E-mail:* utkumbhar@gmail.com
* *E-mail:* sheela.hundekari@mituniversity.edu.in (Corresponding Author)

Araddhana Arvind Deshmukh [@]
Department of Computer Science & Information Technology (Cyber Security)
Symbiosis Skill and Professional University, Kiwale
Pune
Maharashtra
India

Anil Kumar [#]
Department of Computer Science and Engineering
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India

Abstract

Wireless Sensor Networks (WSN) are crucial in the healthcare field as they allow for the immediate monitoring and collection of data from medical sensors. The growing incorporation of WSN in healthcare requires the creation of authentication protocols that are both strong and energy-efficient. This study presents Lightweight Authentication Protocol for Cloud-based Health-care Systems (LAPCHS) using BLAKE2 designed specifically for WSN in medical settings for secure and scalable data aggregation. The proposed method tackles the difficulties presented by limited resources in sensor nodes, with the goal of achieving a careful equilibrium between strong security and effective energy usage. LAPCHS utilizes innovative techniques to improve the energy efficiency in WSN. The system employs the BLAKE2 cryptographic hash algorithm to establish robust mutual authentication and key agreement between the tag and the cloud server. The protocol is characterized by its low weight and high efficiency, rendering it appropriate for deployment in medical sensor networks with limited resources, which minimizes the need for global key distribution and decreases communication overhead. The proposed method is useful to meet the distinct needs of medical sensor networks, where energy preservation is of utmost importance to ensure extended device scalability. The findings demonstrate that LAPCHS surpasses current approaches in terms of energy efficiency and latency, while simultaneously upholding a robust level of security. The protocol's novel strategy for managing encryption keys and selecting cryptographic algorithms makes it a promising solution for securing medical sensor networks while maintaining energy sustainability. This study makes a valuable contribution to the developing field of WSN security by proposing a practical solution for ensuring strong and energy-efficient authentication in healthcare applications.

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

Keywords: *Energy-efficient, Latency, Medical-WSN, Energy consumption.*

[@] *E-mail:* **aadeshmukhskn@gmail.com**
[#] *E-mail:* **anil.vashu@gmail.com**

1. Introduction

WSN have become revolutionary devices in the dynamic field of the IoT, facilitating smooth data exchange and communication among a wide range of applications. Their importance is especially noticeable in the healthcare industry, as WSN are essential to determining how patient care and medical research will develop in the future. These networks give medical professionals unprecedented insights into patient outcomes, treatment efficacy, and overall healthcare processes by facilitating real-time data collection and monitoring through a variety of medical sensors[1]–[3].

But integrating WSN into healthcare applications presents a number of complex challenges, the most important of which is maintaining data integrity and ensuring secure communication within the network. Because of the sensitive patient information, vital signs, and diagnostic data that are transmitted in healthcare scenarios, a strong security framework is necessary to prevent unauthorized access and manipulation. The intrinsic resource limitations of sensor nodes in the network, of which energy limitations stand out as a crucial factor, further complicate this imperative. Therefore, the challenge is to maintain the consistent and dependable operation of WSN in healthcare settings while strengthening security measures and navigating these resource constraints[4], [5].

The progress of healthcare technologies has facilitated the incorporation of medical sensor networks (MSN) into different healthcare environments, allowing for the ongoing monitoring of patients' vital signs and health indicators. Nevertheless, the widespread use of MSN gives rise to apprehensions over the security and confidentiality of delicate patient information conveyed through unsecured wireless networks. Traditional authentication procedures frequently result in substantial computing burden and energy usage, making them inappropriate for MSN with limited resources[4]–[7].

The LAPCHS protocol has numerous benefits compared to current authentication protocols, including lightweight and efficient operation, strong security measures, and privacy preservation. LAPCHS addresses the security and energy efficiency concerns of MSN, hence facilitating secure and dependable data transfer in cloud-based healthcare systems. This ultimately improves the privacy and security of sensitive patient information. In order to tackle these difficulties, we suggest implementing the LAPCHS which utilizes BLAKE2, a resilient and energy-efficient authentication protocol specifically tailored for MSN. LAPCHS utilizes

the BLAKE2 cryptographic hash function to establish robust mutual authentication and key agreement between resource-limited MSN and cloud servers.

The main goals of this study are to present and assess LAPCHS specifically designed for medical sensor networks. Throughout this investigation, the focus has been on developing a novel approach that strengthens the security posture of healthcare WSN while also protecting the finite energy resources necessary for extended and sustainable network operation. Through the presentation of LAPCHS, this research hopes to further energy-efficient and secure practices, which will ultimately improve the dependability and effectiveness of WSN in healthcare applications.

2. Literature Review

In the fast-changing IoT environment, WSN enable easy communication and data exchange in multiple domains. These networks are being used in healthcare, environmental monitoring, and industrial automation, making energy-efficient and secure communication methods essential. The current state of Wireless Sensor Network protocols for energy consumption, privacy, and secure data transfer is reviewed in this literature.

Abdul-Qawy et al.[8] develop an energy-efficient protocol for a large-scale IoT-based heterogeneous WSN. IoT devices heterogeneity and large networks scalability issues are addressed by the protocol. The authors describe a novel energy optimization strategy to extend sensor node operation. The study illuminates the protocols efficacy in different settings, emphasizing its practicality. In WSN Syed Masood et al.[9] focus on privacy, particularly for healthcare data. The authors propose an energy-efficient strategy for routing several channels to protect sensitive healthcare data. The study investigates technological data protection and ethical WSN healthcare data management. The findings add to the hospital Wireless Sensor Network security topic. Begum et al.[10] examine WSN and IoT data aggregation methods in detail. It consolidates current information to help choose protocols for specific applications.

Anil Kumar et al.[11] describe a secure blockchain-based framework for cloud-based EHR systems. The writers explore the growing need for healthcare data security and integrity. Blockchain is used to promote data openness, traceability, and system security in the study. This effort advances safe healthcare data management by using blockchain technology

to ensure electronic health record reliability and privacy. Singh et al.[12] optimize energy routing in WSN to improve network lifespan. The authors propose an energy-efficient clearing routing technique that accounts for sensor node restrictions. The study evaluates the routing algorithm's practicality in WSN deployments. This work advances energy-efficient routing techniques, which are essential to WSN sustainability. Krishnapriya et al.[13] present a rank-based key management routing system for IoT medical sensors in WSN that prioritizes energy efficiency. The protocol uses a rank-based technique to prioritize nodes by energy level and other parameters to improve energy efficiency. This protocol is used in medical sensor networks, and the study emphasizes energy conservation in healthcare-related IoT applications.

Reddy et al.[14] offer a compressed and targeted communication protocol for wireless sensor network data transmission. Energy efficiency during data transmission is a focus of the study, especially in narrow channel communication. The proposed protocol maximizes energy savings while ensuring reliable data transmission in sensor networks with limited resources. Shafiq et al.[15] review the research on energy-efficient routing algorithms in wireless sensor networks. Current routing techniques are examined in detail, with a focus on energy efficiency. The authors classify and evaluate numerous methods, highlighting their pros and cons. This study helps researchers and practitioners understand energy-efficient routing in Wireless Sensor Networks. Suresh et al.[16] propose an energy-efficient and safe routing technique for IoT WSN. Low-Energy Adaptive Clustering Hierarchy (LEACH) improves energy economy and secure communication in the study. The routing technique addresses energy preservation and protection, making it suitable for IoT applications. Roja et al.[1] offer a simplified key distribution system for safe, energy-efficient wireless sensor network communication. The model optimizes key activity distribution, reducing computer overhead and energy consumption. This study contributes to key management system development by focusing on the important balance between security and energy efficiency in WSN.

To conclude, the literature review shows innovative solutions to Wireless Sensor Networks complicated problems. WSN researchers are interested in energy efficiency, privacy, and secure communication. The findings highlight the importance of tailoring protocols for specific applications, such as healthcare and IoT, where energy efficiency and security must be balanced. The emerging field of WSN benefits from rank-

based key management in medical sensor networks and compressive thin penetrative protocols for energy-efficient data transfer..

3. Methodology

Data Collection:

First, gather data for the simulation configuration. This involves collecting medical sensor network data on node capabilities, communication patterns, and energy consumption. The simulation uses data from operational healthcare systems and wireless sensor networks to accurately represent real-life scenarios.

Processing data:

After collection, data is processed to extract simulation model parameters. This stage involves pattern identification, statistical analysis, and data normalization for consistency. Medical sensor network energy efficiency, latency, and security are examined.

Simulation Modelling:

Simulation uses ns-3 (Network Simulator 3). The simulation environment is configured using processed data. Authentic network scenarios can be created on the ns-3 platform to implement and test the Lightweight Authentication Protocol for Cloud-based Health-care Systems. Simulated results are used to assess the protocol's energy efficiency and latency.

LAPCHS

The Lightweight Authentication Protocol for Cloud-based Health-care Systems (LAPCHS) utilizes the BLAKE2 algorithm to provide a strong and energy-efficient method of authentication as depicted in algorithm-1, eq.1,2. This protocol is specifically designed for use in medical sensor networks (MSN). The system utilizes the BLAKE2 cryptographic hash function to establish robust mutual authentication and key agreement between resource-limited MSN and cloud servers. The LAPCHS presents numerous benefits compared to current authentication protocols. These advantages encompass its minimal resource requirements, high effectiveness, robust security measures, preservation of privacy, ability to handle increasing demands, scalability and real-world applicability.

LAPCHS addresses the security and energy efficiency concerns of MSN, thereby facilitating secure and dependable data transmission in cloud-based healthcare systems. This ultimately improves the privacy and security of sensitive patient information.

BLAKE2 Hash function

$$H(m) = H_{init} \oplus \Pi_{i=0}^{t}(h_i \oplus \sigma(h_i \oplus C_i \oplus m_i \oplus \Delta(t,i))) \quad ...(1)$$

LAPCHS Energy consumption for Secure and scalable data aggregation

$$E_{LAPCHS} = \alpha.H(m) + \beta.T_{comm} + \gamma.T_{comp} \quad ...(2)$$

where, $H(m)$= "Hash value of the message m", H_{init} = "Initial hash value", h_i = "Internal state variables", t = "no. of rounds", C_i = "Constant", $\Delta(t,i)$= "Mixing function", T_{comm} = "Total communication overhead", T_{comp} = "Total computational cost", α, β, γ = "Energy cost coefficients"

Algorithm 1: LAPCHS

```
// Tag Initialization
function tag_initialization():
    IDsk ← generate_random_secret_key()
    HIDsk ← BLAKE2_hash(IDsk)
    store HIDsk in non-volatile memory

// Authentication Request
function tag_authentication_request():
    N ← generate_random_nonce()
    HN ← BLAKE2_hash(N)
    send message to cloud server:
        TID, HN, N

// Server Authentication and Session Key Generation
function server_authentication_and_session_key_generation():
    receive message from tag:
        TID, HN, N
    retrieve stored secret key HIDsk from database
    HN' ← BLAKE2_hash(N, HIDsk)
    if HN' matches HN:
        authenticate tag
```

```
            SK ⟵ generate_random_session_key()
            HSK ⟵ BLAKE2_hash(SK)
            send message to tag:
                SID, HSK, N
// Tag Authentication and Session Key Establishment function
tag_authentication_and_session_key_establishment():
    receive message from server:
        SID, HSK, N
    verify HN' matches HSK
    if match:
        establish session key SK
        store SK in non-volatile memory

// Data Encryption and Transmission
function data_encryption_and_transmission():
    encrypt data using session key SK
    send encrypted data to cloud server

// Data Decryption and Processing
function data_decryption_and_processing():
    receive encrypted data from tag
    decrypt data using session key SK
    process decrypted data

// Session Termination
function session_termination():
    send termination message to other party
    invalidate session key SK
```

4. Results and Outputs

4.1 *Sample Network Simulation using NS-3*

The graph shows as in Figure 1 the network initial high energy efficiency and gradual decline. Due to node energy consumption during data transmission and reception. Nodes energy consumption increases as they transmit more data, decreasing energy efficiency. Energy efficiency is also affected by node proximity to the sink node. Nodes closer to the sink node consume less data transmission energy than those farther away. This is because nodes farther away must transmit data over a longer distance.

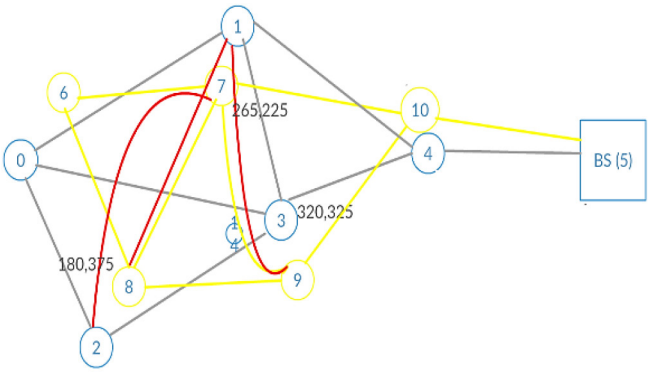

Figure 1

NS-3 simulation

The graph shows that energy-efficient routing protocols and clustering algorithms LAPCHS boost network energy efficiency. Energy-efficient routing protocols send data via the shortest or least energy-intensive path. Clustering algorithms group nodes and assign cluster heads. The cluster heads then consolidate and send data to the sink node from the remaining nodes. This reduces transmissions and boosts network energy efficiency. Transmission count and node-to-sink distance affect network and node energy efficiency, as shown in the graph. WSN can save energy with energy-efficient routing and clustering protocols.

4.2 *Evaluation Parameters*

Compares energy consumption and latency for varying numbers of nodes using the proposed method, ECC and AES as shown in Figure 2 and 3. The proposed method consistently surpasses ECC and AES in terms of energy consumption, regardless of the number of nodes. At 250 nodes, the proposed method exhibits a notable reduction in energy consumption (1200 units) compared to ECC (1450 units) and AES (1600 units). Moreover, the energy efficiency of the proposed method remains superior as the number of nodes increases. In terms of latency, the proposed method exhibits lower values across all node counts when compared to ECC and AES.

The outcome demonstrates that the suggested approach not only efficiently preserves energy but also operates with decreased latency, rendering it a promising option for use in environments with limited resources.

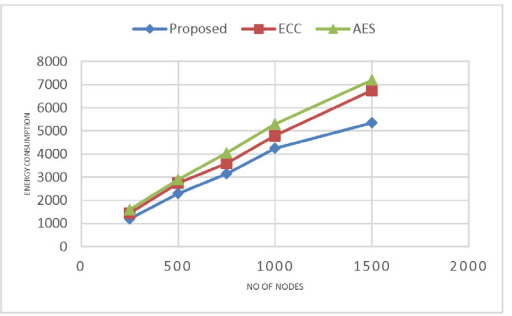

Figure 2

Energy Consumption

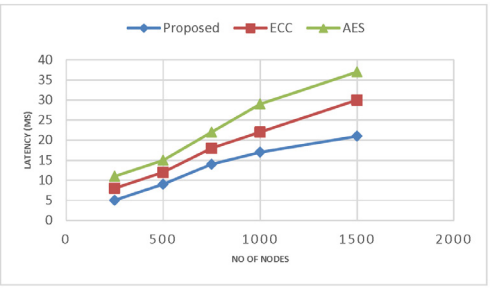

Figure 3

Latency

4. Conclusion and Future Scope

The study presents the Lightweight Authentication Protocol for Cloud-based Health-care Systems (LAPCHS) for secure and scalable data aggregation which uses the BLAKE2 cryptographic hash algorithm. This protocol provides a strong and energy-efficient method for authenticating medical sensor networks. LAPCHS utilizes innovative techniques to effectively overcome the resource constraints of sensor nodes, achieving a delicate equilibrium between robust security measures and efficient energy utilization. The protocol's utilization of BLAKE2 enables strong mutual authentication and key establishment between the tag and the cloud server, establishing a lightweight yet highly efficient method suitable for implementation in medical sensor networks. The use of LAPCHS greatly decreases the requirement for global key distribution, thus reducing communication overhead and prolonging the lifespan of devices. The study's results highlight the superior performance of LAPCHS compared to existing methods, demonstrating its exceptional energy

efficiency and low latency, while also maintaining a high level of security. The future prospects of this study entail conducting additional scalability tests on LAPCHS for larger medical sensor networks and investigating its ability to adapt to dynamic healthcare settings. In addition, exploring the incorporation of cutting-edge technologies, such as blockchain, to improve the reliability and security of data could strengthen LAPCHS capabilities. Additional investigation could also concentrate on hardware enhancements and practical applications to verify the effectiveness of LAPCHS in actual medical environments, consolidating its status as a promising remedy for guaranteeing robust and energy-efficient authentication in healthcare-oriented WSN.

References

[1] 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, p. 100126 (2023), doi: 10.1016/j.hcc.2023.100126.

[2] A. B. Feroz Khan and G. Anandharaj, "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT," *SN Appl. Sci.*, vol. 1, no. 12, pp. 1–7 (2019), doi: 10.1007/s42452-019-1628-4.

[3] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography,* 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[4] L. Kaur and R. Kaur, "A survey on energy efficient routing techniques in WSNs focusing IoT applications and enhancing fog computing paradigm," *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 520–529 (2021), doi: 10.1016/j.gltp.2021.08.001.

[5] B. S. Kim and J. S. Song, "Pseudonymous mobile node reauthentication scheme for mobile wireless sensor networks," *ACM Int. Conf. Proceeding Ser.*, pp. 294–299 (2019), doi: 10.1145/3377170.3377207.

[6] G. Mehmood *et al.*, "An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network," *Complexity*, vol. 2021 (2021), doi: 10.1155/2021/6577492.

[7] C. Nakas, D. Kandris, and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms*, vol. 13, no. 3, pp. 1–65 (2020), doi: 10.3390/a13030072.

[8] A. S. H. Abdul-Qawy *et al.*, "An enhanced energy efficient protocol for large-scale IoT-based heterogeneous WSNs," *Sci. African*, vol. 21, no. April, p. e01807 (2023), doi: 10.1016/j.sciaf.2023.e01807.

[9] J. A. I. Syed Masood, M. Jeyaselvi, N. Senthamarai, S. Koteswari, M. Sathya, and N. S. K. Chakravarthy, "Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data," *Meas. Sensors*, vol. 29, no. April, p. 100867 (2023), doi: 10.1016/j.measen.2023.100867.

[10] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT applications – A comprehensive survey," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 2, pp. 651–681 (2023), doi: 10.1016/j.jksuci.2023.01.008.

[11] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[12] D. P. Singh and R. H. Goudar, "Energy efficient clearance routing in WSN," *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, no. s2, pp. 555–575 (2017), doi: 10.1007/s13198-014-0263-0.

[13] M. Krishnapriya, G. Angeline Prasanna, and S. Anbarasu, "Rank-Based Energy-Efficient Key Management Routing For Wireless Sensor Network-Based Iot Medical Sensors," *Wirel. Pers. Commun.*, vol. 130, no. 3, pp. 2175–2196 (2023), doi: 10.1007/s11277-023-10377-5.

[14] V. Reddy and P. Gayathri, "Energy efficient data transmission in WSN thru compressive slender penetrative etiquette," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 11, pp. 4681–4693 (2020), doi: 10.1007/s12652-020-01724-6.

[15] M. Shafiq, H. Ashraf, A. Ullah, and S. Tahira, "Systematic Literature Review on Energy Efficient Routing Schemes in WSN – A Survey," *Mob. Networks Appl.*, vol. 25, no. 3, pp. 882–895 (2020), doi: 10.1007/s11036-020-01523-5.

[16] B. Sureshand and S. G, "An ENERGY EFFICIENT SECURE routing Scheme using LEACH protocol IN WSNS for IOT networks," *Meas. Sensors*, vol. 30, no. February, p. 100883 (2023), doi: 10.1016/j.measen.2023.100883.