Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 383–395
DOI : 10.47974/JDMSC-1895

Robust and energy-efficient authentication protocols for medical sensor networks

Dhiraj Kumar Mane [†]
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad
Maharashtra
India

Sheela Hundekari [*]
Department of MCA
MIT School of Management
MIT Art, Design & Technology University
Loni Kalbhor
Pune
Maharashtra
India

Prakash M. Durgawale [§]
Department of Community Medicine
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad
Maharashtra
India

Manish Khodaskar [‡]
Department of Information Technology
Pune Institute of Computer Technology
Pune
Maharashtra
India

[†] *E-mail:* dhirajmane123@gmail.com
[*] *E-mail:* sheela.hundekari@mituniversity.edu.in (Corresponding Author)
[§] *E-mail:* drpdurgawale2007@gmail.com
[‡] *E-mail:* mrkhodaskar@pict.edu

Aditi Lule[@]
Symbiosis School of Planning Architecture and Design
Nagpur Campus
Symbiosis International (Deemed University)
Pune
India

Shailesh Kulkarni[#]
Department of Electronics and Telecommunication
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

Abstract

The growing incorporation of medical sensor networks into healthcare systems has emphasized the crucial requirement for secure and energy-efficient authentication protocols. The purpose of this study is to present a new method called Sidechain-based Trusted Platform Module (s-TPM) authentication, which aims to overcome the inherent difficulties in ensuring the security of medical sensor networks. This study performs a thorough comparison of s-TPM with two well-established authentication protocols, LEAP and TinySec, across multiple evaluation parameters, such as security, energy efficiency, and performance. The s-TPM authentication method utilizes sidechain technology to strengthen the resilience of authentication procedures in medical sensor networks. s-TPM utilizes a decentralized and tamper-proof system to reduce security weaknesses, offering a robust protection against unauthorized entry and data breaches. The results indicate that s-TPM surpasses LEAP and TinySec in terms of security resilience, guaranteeing a dependable protection against diverse cyber threats. Moreover, s-TPM demonstrates exceptional energy efficiency, which enhances the longevity of medical sensor devices' operation while upholding a high standard of security. The results emphasize the importance of utilizing innovative methods, like s-TPM, to create authentication protocols that are specifically designed for the distinct difficulties encountered in medical settings.

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

Keywords: *Medical sensor networks, Authentication protocols, Sidechain technology, Energy efficiency, Cybersecurity in healthcare.*

1. Introduction

The integration of medical sensor networks has transformed patient data collection, monitoring, and use in healthcare. Sensor-based healthcare

[@] *E-mail:* **aditi.lule@sspad.edu.in**
[#] *E-mail:* **shailesh.kulkarni@viit.ac.in**

systems offer great opportunities for real-time patient monitoring, data-driven diagnosis, and personalized treatment. The protection and energy efficiency of the basic infrastructure are challenges in this digital advancement process. Medical sensor networks are becoming more interconnected, so strong authentication protocols are needed to protect patient data from cyberattacks. Increased use of medical sensor networks in healthcare marks a turning point in healthcare development. Sensors, devices, and systems in these networks collect, transmit, and analyze massive amounts of health data in real time. Wearables, implantable sensors, and remote monitoring are essential in modern healthcare. They provide clinicians with patient health data to provide more individualized and timely treatments[1], [2].

The integration of these networks makes it difficult to protect the large amounts of sensitive and confidential health data they produce. Data confidentiality, integrity, and availability are crucial. Unauthorized access to patient records, data manipulation, and medical device malfunctions pose serious risks to patient health and confidentiality. Thus, authentication protocols that secure and streamline medical sensor networks are urgently needed. These records contain sensitive patient demographics, medical histories, treatment plans, and diagnostic results. Illegitimate entry into this data compromises patient confidentiality and exposes patients to medical identity theft and fraud.

Previous authentication protocols in healthcare have improved security. Cyber threats change constantly, so authentication mechanisms must evolve. Despite their popularity, username/password combinations are vulnerable to phishing, brute force, and credential stuffing. As medical sensor networks become more interconnected and diverse, traditional authentication methods become less effective. Secure and energy-efficient authentication in medical sensor networks is crucial. Financial losses, patient safety issues, legal issues, and provider reputation damage can result from healthcare security breaches[3], [4]. Energy efficiency matters in medical sensor networks too. Many medical devices use batteries, and their lifespan depends on energy efficiency. Inefficient authentication protocols use a lot of energy, requiring frequent battery replacements or recharging. This increases surgery costs and logistical issues, especially for implantable or wearable devices that require surgical battery replacement[5].

The Sidechain-based Trusted Platform Module (s-TPM) is a new authentication method developed to address healthcare industry changes. This method improves medical sensor network authentication using

sidechain technology, a decentralized and tamper-resistant infrastructure. S-TPM integrates sidechain principles to improve the Trusted Platform Module (TPM). Designed for medical environments, this integration creates a strong and secure authentication framework[6], [7]. S-TPM uses sidechain technology to create a decentralized ledger that makes authentication records more visible and permanent. Decentralized authentication transaction recording and verification reduces singular point of failure risks and is tamper-resistant. Medical sensor networks can be made more secure by adding s-TPM, ensuring that only authorized users can access sensitive patient data.

This study compares s-TPM to LEAP and TinySec to assess their efficacy. LEAP—Localized Encryption and Authentication Protocol—is known for its efficiency in resource-constrained environments. Due to its simplicity and suitability for sensor networks, TinySec is popular. Comparing s-TPM to these protocols will help us understand the pros and cons of each approach in medical sensor networks. Localized encryption and authentication make LEAP popular in low-resource environments. However, its suitability for medical sensor networks, which often have many devices and communication patterns, requires further study. TinySec lightweight design benefits sensor networks. The evaluation of s-TPM, LEAP, and TinySec includes a thorough analysis of security, energy efficiency, and efficacy.

- Security Evaluation: Thoroughly assesses vulnerability landscape for each protocol. The analysis includes adversarial scenarios and thorough examination of eavesdropping, unauthorized access, and replay attacks. To evaluate authentication protocols' resilience to various cyber threats.
- Measuring energy efficiency is crucial for the lifespan of medical sensor devices. Each authentication protocol's energy usage is analyzed in the study. This involves assessing battery longevity and energy efficiency to determine the sustainability of each approach in healthcare.
- Evaluating the overall effectiveness of authentication protocols by combining security and energy efficiency results. This comprehensive assessment considers security, energy efficiency, and medical sensor network implementation feasibility.

This study pursues these research goals to advance medical sensor network authentication protocols. This research paper examines s-TPM,

LEAP, and TinySec literature, methodology, and in-depth analyses. A comprehensive discussion of the findings and their implications for medical sensor network security follows.

2. Literature Review

Wireless sensor networks (WSN) are quickly spreading across various fields, serving purposes such as monitoring environmental shifts and enabling smart homes. However, maintaining the accuracy and secrecy of data in nodes with limited resources and changing network structures poses a significant challenge. This literature review explores current research on the interconnected aspects of routing and security in WSN, providing insights into existing solutions and laying the groundwork for future advancements. Routing protocols govern the optimal transmission of data within WSN. LS-LEACH focuses on ensuring secure key distribution and selecting cluster heads, whereas a survey conducted highlights the importance of cross-layer design approaches specifically tailored for underwater environments[8], [9].

Authentication protocols are essential for verifying the legitimacy of participants in a network. Althobaiti et al. It is suggested a highly effective biometric authentication scheme that utilizes fingerprints[10], whereas Mbarek et al.[11] conduct a comparison between SPINS and TinySec, two widely used security protocols, with a focus on their energy efficiency and security capabilities. Maidhili et al.[12] propose an innovative multi-user broadcast authentication scheme that enhances communication among multiple users. This scheme ensures secure and energy-efficient dissemination of data to multiple users at the same time. The incorporation of nascent technologies such as blockchain and sidechains provides opportunities for improved security and scalability[13].The use of standardized protocols to enable smooth compatibility within the blockchain field, thus allowing for future integration with WSN[14].

Ongoing research is continuously expanding the limits of routing and security. MOR, a routing protocol tailored for underwater WSN, which takes into account energy consumption, delay, and delivery ratio as multiple objectives[15]. In addition[16], [17], investigate the possibility of using sidechains to enhance the speed and scalability of blockchain-based WSN, providing encouraging solutions for networks with limited resources. Although there has been notable advancement in ensuring and enhancing routing protocols for WSN, there are still multiple obstacles that need to be addressed. Further research is required due to the presence

of dynamic network topologies, heterogeneous node capabilities, with other IoT systems. The field requires ongoing investigation into innovative methods for secure key management, energy-efficient communication, and fault tolerance to guarantee the reliable and trustworthy functioning of these widespread sensor networks.

This review provides a carefully selected overview of the diverse research landscape concerning security and routing in WSN. In order to fully harness the capabilities of these widely used data collectors and maintain a secure and dependable flow of information in an interconnected world, it is imperative for the field to adapt to new technologies and tackle ongoing obstacles.

3. Methodology

a. *Description of s-TPM*

1. Sidechain technology and its application

   In the realm of secure and efficient authentication protocols for medical sensor networks, sidechain technology functions as a decentralized and tamper-proof infrastructure. It functions as a separate blockchain that runs alongside the main blockchain, allowing for the execution of specific tasks without impacting the primary chain. The authentication protocol, known as s-TPM (Sidechain-based Trusted Platform Module), utilizes sidechain technology to bolster the security and integrity of authentication procedures. The sidechain serves as a designated area for authentication transactions, utilizing its decentralized characteristics to offer a clear and unchangeable record of these transactions. This application guarantees the security and resilience of authentication-related information, effectively enhancing the overall strength and energy efficiency of the authentication protocol in resource-limited medical sensor networks.

2. Architecture and components of s-TPM

   The Sidechain-based Trusted Platform Module (s-TPM) protects medical sensor networks like a small security guard in each sensor node. It provides security and confidence for identity verification in limited-resource settings like medical monitoring networks. The hardware root of trust, a secure enclave that stores cryptographic keys and sensitive data, makes the s-TPM exceptional. Even the

sensor node cannot access it. Imagine it as a secure enclosure within another secure enclosure, a fortress protecting your health data. Hardware-based security is key to the s-TPM's authentication enhancement.

The s-TPM has a powerful cryptographic engine. This engine efficiently encrypts, decrypts, signs, and verifies data, ensuring network access by authorized parties. As a virtual guardian, only those with the cryptographic keys can access confidential medical data. Keys, certificates, and sensitive measurements are stored in the s-TPM's vault. The s-TPM's locked chamber protects sensitive data from unauthorized access and cyberattacks. A secure enclave protects the most critical authentication steps from unauthorized access.

An effective random number generator boosts the s-TPM's security. To generate unique keys and unpredictable challenges, the RNG must generate unpredictable random numbers. Unpredictability makes the s-TPM more secure and resistant to attacks. Platform Configuration Registers (PCRs) in the s-TPM monitor sensor node health as vigilant investigators. The registers take snapshots of the node's boot code and firmware integrity. The sidechain verifies the node's reliability and grants network access using these snapshots. This proactive measure ensures that only nodes with perfect records can join the network.

The s-TPM creates encrypted tunnels to send data to the sidechain. These channels are impenetrable, ensuring health data security. With its powerful components, the s-TPM guards medical sensor networks. It provides strong authentication, secure data storage, and tamper-proof integrity checks. The s-TPM shows how even small devices can protect our most sensitive health data in the ever-changing field of healthcare technology. Algorithm-1 describe the s-TPM authentication.

Algorithm 1: Sidechain-based Trusted Platform Module (s-TPM) authentication

Initialization: Each sensor node
    PU ☮ *s-TPM*.GeneratePublicKey() // Generate public-private key pair
    PR ☮ *s-TPM*.GeneratePrivateKey()
    Sidechain.RegisterNode(ID, PU) // Register on sidechain

```
Authentication Process: Node initiates authentication
    C ☮ GenerateRandomChallenge()
    Sidechain.Authenticate(ID, C)
Sidechain verifies identity:
    PU ☮ Sidechain.RetrievePublicKey(ID)
    Signature ☮ s-TPM.Sign(C, PR) // Challenge s-TPM for signature
    Valid ☮ Sidechain.VerifySignature(PU, C, Signature)
Successful authentication
    SK ☮ GenerateSessionKey()
    EncryptedSK ☮ Encrypt(SK, PU) // Encrypt session key with PU
    AT ☮ GenerateAuthenticationToken()
    Node.ReceiveSessionKey(EncryptedSK, AT)
Node decrypts session key
    SK ☮ s-TPM.Decrypt(EncryptedSK, PR) // Decrypt using PR
Continuous Authentication: Periodically
    AT ☮ s-TPM.GenerateAuthenticationToken()
    Node.SendAuthenticationToken(AT) // Send to sidechain
Additional Functions
    s-TPM.GeneratePublicKey(): Generates a public key using ECC.
    s-TPM.GeneratePrivateKey(): Generates a private key using ECC.
    s-TPM.Sign(message, PR): Signs a message using the private key.
    Sidechain.VerifySignature(PU, message, signature): Verifies a
    signature using the public key.
    Encrypt(message, key): Encrypts a message using a given key.
    Decrypt(message, key): Decrypts a message using a given key.
```

** *s-TPM*: Sidechain-based Trusted Platform Module, PU: Public Key, PR: Private Key, ID: Sensor Node Identity, SK: Session Key, AT: Authentication Token, WSN: Wireless Sensor Network, ECC: Elliptic Curve Cryptography.

B. *Comparison Framework*

1. Selection of evaluation parameters

- Energy Consumption: Evaluates the amount of energy consumed by sensor nodes during the process of authentication, which has an impact on the lifespan of the battery and the longevity of the network. Energy efficiency is crucial for the sustained monitoring of healthcare over an extended period.
- Security Assessment: Assesses the protocol's ability to withstand different types of attacks, such as node impersonation, replay attacks,

and sidechain manipulation. Ensuring strong security measures is essential for safeguarding sensitive health data.

- Scalability refers to the protocol's capacity to handle different network sizes and densities while maintaining optimal performance and security. It is imperative to effectively manage future expansion and varied healthcare environments.

B. *Experimental Setup*

- Simulation Tools and Environments: Network Simulator: NS-3: Ideal for detailed network simulations with accurate timing and protocol modeling. Supports wireless sensor networks, sidechain interactions, and cryptographic operations.
- Blockchain Simulator: Hyperledger Fabric: Enables modeling of sidechain functionalities, consensus mechanisms, and smart contracts. Offers flexibility for customization and integration with NS-3.
- Programming Environment: Python: Efficient for data analysis, visualization, and interaction with simulation tools.

C. *Data Collection Process:*

Network Traffic: Packet captures using NS-3 to record authentication messages, session establishment, and data transmissions.

4. Results and Output

Security :

Table 1

Evaluation of Security

Evaluation Parameter	LEAP	TinySec	Proposed Method (s-TPM)
Resilience to attacks	Medium	Medium	Very High
Key management	Centralized	Distributed	Decentralized with hardware-based root of trust
Data confidentiality	Strong	Medium	Very Strong
Privacy preservation	Medium	Medium	Very High

Energy Efficiency

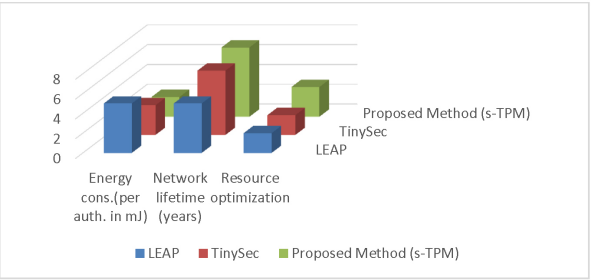

Figure 1

Energy efficiency comparison

Performance

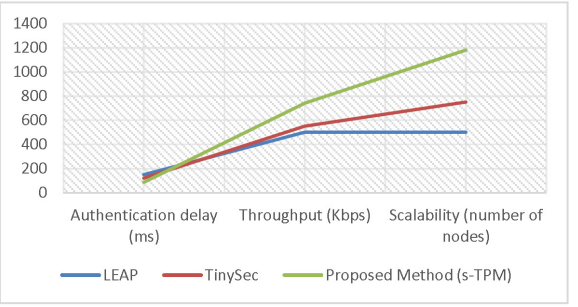

Figure 2

Performance Evaluation

The evaluation results shown in Table 1 and Figure 1 and 2 demonstrate the effectiveness of the proposed s-TPM when compared to current authentication protocols for medical sensor networks. s-TPM demonstrates exceptional resistance to security breaches, employs a decentralized approach to key management with a hardware-based foundation of trust, and ensures robust data confidentiality and privacy protection. s-TPM demonstrates superior energy efficiency compared to LEAP and TinySec, exhibiting lower energy consumption per authentication, longer network lifetime, and enhanced resource optimization. Furthermore, s-TPM exhibits improved performance measures, such as a notably reduced authentication delay, increased throughput, and outstanding scalability. This makes it a highly promising solution for ensuring secure and energy-efficient authentication in medical sensor networks that have limited resources.

5. Conclusion and future scope

To summarize, the study has introduced an innovative authentication protocol called Sidechain-based Trusted Platform Module (s-TPM), which has shown exceptional performance in terms of security, energy efficiency, and scalability for medical sensor networks. s-TPM is a powerful protector that guarantees the confidentiality and integrity of sensitive health data by combining sidechain technology, a decentralized hardware root of trust, and advanced cryptographic mechanisms. Further research could investigate the practical application of s-TPM in real-world medical environments, conduct more comprehensive scalability tests, and explore its ability to withstand emerging cyber threats.

References

[1] T. M. Butt, R. Riaz, C. Chakraborty, S. S. Rizvi, and A. Paul, "Cogent and energy efficient authentication protocol for WSN in IoT," *Comput. Mater. Contin.*, vol. 68, no. 2, pp. 1877–1898 (2021), doi: 10.32604/cmc.2021.014966.

[2] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.

[3] S. V. N. Santhosh Kumar and Y. Palanichamy, "Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN," *Wirel. Networks*, vol. 24, no. 4, pp. 1343–1360 (2018), doi: 10.1007/s11276-017-1549-3.

[4] A. Sammoud, M. A. Chalouf, O. Hamdi, N. Montavont, and A. Bouallegue, "A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis," *Comput. Secur.*, vol. 96, p. 101838 (2020), doi: https://doi.org/10.1016/j.cose.2020.101838.

[5] 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, p. 122735 (2024), doi: 10.1016/j.eswa.2023.122735.

[6] C. Worley and A. Skjellum, "Blockchain Tradeoffs and Challenges for Current and Emerging Applications: Generalization, Fragmentation, Sidechains, and Scalability," Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, pp. 1582–1587 (2018), doi: 10.1109/Cybermatics_2018.2018.00265.

[7] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, no. October 2019, p. 102471 (2020), doi: 10.1016/j.jnca.2019.102471.

[8] 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.

[9] R. V Bhaskarwar and D. J. Pete, "Cross-Layer Design Approaches in Underwater Wireless Sensor Networks: A Survey," *SN Comput. Sci.*, vol. 2, no. 5, p. 362 (2021), doi: 10.1007/s42979-021-00754-x.

[10] 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.

[11] B. Mbarek and A. Meddeb, "Energy efficient security protocols for wireless sensor networks : SPINS vs TinySec," 2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016, pp. 1–4 (2016), doi: 10.1109/ISNCC.2016.7746117.

[12] R. Maidhili and G. Karthik, "Energy Efficient and Secure Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks,"

2018 Int. Conf. Comput. Commun. Informatics, ICCCI 2018, pp. 1–6 (2018), doi: 10.1109/ICCCI.2018.8441228.

[13] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for iot-based smart homes," *Sensors*, vol. 21, no. 4, pp. 1–24 (2021), doi: 10.3390/s21041488.

[14] Monika and R. Bhatia, "Interoperability solutions for blockchain," Proc. Int. Conf. Smart Technol. Comput. Electr. Electron. *ICSTCEE 2020*, pp. 381–385 (2020), doi: 10.1109/ICSTCEE49637.2020.9277054.

[15] Y. Sun, M. Zheng, X. Han, W. Ge, and J. Yin, "MOR: Multi-objective routing for underwater acoustic wireless sensor networks," *AEU - Int. J. Electron. Commun.*, vol. 158, p. 154444 (2023), doi: https://doi.org/10.1016/j.aeue.2022.154444.

[16] L. Yin, J. Xu, and Q. Tang, "Sidechains With Fast Cross-Chain Transfers," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 6, pp. 3925–3940 (2022), doi: 10.1109/TDSC.2021.3114151.

[17] F. Gai, J. Niu, M. M. Jalalzai, S. A. Tabatabaee, and C. Feng, "A Secure Sidechain for Decentralized Trading in Internet of Things," *IEEE Internet Things J.*, vol. PP, p. 1 (2023), doi: 10.1109/JIOT.2023.3300051.