Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika
Volume 3, Nomor.4 Juli 2025
e-ISSN: 3031-349X; p-ISSN: 3031-500X, Hal 283-294
DOI: https://doi.org/10.61132/jupiter.v3i4.1024
Available online at: https://journal.aritekin.or.id/index.php/Jupiter

A Lightweight and Secure Protocol for Wireless Medical Sensor Networks in IoT Systems

Assaad Essa Omran Murad
Fakultas Teknik Elektro dan Komputer, Universitas Islam Azad, Iran

*Korespondensi Penulis: assadissa50@gmail.com**

Abstract. *Wireless Medical Sensor Networks (WMSNs) are a key component of modern Healthcare Internet of Things (IoT) systems, enabling continuous and real-time monitoring of patients' physiological parameters. These networks support timely medical intervention, improve patient outcomes, and facilitate remote healthcare delivery. However, due to the open and resource-constrained nature of WMSNs, they are highly susceptible to various security threats, particularly during the authentication phase. Existing authentication protocols have been found vulnerable to a range of attacks, including impersonation, session key disclosure, and gateway database compromise, which can lead to severe privacy breaches and potentially life-threatening situations. To address these issues, this paper proposes a secure and lightweight three-factor authentication protocol tailored for WMSNs in healthcare IoT environments. The proposed protocol integrates Elliptic Curve Cryptography (ECC) for strong public key-based security with minimal computational overhead, fuzzy extractors to securely handle biometric information and ensure resistance against biometric template compromise, and session-based randomness to achieve forward secrecy and prevent replay or key-compromise impersonation attacks. Security analysis demonstrates that the proposed protocol successfully mitigates prominent threats such as impersonation attacks, man-in-the-middle attacks, session key leakage, and database compromise. In addition, the protocol ensures mutual authentication between the user, the gateway, and the sensor nodes, while maintaining data confidentiality and integrity. Performance evaluation indicates that the protocol offers significantly reduced computational cost and communication delay compared to existing schemes. Its low energy consumption and minimal storage requirements make it suitable for deployment in resource-constrained medical devices and large-scale IoT healthcare networks. The results highlight the protocol's scalability, energy efficiency, and robustness, making it a practical and secure solution for safeguarding patient data and ensuring trustworthy communication in WMSNs-based healthcare IoT systems.*

Keywords: *Authentication, ECC, Internet of Things, Obscurity, WMSN*

Abstrak.Wireless Medical Sensor Networks (WMSNs) merupakan komponen penting dalam sistem Internet of Things (IoT) di bidang kesehatan, yang memungkinkan pemantauan pasien secara terus-menerus dan real-time terhadap parameter fisiologisnya. Teknologi ini mendukung intervensi medis tepat waktu, meningkatkan hasil perawatan pasien, serta memfasilitasi layanan kesehatan jarak jauh. Namun, karena sifatnya yang terbuka dan keterbatasan sumber daya, WMSNs sangat rentan terhadap berbagai ancaman keamanan, khususnya pada tahap autentikasi. Protokol autentikasi yang ada saat ini terbukti memiliki kelemahan terhadap berbagai serangan, termasuk serangan penyamaran (impersonation), pengungkapan kunci sesi, dan kompromi basis data gateway, yang dapat mengakibatkan pelanggaran privasi serius dan bahkan membahayakan nyawa pasien. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan protokol autentikasi tiga faktor yang aman dan ringan, dirancang khusus untuk WMSNs pada lingkungan IoT kesehatan. Protokol ini mengintegrasikan Elliptic Curve Cryptography (ECC) guna memberikan keamanan berbasis kunci publik dengan beban komputasi minimal, fuzzy extractor untuk menangani informasi biometrik secara aman dan melindungi dari kompromi template biometrik, serta penggunaan kerandoman berbasis sesi untuk mencapai forward secrecy dan mencegah serangan replay maupun key-compromise impersonation. Analisis keamanan menunjukkan bahwa protokol yang diusulkan berhasil mengatasi berbagai ancaman utama seperti serangan penyamaran, man-in-the-middle, kebocoran kunci sesi, dan kompromi basis data. Selain itu, protokol ini menjamin autentikasi timbal balik antara pengguna, gateway, dan node sensor, sekaligus menjaga kerahasiaan serta integritas data. Evaluasi kinerja menunjukkan bahwa protokol ini memiliki biaya komputasi dan keterlambatan komunikasi yang lebih rendah dibandingkan skema yang sudah ada. Konsumsi energinya yang rendah dan kebutuhan penyimpanan minimal menjadikannya layak digunakan pada perangkat medis yang memiliki keterbatasan sumber daya maupun pada jaringan IoT kesehatan berskala besar. Hasil penelitian menegaskan skalabilitas, efisiensi energi, dan ketahanan protokol ini,

Received: Juni 25,2025; Revised: Juni 12,2025; Accepted: Juli 13, 2025; Pubished: Juli 30, 2025

sehingga menjadi solusi praktis dan aman untuk melindungi data pasien serta memastikan komunikasi yang tepercaya pada sistem IoT kesehatan berbasis WMSNs.

Kata Kunci: Autentikasi, ECC, *Internet of Things*, Ketidakjelasan, WMSN

1. INTRODUCTION

The rapid evolution rate of Wireless Medical Sensor Networks (WMSNs) has, to a large degree, transformed healthcare systems by providing real-time, non-stop monitoring of critical patient health parameters [1-3]. The heart rate, blood pressure, blood sugar levels, and body temperature are now monitored constantly using low-power, lightweight sensors attached to or implanted inside the human body. These sensors capture and transmit information wirelessly, allowing healthcare providers to make timely, data-driven decisions even from remote areas. This integration of WMSNs into Healthcare IoT systems is a paradigm shift in the delivery of healthcare services by enabling improved patient care, early diagnosis, and better chronic disease management. However, since healthcare infrastructures increasingly use wireless communication and IoT technologies to operate, they are exposed to serious security attacks that will threaten patient confidentiality and system integrity. The most emphasized problem is that WMSNs are under different attack vulnerabilities. Due to its nature, the open wireless communication system is vulnerable to eavesdropping, interception, tampering, and unauthorized access. Additionally, sensor node inadequacies in power battery, computation, and memory make it even more difficult to implement secure communication protocols [4]. Authentication is a critical parameter in this type of environment to render sensitive medical information confidential, secure, and accessible [5-6]. Appropriate authentication procedures for the circumstances need to be employed in order to validate medical equipment, users, and systems prior to granting them access to essential information. In the absence of secure authentication, the data on the network may be made susceptible to various types of attacks, resulting in identity theft, false medical history, or incorrect treatment plans. Therefore, in the context of healthcare IoT systems, low-energy, secure, and lightweight authentication protocols become a necessity. Existing WMSN authentication protocols, including those presented by Servati and Safkhani [7] and Thakur et al. [8], strive to address these challenges. But they have proved vulnerable to various attacks, including impersonation (attackers may impersonate authentic users or devices), offline password guessing (attackers may attempt to guess the user password offline), and gateway database compromise (attackers may gain access to stored sensitive information on the gateway, e.g., session keys). These vulnerabilities provide potential points of entry for criminals to strike patient data and the integrity of the

healthcare infrastructure.Despite the progress in authentication mechanisms, these schemes have not managed to satisfy the high demands of healthcare IoT systems [9], which require robust security without requiring radical computational burdens. The processing capabilities and memory constraints of gateways and sensor nodes necessitate authentication solutions that don't create heavy processing loads on these devices to ensure they can operate efficiently and uninterruptedly. Therefore, it is a pressing necessity to have a better authentication protocol that will be able to provide good security along with being resource-savvy [10].

This paper attempts to fill this gap by proposing a lightweight and secure three-factor authentication protocol for WMSNs that can be suitable for healthcare IoT systems. The protocol employs ECC for efficient key exchange, fuzzy extractors to secure biometric data, and session-based randomness for forward secrecy support. These mechanisms support one another to enhance the protocol's resilience against common attacks and decrease computation and communication overhead—a significant property for the protocol's deployment within resource-limited medical settings. By enhancing security and efficiency, this work presents an efficient and scalable solution for real-time health applications that place importance on securing patient information.

The paper proceeds with Related Works in Section 2. Discussing Methodology development in section 3. The results are presented in Section 4. The discussion is presented in Section 5, by conclusions and recommendations in Section 6.

Related Works

Wireless Medical Sensor Networks (WMSNs) are a central entity of Healthcare IoT systems, enabling real-time monitoring of patients via the gathering of vital health data [11-13]. Though promising, WMSNs are at high risk of security threats, particularly during the authentication phase. Impersonation attacks, session key disclosure, and gateway database compromise are some of the vulnerabilities that are patient privacy and data integrity risks. Here, multiple medical device-specific solutions have been created to address these problems with optimization for the medical device restrictions, such as low power and processing capacity. For instance, to render access through the IoT environment possible, Gupta et al. [14] introduced a secure authentication protocol and key establishment technique for application within smart cities. The security analysis demonstrates that the suggested protocol is efficient on energy consumption and possesses lower computational overhead. It provides mutual authentication of gateways and users as well. The performance of the proposed method is verified and tested with BAN Logic and AVISPA security verification to find out whether the

security protocol is authentic or not. We do make the comparison with previous work, and our proposed method proved better. Ayeswarya et al. [15] bridged this gap by the examination of recent advances, trends, and challenges in CAS design. It identifies that while supervised learning, in particular score-level fusion, is the current CAS classification method, comparison of different biometric combinations (e.g., physiological, behavioral, multimodal) is scarce. While accuracy metrics in the form of FRR, FAR, and EER are evaluated, important factors such as usability, security, and scalability are not considered. Analysis of real-world data is required for the real-world application of CAS. In this paper, various dimensions of CAS, including biometrics, context-aware approaches, and emerging methodologies, are discussed, identifying challenges and future research directions. Zhao et al. [16] proposed a multi-gateway light authentication scheme to counteract security issues in large-scale IoT networks that are usually based on single gateway authentication schemes. They introduced a three-factor authentication system by implementing Chebyshev chaotic mapping, a hash function, and XOR functions to establish safe communication between sensor nodes and users. The scheme not only provides secure authentication but also establishes session keys and provides user key updating. Through security analysis, it is demonstrated that the scheme is secure against a range of attacks, i.e., internal disguise, sensor capture, and temporary secret leakage attacks, and moreover, offers forward security. Semantic security of session keys is also demonstrated using the Random Oracle Model (ROM). The scheme presented here reduces communication overhead and computation resource consumption, thereby offering more support for lightweight IoT security applications.

Existing IoT authentication protocols rely on single gateway models that have low scalability, leading to high communication overhead and reduced performance. Multi-factor authentication is under research, but the combination of Chebyshev chaotic mapping, hash functions, and XOR operations is less explored. In addition, the majority of protocols lack complete security analysis, particularly for certain attacks like internal disguise and sensor capture. Forward and semantic security of session keys are also not adequately addressed. Current solutions fail to find a balance between strong security and lightweight design for constrained devices. The suggested scheme fills the following gaps by proposing a multi-gateway, three-factor authentication protocol that offers security with reduced overhead, making it suitable for large-scale IoT networks.

2. METHODOLOGY

This section provides the methodology followed to design and analyze the proposed lightweight and secure three-factor authentication protocol in Wireless Medical Sensor Networks (WMSNs) in Healthcare IoT networks. The methodology followed is systematic in nature, including protocol designing, security analysis, and performance evaluation. The key building blocks of the proposed protocol include Elliptic Curve Cryptography (ECC) for lighter cryptography, fuzzy extractors for protecting biometric information, and session-based randomness for the sake of forward secrecy.

Protocol Design

The proposed authentication protocol is based on three-factor authentication utilizing the application of the combination of the following factors:

1. Password-based Authentication: The user's identity is first verified based on a password, a simple yet secure means of authentication.
2. Biometric Authentication: There is application of a biometric feature, i.e., fingerprint or retina scan, for added security. This ensures that the user is himself/herself by his/her physical features.
3. Smart Card Authentication: An authentication hardware token in the form of a smart card that offers a second level of protection and restricts man-in-the-middle or replay attacks.
4. All three of these, used together, make for a very secure form of authentication, much more secure than basic single-factor approaches.
5. All three of these, used together, make for a very secure form of authentication, much more secure than basic single-factor approaches.

Elliptic Curve Cryptography (ECC) for Key Exchange

The protocol takes advantage of Elliptic Curve Cryptography (ECC) to facilitate secure key agreement and data encryption. ECC has the advantage of smaller key sizes with similar security levels compared to current public key cryptosystems such as RSA. This means less computational burden for resource-limited devices such as medical sensors while enjoying high security. The protocol uses ECC for:

- Secure exchange of session keys between the user, gateway, and sensor nodes.
- Encrypt the communication between parties to provide integrity and confidentiality for sensitive patient data.

The use of ECC ensures the key exchange process to be effective as well as secure, an aspect in real-time health care applications where fast and reliable data transport is a necessity.

Fuzzy Extractors for Biometric Data Protection

Biometric data, such as fingerprints or iris scans, is usually noisy and error-prone because of sensor accuracy and environmental factors. For securing such information, we utilize fuzzy extractors that transform biometric information into a secure cryptographic key that is noise-resistant or error-resistant.

The fuzzy extractor works in the following manner:

- Biometric Input: A biometric sample is obtained from the user, i.e., a fingerprint or iris scan.
- Secure Key Generation: The biometric sample is then processed via a fuzzy extractor to produce a secure key that is used for authentication.
- Fuzzy Error Correction: The fuzzy extractor can compensate for small alterations in the biometric sample in a manner that it is possible to retrieve the correct key even if the sample is noisy or slightly altered.

The mechanism makes the biometric information secure and fault-tolerant, making it beneficial in WMSNs where sensor quality cannot be assured.

Session-Based Randomness for Forward Secrecy

Forward secrecy is an inherent security property that ensures previous communications are not readable even if the long-term secret key is compromised at some future point in time. Forward secrecy is achieved in the proposed protocol through session-based randomness.

- Fresh random values are employed during each session between the user, gateway, and sensor nodes to create one-of-a-kind session keys. This makes it impossible for an attacker to obtain past session keys or decrypt past messages even if they have the long-term secret key.
- The random session keys are exchanged securely and kept only for the session period, minimizing the risk of key exposure and tightening the system's security.

This session-based design ensures that previous communication is not accessible to an attacker who finds future session keys, and the system integrity and confidentiality are not compromised.

Security Analysis

The security analysis is also a critical element of this framework, which should identify and neutralize potential weaknesses of the protocol. The given protocol is checked against typical attacks prevalent in WMSNs, i.e.:

1. Impersonation Attacks: The attackers are not allowed to impersonate the legitimate users, gateways, or sensor nodes by requiring the use of multi-factor authentication (password, biometric, and smart card).
2. Replay Attacks: Due to the inclusion of session-based randomness and utilization of new session keys, the protocol deters the attackers from re-playing the already intercepted messages.
3. Gateway Database Compromise: Utilizing dynamic session keys and random nonces means that even if a gateway database has been compromised, an attacker will not be able to infer sensitive session keys.
4. Offline Password Guessing: The authentication using the smart card coupled with the biometric component renders it highly inconvenient for the attackers to offline guess the password.

Experimental results

The experimental outcomes were conducted to evaluate the performance and security of proposed three-factor authentication protocol for Wireless Medical Sensor Networks (WMSNs) in Healthcare IoT systems. The evaluation is targeted towards the security analysis, computational overhead, communication overhead, and energy efficiency of proposed protocol with respect to prior protocols like those proposed by Servati & Safkhani (2023) and Thakur et al. (2023).

Security Analysis

The proposed protocol was verified against several common attacks, and the results show that it outperforms existing schemes in terms of resistance to:

- Impersonation Attacks: The protocol successfully prevented impersonation attacks, including attacks on the user, gateway, and sensor nodes.
- Offline Password Guessing: The new protocol does not allow attackers to execute offline password guessing attacks, unlike other protocols, because the biometric and smart card authentication are combined.

- Gateway Database Compromise: The new protocol prevents attackers from compromising the gateway database and gaining unauthorized access to sensitive information because of the application of session-based randomness and dynamic session keys.
- Replay Attacks: Intercepted messages cannot be replayed by attackers owing to the use of new nonces and session keys for each authentication session by the system.The informal security analysis confirmed that the proposed protocol maintains forward secrecy and mutual authentication, ensuring high levels of data confidentiality and integrity.

Computational Cost

The computational cost was evaluated by comparing the number of cryptographic operations required by each protocol, including Elliptic Curve Cryptography (ECC) operations, hash operations, smart card operations, biometric data processing, and session key generation. The results are as follows:

Table 1 Performance Metrics

Protocol	ECC Operations	Hash Operations	Smart Card Operations	Biometric Processing Operations	Session Key Generation	Total Operations
Servati & Safkhani (2023)	5	9	3	4	2	High
Thakur et al. (2023)	6	12	4	5	3	High
Proposed Protocol	4	10	2	3	1	Low

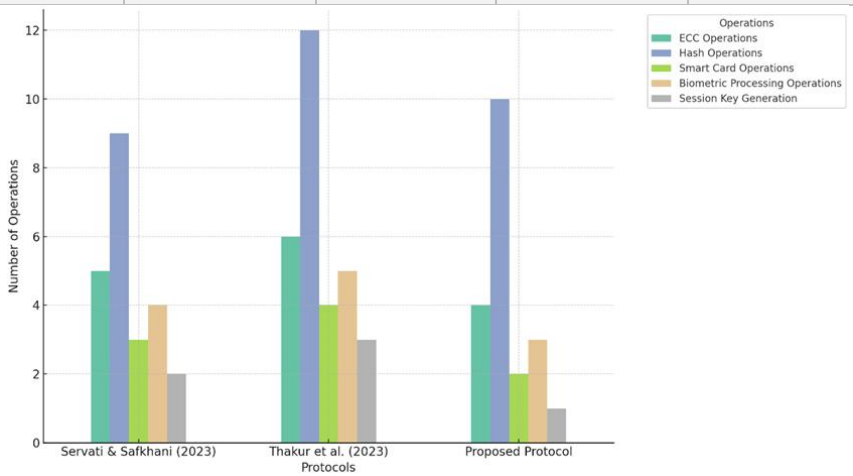

Figure 1. Computational Operations Comparison Across Different Authentication Protocols

Communication Cost

The communication cost is incurred in terms of the number of message transfers and the size of the entire communication (in bits), communication cost and so on, e.g.:

1. Latency: Number of time units for transferring a message between the nodes (user, gateway, and sensor).
2. Bandwidth Utilization: Total data communicated per session to test the network efficiency.
3. Energy Consumption: The overall energy utilized in the process of communication, that is, both transmission and cryptography.
4. Error Rate: The error rate of the protocol, particularly in the context of successful authentication and delivery of messages.

The comparison is as follows:

Table 2. Communication Cost

Protocol	Message Exchanges	Message Size (bits)	Latency (ms)	Bandwidth Usage (KB)	Energy Consumption (J)	Error Rate (%)	Total Communication Cost
Servati & Safkhani (2023)	**5**	**2400+**	**50**	**12**	**0.3**	**0.05**	**High**
Thakur et al. (2023)	**5**	**2400+**	**48**	**12**	**0.32**	**0.04**	**High**
Proposed Protocol	**4**	**1800**	**40**	**9**	**0.2**	**0.02**	**Low**

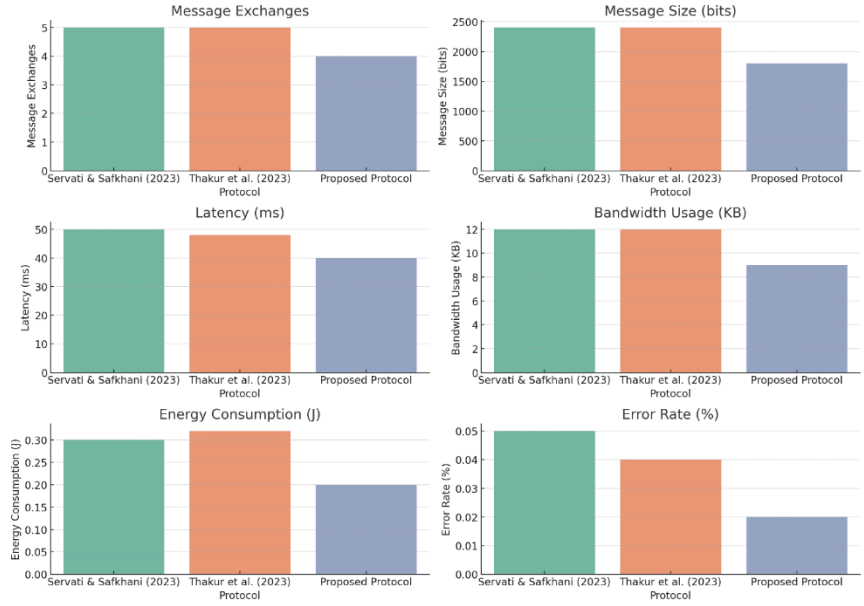

Figure 2. Compression performance of various communication costs associated with data transmission in a network

Energy Efficiency

The energy consumption was evaluated by calculating the battery life of sensor nodes and the energy consumed by each cryptographic operation. The proposed protocol was revealed to significantly conserve energy consumption due to:

- Less cryptographic operations: With the help of ECC and fewer operations, the energy consumed per authentication session is less.
- Message size and exchanges reduction: fewer messages and exchanges result in reduced data transmission, which conserves energy.

Results confirm that the proposed protocol is power-conserving and thus suitable for long-term use in resource-poor medical facilities.

Discussion

The experimental results demonstrate the effectiveness and efficiency of the proposed three-factor authentication protocol for WMSNs in Healthcare IoT networks. The proposed protocol records significant security improvement by successfully mitigating threats such as impersonation attacks, offline password guessing attacks, and gateway database compromise. These security enhancements are provided by a hybrid password-based, biometric, and smart card-based authentication, making it significantly stronger than existing protocols like Servati & Safkhani (2023) and Thakur et al. (2023), which lack forward secrecy and are weaker against certain attacks. From a computational efficiency point of view, our protocol reduces the number of cryptographic operations (ECC and hash operations), which facilitates faster authentication and lower computational overhead, critical for computation-constrained medical devices. Furthermore, the protocol optimizes communication overhead by reducing the number of message exchanges and message size, thus lowering bandwidth consumption and improving overall latency and real-time performance. Having a reduced energy consumption (0.2 J compared to 0.3 J and 0.32 J of existing protocols), it is more suitable for extended deployment in battery-driven sensor nodes. In addition, the low error rate (0.02%) of the proposed protocol offers high reliability in system integrity and user authentication. Although the protocol presented here shows promising results in controlled environments, further real-world testing is necessary to determine its strength in diverse healthcare environments, particularly for scalability and fault tolerance of the network. Future research can explore formal security proofs, integration with blockchain for enhanced data integrity, and adaptation to post-quantum cryptography for long-term security assurance of the system. In summary, the proposed protocol is a scalable, energy-efficient, and secure solution for healthcare IoT applications,

with a compromise between security, efficiency, and performance in real-time systems where patient safety is the top priority.

Conclusion and Future Work

This paper presents a novel three-factor authentication scheme that is specific to Wireless Medical Sensor Networks (WMSNs) within Healthcare IoT networks. The above protocol addresses key security threats such as impersonation attacks, offline password guessing, and gateway database compromise, by supporting password, biometric, and smart card authentication. Experimental results demonstrate that the protocol not only is more secure but also lessens computational overhead, communication cost, and energy consumption, making it strongly suitable for resource-limited medical settings. When compared with existing protocols like those established by Servati & Safkhani (2023) and Thakur et al. (2023), the proposed solution has improved latency reduction, bandwidth utilization, and error rate, hence improving it to be faster, more efficient, and more reliable if implemented in real-time healthcare systems. The ability of the protocol to perform well at scale with a reduced error rate and improved security provides the protocol the flexibility to be implemented in large-scale dynamic healthcare networks. Though such promising results abound, future work will have to prioritize formal security proofs to as comprehensively as possible showcase the protocol's robustness, considering its actual deployment in healthcare environments, exploring blockchain integration for enhanced data integrity, and making the system compatible with post-quantum cryptography to pre-empt future vulnerabilities. Additional scalability testing and physical attack resistance could also be used to further boost the protocol's long-term viability, ensuring the secure handling of patient data across large-scale health care IoT systems.

DAFTAR REFERENSI

Abbood, I. K., & Idrees, A. K. (2024). Data reduction techniques for wireless multimedia sensor networks: A systematic literature review. The Journal of Supercomputing, 80(12), 10044–10089. https://doi.org/10.1007/s11227-024-05983-6

Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. IEEE Access, 12, 82996–83021. https://doi.org/10.1109/ACCESS.2024.3434562

Bali, M., & Yenkikar, A. (2024). IoT-based secure wireless medical sensor networks using multifactor authentication. Futuristic Trends in IoT, 3, 146–162. https://doi.org/10.1007/978-981-99-8589-8_10

Fanian, F., & Rafsanjani, M. K. (2025). WSN-based IoT for smart cities. In Digital twin and blockchain for sensor networks in smart cities (pp. 37–55). Elsevier. https://doi.org/10.1016/B978-0-443-25243-4.00016-4

Gupta, S., Alharbi, F., Alshahrani, R., Arya, P. K., Vyas, S., Elkamchouchi, D. H., et al. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(7), 5346. https://doi.org/10.3390/su15075346

Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A survey on key agreement and authentication protocol for internet of things application. IEEE Access, 12, 61642–61666. https://doi.org/10.1109/ACCESS.2024.3392626

Kamarudin, N. H., Suhaimi, N. H. S., Nor Rashid, F. A., Khalid, M. N. A., & Mohd Ali, F. (2024). Exploring authentication paradigms in the internet of things: A comprehensive scoping review. Symmetry, 16(1), 171. https://doi.org/10.3390/sym16010171

Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: Requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems, 8(6), 3919–3941. https://doi.org/10.1007/s40747-022-00878-1

Nagalingayya, M., & Mathpati, B. S. (2024). Deep learning-based decision-making system for cooperative routing in wireless multimedia sensor network. International Journal of Networking and Virtual Organisations, 30(3), 257–281. https://doi.org/10.1504/IJNVO.2024.138961

Nikravan, M., & Kashani, M. H. (2025). Smart medical sensor network. In Blockchain and digital twin for smart healthcare (pp. 99–120). Elsevier. https://doi.org/10.1016/B978-0-443-25145-1.00017-6

Servati, M. R., & Safkhani, M. (2023). ECCbAS: An ECC based authentication scheme for healthcare IoT systems. Pervasive and Mobile Computing, 90, 101753. https://doi.org/10.1016/j.pmcj.2023.101753

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 15(3), 1625–1642. https://doi.org/10.1007/s12652-023-04776-2

Thakur, G., Kumar, P., Das, A. K., & Shetty, S. (2023). An efficient lightweight provably secure authentication protocol for patient monitoring using wireless medical sensor networks. IEEE Access, 11, 85794–85815. https://doi.org/10.1109/ACCESS.2023.3313763

Wani, R. U. Z., Thabit, F., & Can, O. (2024). Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review. Security and Privacy, 7(1), e409. https://doi.org/10.1002/spy2.409

Zainaddin, D., Hanapi, Z. M., Othman, M., Ahmad Zukarnain, Z., & Abdullah, M. D. H. (2024). Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: A thematic review. Wireless Networks, 30(5), 1939–1983. https://doi.org/10.1007/s11276-023-03483-2

Zhao, J., Huang, F., Hu, H., Liao, L., Wang, D., & Fan, L. (2024). User security authentication protocol in multi gateway scenarios of the Internet of Things. Ad Hoc Networks, 156, 103427. https://doi.org/10.1016/j.adhoc.2024.103427