

Secure and Lightweight Authentication Protocol for WBANs with ECC Modification

Pali Kumari ¹, Anand Sharma ²

^{1,2} Department of CSE, SET, Mody University of Science and Technology, Lakshmangarh

¹ pritypriya303@gmail.com, ² anand_glee@yahoo.co.in

HOW TO CITE:

Pali Kumari, Anand Sharma
(2026). Secure and Lightweight
Authentication Protocol for
WBANs with ECC Modification.
International Journal of Special
Education, 41(10s), 1274-1286

ABSTRACT:

The Wireless Body Area Networks (WBANs) technique has become an important technology in the context of intelligent healthcare systems, owing its capabilities to the real-time collection and transmission of patients' physiological data with the help of wearable and implantable sensor devices. WBANs will facilitate continuous health monitoring by wearable and implanted sensors. WBANs are vulnerable to a range of security attacks such as impersonation attacks, replay attacks, man-in-the-middle attacks and unauthorized access. For WBANs, authentication protocols are used for protecting access to real-time data from sensor nodes. But, they are limited in scope and susceptible to different security attacks.

To solve these problems, this paper proposes an authentication protocol for WBANs that is secure and light, and has been improved by adding Elliptic Curve Cryptography (ECC) modification. To meet security requirements, the proposed protocol is a combination of anonymous authentication method and ECC key exchange method.

The protocol provides mutual authentication, confidentiality, integrity, anonymity, forward security and efficient computation by optimized ECC operations with lightweight hashing. The proposed ECC modified scheme is mathematically modeled, formally analyzed from security perspective, and evaluated using simulation techniques and results, which show good security performance with reasonable efficiency for the resource-constrained WBAN devices. Optimized ECC operations and lightweight hash functions are used during the authentication process to establish an efficient key generation and secure communication for resource-limited WBAN devices.

A mathematical model and formal security analysis prove that the proposed scheme is flexible to the main security attacks. In addition, performance evaluation results show that the proposed Modified ECC protocol has computational complexity and communication overhead is reduced, and it has high security. The results validate the proposed scheme, which has been proven to be secure and efficient enough for next generation applications of WBAN with a healthcare focus.

Keywords: Authentication, Elliptic Curve Cryptography (ECC), Wireless Body Area Networks (WBANs), Health Monitoring.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the
terms and conditions
of the Creative Commons Attribution
(CC BY)
license (<http://creativecommons.org/licenses/by/4.0/>).

1. INTRODUCTION

In medical network, WBANs have provided enhanced potential to healthcare network with the benefits of sensing and disseminating information and emerged as a leading paradigm for research. Modern technologies, like wireless communication, low-power integrated circuits and sensors, are pushing the medical system to become more intelligent and capable of real-time response with WBANs. Medical workers in WBAN-based healthcare system could carry out regular health monitoring if patient's health is monitored regularly by the WBANs. These healthcare systems gather patient's physiological data such as temperature, blood pressure, serum cholesterol, heart rate, glucose level etc. via the wearable sensors [1]. The number of smart devices used in WBANs for the efficient and accurate diagnosis and treatment response, vital sign monitoring and health management is growing [2].

In addition to the security issues, there are numerous practical issues that need to be considered in realizing reliable operation of WBANs. These encompass signal interference, inadequate supply of electricity, restricted bandwidth, storage and computational power limitations, data redundancy and negative environmental effects that can impact signal sensing precision and communication quality. These problems have been extensively studied in the context of wireless and medical sensor networks [3]. Thus, any practical WBANs protocols should not only ensure robust security capabilities, but also take these physical and environmental constraints into account to ensure reliability and scalability in real deployment [4]. Also, since WBAN communicates via open wireless channels which can be attacked, a patient's medical information could be obtained by an attacker who eavesdrops on the information exchange or provide medical information to the user that is not accurate [5].

Given this, a communications failure in a system and the alteration of medical data by an attacker could make it impossible to determine the status

of a patient. As it impacts directly on the patient's lives, secure information exchange requires light user, gateway and sensor node authentication using a session key that are predetermined. As a result, not only does data encryption need to be ensured, but protocols must also be put in place to confirm who is communicating with whom and to ensure data integrity. The use of authentication protocols helps to secure the data transmission process and prevents unauthorized access or modifications, which is crucial for ensuring the security of both parties involved in the communication and the confidentiality of the sensitive medical data being transmitted [6]. A number of authentication schemes have been suggested to secure WMSNs. Many security vulnerabilities and design issues have been uncovered. The server is an important role in WBANs. It not only verifies identities but also, it protects the security of contents of communication. But in real world conditions, the server may not be a fully trusted node, which is not typically the case for existing protocols. For a long time, some protocols [7,8] have added biometric data, random numbers and user passwords to the password to further improve password protection, but they all still generate the long term private key of the terminal device on the server side, overlooking the security problems caused by the semi-trusted server.

Some other schemes [9,10] generate long-term keys independently at the user and device sides, in order to improve the key privacy, but there is still the critical information stored at the server side in the registering phase.

This means that internal staff of the server can access this information along with the information they already have on the public channel to conduct impersonation attacks. These studies are complementary for the proposed ECC-based authentication protocol for the confidentiality, imperceptibility of medical data transmission. Security of the proposed protocol is formally proved and correctness of the proposed protocol is also validated. The results demonstrate that the

proposed protocol is efficient in communication and computation and is able to withstand the common known attacks.

1.1 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a more recent public-key cryptography technique that uses an algebraic structure called an elliptic curve over a finite field. It offers the same amount of cryptographic security as traditional systems such as RSA, but uses much smaller key sizes to achieve this. The equation of an Elliptic Curve is as follows.

$$y^2 = x^3 + ax + b$$

ECC provides smaller key sizes, lower energy consumption compared to RSA and strong security per bit.

1.2 Motivation

- Rapid growth of IoT-based healthcare
- Increasing need for secure remote monitoring
- Limitations of purely hash-based protocols in advanced threat scenarios
- Need for lightweight ECC integration for stronger cryptographic guarantees

1.3 Contributions

- Hybrid ECC + lightweight hash-based authentication protocol
- Reduced ECC computation using optimized scalar multiplication
- Formal security verification including forward secrecy
- Simulation-based performance evaluation

The structure of the paper is as follows: Section 2 provides an overview of related work as literature survey. Section 3 presents an enhanced adversary model and evaluation criteria. Section 4 provides a security analysis of the proposed protocol. Section 5 presents a Computational Analysis.

Section 6 shows the graphs of results and compares the proposed protocol with other

related protocols. The Section 7 shows the limitations and future work to be carried out, at the end conclusion is there as section 8.

2. LITERATURE SURVEY

In 2014, Girl et al. [11] suggested an RSA-based user authentication system to enhance Khan and Kumari's method. Girl et al. asserted through informal study that their scheme is safe from insider, replay, and offline password guessing attacks, among other security threats. Amin and Biswas [12] found in 2015 that Girl et al.'s approach is susceptible to privileged insider attacks and offline password guessing. They then proposed an enhanced RSA-based authentication method. To confirm its security, they also do the AVISPA.

To encourage the growth of WBANs, Jiang et al. [13] presented a three-factor authentication mechanism in 2016. Additionally, a strong ECC-based provable safe authentication system with privacy preservation for the industrial Internet of Things was proposed by Li, X. et al. [14] in 2017. Wang et al. [15] presented a strict attacker model in 2018, yet the study concluded that servers should not be trusted since unwanted port listening events and data breaches have been more frequent in recent years.

Ayub et al. [16] noted that despite the protocol's purported robustness, it was unable to ensure clock synchronization and withstand attacks such as user impersonation and smart card loss. The system [16] was later shown to be vulnerable to replay and man-in-the-middle attacks by Peralta-Ochoa et al. [17].

An attacker can easily determine the session key once the ephemeral secret is obtained because in schemes [18], the generation of the session key primarily depends on temporary random numbers and public parameters (such as elliptic curve points G or P , as well as intermediate variables transmitted through the public channel). In conclusion, two significant challenges that have not received enough attention in previous research are insider assaults and ESL attacks.

While several studies from 2020 [19] concentrate on the protocol's resistance to recognized security concerns (such synchronization attacks, replay attacks, and offline dictionary guessing attacks), they are unable to stop server insiders from utilizing registration information to determine the session key.

Using IoT-enabled devices, Sahoo et al. [20] created a mutual authentication framework for TMIS in 2021. Their technique uses Elliptic Curve Cryptography (ECC), symmetric cryptography, and biometric information to safeguard sensitive patient data. They asserted that their protocol is resistant to replay attacks, offline password guessing, and smartcard theft, among other security threats.

In 2022, Masud et al. [21] developed a lightweight, privacy-protected authentication method for IoT-based healthcare that makes use

of the sensors on a patient's IoT device. A three-factor authentication protocol for healthcare IoT systems was presented by Servati and Safkhani [22] in 2023. They claimed that most cryptographic attacks, including impersonation, ephemeral secret leakage, offline password guessing, and privileged insider assaults, could be prevented by their technique.

3. PROPOSED WORK

Instead of relying only on hash operations, the proposed protocol integrates lightweight ECC-based key exchange to enhance security while keeping computation minimal even at the authentication phase. The different phases of the proposed algorithm are shown in figure 1.

- Registration Phase
- Authentication Phase
- Session Key Establishment

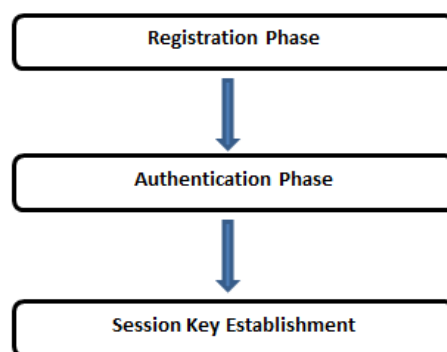


Figure 1. Phases of Propose work

3.1 Registration Phase

SN selects private key:

$$d_{SN} \in Z_q$$

Public key:

$$Q_{SN} = d_{SN} \cdot P$$

MS stores: $\{ID_{SN}, Q_{SN}\}$

Send: $\{ID_{SN}, R_1, A_1\}$

Step 2: Gateway $\rightarrow$ Server

GN generates N_2 and forwards: $\{ID_{SN}, R_1, N_1, N_2, A_1\}$

Step 3: Server Verification

MS computes shared secret:

$$S = d_{MS} \cdot R_1$$

Verifies hash and generates response:

$$A_2 = H(S || N_2)$$

Step 4: Mutual Authentication

SN verifies:

$$S = r_1 \cdot Q_{MS}$$

If valid $\rightarrow$ authentication successful

3.2 Authentication Phase

Step 1: Sensor Node $\rightarrow$ Gateway

SN generates nonce N_1 and ephemeral key:

$$R_1 = r_1 \cdot P$$

Compute:

$$A_1 = H(ID_{SN} || N_1 || R_1)$$

3.3 Session Key Establishment

$$K_s = H(S || N_1 || N_2)$$

4. SECURITY ANALYSIS

4.1 Mutual Authentication

Achieved via shared ECC secret and hash verification.

Explanation:

Before transferring sensitive health information, communication entities, such as a sensor node and the medical server/gateway, must confirm each other's validity. This is why mutual authentication is a basic security need in WBANs. ECC is used in the proposed Modified ECC-based authentication technique to generate a shared secret for mutual authentication. Both organizations use their private keys and the shared public keys to independently calculate the same session key throughout the authentication procedure.

Authentication tokens are then produced by combining the generated shared secret with cryptographic hash functions. Each party confirms the identity of the communicating entity by checking the hash values after obtaining these tokens. An adversary cannot produce valid authentication hashes since only authorized parties have the necessary ECC private keys. As a result, the suggested method offers robust mutual authentication with minimal computational overhead, making it appropriate for WBN devices with limited resources.

4.2 Forward Secrecy

Ephemeral ECC keys ensure past sessions remain secure.

Explanation:

An essential security feature is forward secrecy, which safeguards previously created session keys even in the event that long-term private keys are later compromised. The Modified ECC technique uses ephemeral ECC key pairs for every communication session in order to achieve forward secrecy. To create a unique session key,

new temporary private and public keys are created for each new session.

These temporary keys are thrown away after the session ends. Because the temporary session-specific keys are no longer accessible, an attacker cannot recreate the session keys used in earlier interactions, even if they manage to steal the long-term private key of a sensor node or gateway later on. In healthcare applications, where patient data security must be maintained for long periods of time, this functionality is very crucial. As a result, the suggested ECC-based system guarantees the long-term defense of private medical data against potential key compromise attempts.

4.3 MITM Resistance

ECC key exchange prevents attacker from deriving shared secret.

Explanation:

A Man-in-the-Middle (MITM) assault happens when an adversary poses as each of the two lawful parties in order to intercept and maybe alter messages transmitted between them. Through safe ECC-based key exchange and authentication procedures, the Modified ECC algorithm successfully reduces MITM attacks. Both communication entities exchange ECC public keys and use their individual private keys to create a shared secret during the key establishment phase.

Even if the public keys are intercepted, an attacker cannot produce the right session key since the computation of the shared secret requires knowledge of the private key. Furthermore, the exchanged communications are linked to the identities of authorized participants through the use of cryptographic hash verification and authentication tokens. When an attacker modifies transmitted data, hash discrepancies cause authentication to fail. As a result, the suggested method guarantees secure end-to-end communication within the WBAN environment and stops adversaries from successfully entering the communication channel.

4.4 Replay Attack Resistance

Nonces ensure freshness.

Explanation:

In order to obtain unauthorized access or interfere with network operations, replay attacks entail an adversary intercepting legitimate authentication messages and retransmitting them later. The Modified ECC-based authentication technique uses session-specific parameters and randomly generated nonces to thwart replay attacks. Both communicating entities create new nonces during each authentication session, which are subsequently included in the session key generation process and authentication messages.

These nonces guarantee that each authentication exchange is distinct and cannot be used again in later sessions. Before authenticating a communication, the recipient confirms that the nonce is current. The message is instantly rejected if a duplicate or previously used nonce is found. Therefore, replaying legitimate communication packets will not result in a successful authentication even if an attacker manages to capture them. By guaranteeing message freshness and prohibiting unwanted session reuse, this method greatly improves the security and dependability of the WBAN.

5. COMPUTATIONAL ANALYSIS

In terms of cryptographic operations carried out during registration, authentication, and session key establishment, computational analysis

assesses the effectiveness of the suggested Modified ECC-based authentication protocol. Reducing cryptographic overhead is crucial since WBAN devices have limited processing power, memory, and battery capacity.

Assumptions

Let:

- T_{EM} = Time required for one ECC scalar multiplication operation
- T_H = Time required for one hash operation
- T_N = Time required for nonce generation (negligible)
- T_A = Time required for simple arithmetic/concatenation operations (negligible)

Since ECC scalar multiplication is the most computationally expensive operation, the overall complexity mainly depends on the number of ECC multiplications.

5.1 Registration Phase

At Sensor Node (SN) –

The Operations performed in the registration phase at sensor node is described in table 1.

Private key generation:

$$d_{SN} \in \mathbb{Z}_q$$

Public key generation:

$$Q_{SN} = d_{SN} \cdot P$$

Table 1. Operations performed

Entity	ECC Multiplication	Hash	Total Cost
Sensor Node	1	0	T_{EM}
Medical Server	0	0	Negligible

Therefore,

$$C_{Reg} = T_{EM}$$

The registration phase is executed only once and thus contributes minimally to overall system overhead.

5.2 Authentication Phase

Step 1: Sensor Node

Generation of ephemeral public key:

$$R_1 = r_1 \cdot P$$

Authentication token:

$$A_1 = H(ID_{SN} || N_1 || R_1)$$

Cost at SN

- 1 ECC scalar multiplication
- 1 Hash operation

$$CAuth_{SN} = T_{EM} + T_H$$

Step 2: Gateway Node

Gateway simply forwards the authentication request and generates nonce N_2

Cost at GN

- Nonce generation only

$$CAuth_{GN} \approx 0$$

Step 3: Medical Server

Shared secret computation:

$$S = d_{MS} \cdot R_1$$

Authentication response:

$$A_2 = H(S || N_2)$$

Cost at MS

- 1 ECC scalar multiplication
- 1 Hash operation

$$CAuth_{MS} = T_{EM} + T_H$$

Step 4: Sensor Verification

Sensor computes:

$$S = r_1 \cdot Q_{MS}$$

and verifies received authentication value.

Cost at SN

- 1 ECC scalar multiplication
- 1 Hash operation

$$CVerify_{SN} = T_{EM} + T_H$$

Total Authentication Cost

Combining all operations:

Sensor Node

$$2T_{EM} + 2T_H$$

Gateway Node

$$0$$

Medical Server

$$T_{EM} + T_H$$

Hence,

$$CAuth = 3T_{EM} + 3T_H$$

5.3 Session Key Establishment Cost

Session key generation:

$$K_s = H(S || N_1 || N_2)$$

Operations

- One hash computation

$$C_{SK} = T_H$$

5.4 Overall Computational Cost

The total computational cost of the proposed Modified ECC scheme is:

$$C_{Total} = 3T_{EM} + 4T_H$$

where:

- $3T_{EM}$ corresponds to ECC scalar multiplications
- $4T_H$ corresponds to hash computations

6. RESULT AND DISCUSSION

This section shows the final result and comparison with other algorithms.

6.1 Computational Cost Comparison (Cryptographic Operations)

Figure 2 displays the computational cost comparison with respect to the cryptographic operations carried out during the authentication procedure. With fewer cryptographic operations overall, the suggested Modified ECC method lessens the processing load on resource-constrained WBAN sensor nodes by requiring moderate hash operations.

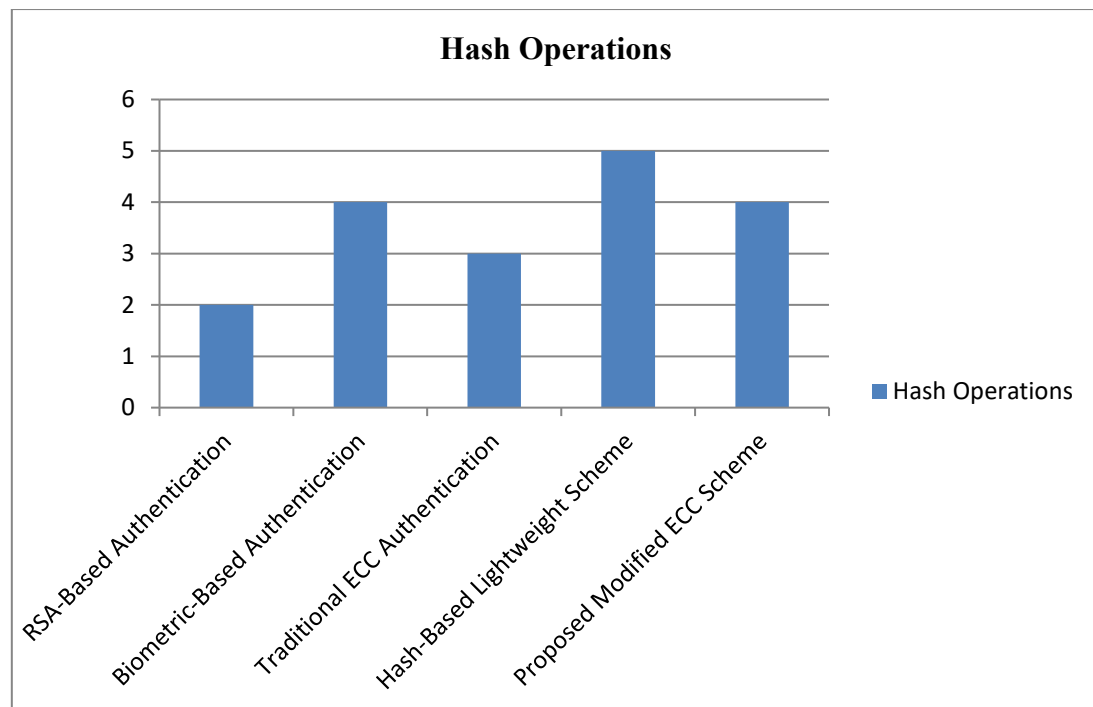


Figure 2. Number of cryptographic operations required during authentication.

6.2 Communication Cost Comparison (Bytes Exchanged)

In WBAN contexts, smaller message sizes result in lower energy and bandwidth consumption.

Figure 3 displays a comparison of communication overhead with respect to bytes exchanged.

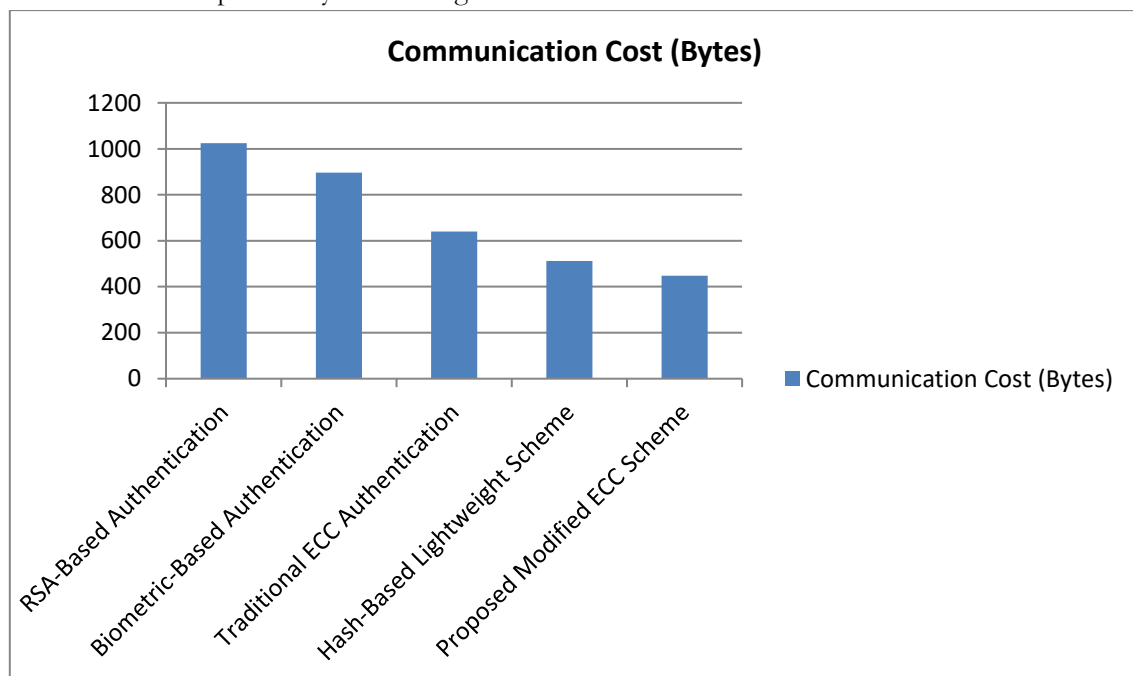


Figure 3. Total communication cost during authentication session.

6.3 Security Features Comparison

Security Strength Comparison is shown in figure 4. Following Security Features are considered while comparing:

- Mutual Authentication
- Session Key Agreement
- Forward Secrecy

- Replay Attack Resistance
- MITM Resistance
- Impersonation Attack Resistance

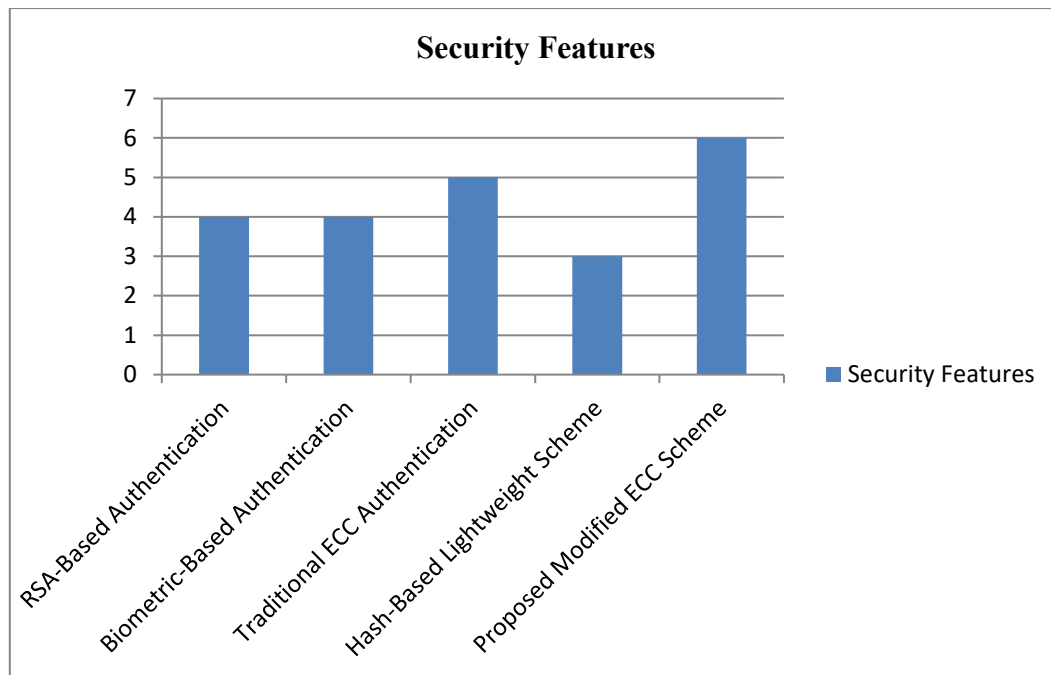


Figure 4. Number of security features supported by each authentication scheme.

6.4 Security Feature Summary

The Security Feature performed by each algorithm is shown in table 2.

Table 2. Security Feature Summary

Security Feature	RSA-Based	Biometric-Based	Traditional ECC	Hash-Based	Proposed Modified ECC
Mutual Authentication	✓	✓	✓	●	✓
Session Key Agreement	✓	✓	✓	✗	✓
Forward Secrecy	✗	✗	✓	✗	✓
Replay Attack Resistance	✓	✓	✓	✓	✓
MITM Resistance	●	●	✓	✗	✓
Impersonation Attack Resistance	●	✓	✓	●	✓

✓ = Fully Supported , ● = Partially Supported , ✗ = Not Supported

6.5 Overall Comparison

The overall comparison is shown in table 3.

Table 3. Overall comparison

Features	RSA-Based Authentication	Biometric-Based Authentication	Traditional ECC Authentication	Hash-Based Lightweight Scheme	Proposed Modified ECC Scheme
ECC Multiplications	4	3	4	0	3
Hash Operations	2	4	3	5	4
Communication Cost (Bytes)	1024	896	640	512	448
Mutual Authentication	Yes	Yes	Yes	Partial	Yes
Session Key Agreement	Yes	Yes	Yes	No	Yes
Forward Secrecy	No	No	Yes	No	Yes
Replay Attack Resistance	Yes	Yes	Yes	Yes	Yes
MITM Resistance	Partial	Partial	Yes	No	Yes
Impersonation Attack Resistance	Partial	Yes	Yes	Partial	Yes

6.6 Discussion

The proposed Modified ECC authentication scheme needs only three scalar multiplication operations of the ECC and four hash operations to achieve complete authentication and session key establishment between the two parties. ECC can provide the same level of security with much smaller keys and lower computation compared to the traditional public-key authentication schemes based on RSA. The proposed cryptographic scheme is very appropriate for WBAN environment, which has strict energy and resource constraints for sensor nodes. Moreover, the gateway does not carry out costly cryptographic calculations, which also minimises the delay for communication and enhances network efficiency. Hence, the Modified ECC algorithm is an optimum algorithm for secure transfer of healthcare data in WBANs with a balance between security and computational complexity.

7. LIMITATIONS AND FUTURE WORK

7.1 Limitations

Although the proposed authentication protocol based on Modified ECC is very efficient and secure, there are some restrictions in this protocol. First, the protocol is based on a secure underlying Elliptic Curve Cryptography framework, which is still an additional computational load over purely lightweight symmetric-key approaches. Optimized ECC operations will require less processing time, but if the sensor nodes are resource constrained, they may consume more energy during a frequent authentication session. Secondly, the existing protocol relies on the trust of a medical server and a gateway node in registration and authentication. The security of the network could be compromised if these things are compromised. Furthermore, the scheme proposed in this paper has been analyzed by

using a mathematical model and a security analysis, and the mobility of nodes, the interference caused by the wireless channel, the packet loss, and scalability in a large-scale healthcare setting have not been fully studied. Additionally, the protocol offers protection against various types of attacks, including replay attack, man-in-the-middle attack, and denial-of-service (DoS) attacks, but does not explicitly mention new threats such as cryptanalysis and advanced DoS attacks by insiders and advanced quantum attacks. All these need further research for security in a changing healthcare ecosystem in the long run.

7.2 Future Work

Future research efforts may be directed towards improving the proposed authentication scheme by extending it to solve the pointed out issues and making it more applicable for use in the next generation healthcare systems. The future path lies in leveraging blockchain for decentralized trust management, secure audit trails, and enhanced data integrity in healthcare networks that are distributed. The other interesting direction is the use of AI and machine learning algorithms for live anomaly detection and intrusion prevention in WBAN. These can help the network's capacity for detecting malicious activity and reacting proactively to security events. Future research could also explore the deployment of post-quantum cryptographic schemes together with ECC-based schemes to ensure security of communications in WBANs against future quantum computing attacks. To test the energy usage, latency, scalability, and reliability for realistic healthcare scenarios, WBAN practical deployment and experimental testing can also be performed using real hardware platforms. In conclusion, the proposed protocol can be further expanded to enable secure, scalable and privacy-preserving communication of medical data in future intelligent healthcare applications, such as an Internet of Medical Things (IoMT) architecture, a cloud-based healthcare system and 6G-enabled smart healthcare network.

8. CONCLUSION

Wireless Body Area Networks (WBANs) are crucial in healthcare for enabling real-time, continuous monitoring and transmission of patients' physiological data. But the open wireless medium and the resource-constrained nature of WBAN devices make them vulnerable to a number of security and privacy risks. Hence, designing an authentication mechanism that will have low computation and communication overhead while having strong security guarantees is a great challenge. In this paper, a secure and lightweight authentication protocol using Modified Elliptic Curve Cryptography (ECC) algorithm was proposed in WBANs. The proposed scheme includes anonymous authentication, ECC-based key exchange and lightweight hash operations which provide secure communication between the sensor nodes, gateways and medical servers. The protocol fulfills the security requirements such as mutual authentication, confidentiality, integrity, anonymity, key agreement (on a session basis), forward secrecy, replay attack resistance, impersonation attack resistance, and man-in-the-middle attack resistance. The Computational analysis showed that the proposed protocol is based on limited number of ECC scalar multiplication and hash operation, which is suitable for the resource constrained WBAN devices. In addition, it was found that the proposed Modified ECC approach has improved security characteristics and reduced computation and communication complexity compared to current authentication methods. The formal security analysis validated the protocol's ability to withstand critical attacks typical in healthcare monitoring systems. In conclusion, the proposed Modified ECC authentication scheme achieves a good trade-off between security, privacy, and efficiency, making it a potential solution for secure applications based on WBAN in healthcare. In the future, blockchain-based trust management, artificial intelligence-based intrusion detection mechanisms, and post-quantum cryptographic techniques can be incorporated to further

improve security and scalability of the next-generation WBANs.

REFERENCES

- Kumari, Pali, and Anand Sharma. "Advancements and Challenges in Wireless Body Area Networks (WBANs): A Comprehensive Review with Emphasis on Security." In *International Conference on Smart Cyber Physical Systems*, pp. 657-670. Singapore: Springer Nature Singapore, 2024.
- Thakur, G.; Prajapat, S.; Kumar, P.; Das, A.K.; Shetty, S. An efficient lightweight provably secure authentication protocol for patient monitoring using wireless medical sensor networks. *IEEE Access* 2023, 11, 114662–114679.
- Kenyeres, M.; Kenyeres, J.; HassankhaniDolatabadi, S. Distributed consensus gossip-based data fusion for suppressing incorrect sensor readings in wireless sensor networks. *J. Low Power Electron. Appl.* 2025, 15, 6.
- Ahmad, R.; Wazirali, R.; Abu-Ain, T. Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors* 2022, 22, 4730.
- L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for Ehealth systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.
- Kumari, Pali, and Anand Sharma. "Effective Authentication Methods for Wireless Body Area Networks." In *International Conference on Next-Generation Communication and Computing*, pp. 25-37. Singapore: Springer Nature Singapore, 2024.
- Kim, K.; Ryu, J.; Lee, Y.; Won, D. An improved lightweight user authentication scheme for the internet of medical things. *Sensors* 2023, 23, 1122.
- Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *J. Ambient. Intell. Humaniz. Comput.* 2024, 15, 1165–1186.
- Chen, C.; Guo, H.; Wu, Y.; Gao, Y.; Liu, J. A novel two-factor multi-gateway authentication protocol for WSNs. *Ad Hoc Netw.* 2023, 141, 103089.
- Kumar, C.M.; Dwivedi, S.K.; Brindha, M.; Al-Shehari, T.; Alfakih, T.; Alsalman, H.; Amin, R. REPACA: Robust ECC based privacy-controlled mutual authentication and session key sharing protocol in coalmines application with provable security. *Peer-to-Peer Netw. Appl.* 2024, 17, 4264–4285.
- D. Giri, T. Maitra, R. Amin, and P. D. Srivastava, "An efficient and robust RSA-based remote user authentication for telecare medical information systems," *J. Med. Syst.*, vol. 39, no. 1, pp. 1–9, Jan. 2015.
- R. Amin and G. P. Biswas, "An improved RSA based user authentication and session key agreement protocol usable in TMIS," *J. Med. Syst.*, vol. 39, no. 8, pp. 1–14, Aug. 2015.
- Jiang, Q.; Khan, M.K.; Lu, X.; Ma, J.; He, D. A privacy preserving three-factor authentication protocol for e-health clouds. *J. Supercomput.* 2016, 72, 3826–3849.
- Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiyah, M.; Kumari, S. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. *IEEE Trans. Ind. Inform.* 2017, 14, 3599–3609.
- Wang, D.; Wang, P. Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound. *IEEE Trans. Dependable Secur.Comput.* 2018, 15, 708–722.
- Minahil; Ayub, M.F.; Mahmood, K.; Kumari, S.; Sangaiah, A.K. Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. *Digit.Communi.Netw.* 2021, 7, 235–244.
- Peralta-Ochoa, A.M.; Chaca-Asmal, P.A.; Guerrero-Vásquez, L.F.; Ordoñez-Ordoñez, J.O.; Coronel-González, E.J. Smart healthcare applications over 5G networks: A systematic review. *Appl. Sci.* 2023, 13, 1469.
- Sureshkumar, V.; Amin, R.; Vijaykumar, V.; Sekar, S.R. Robust secure communication protocol for smart healthcare system with FPGA implementation. *Future Gener.Comput. Syst.* 2019, 100, 938–951.
- Wazid, M.; Das, A.K.; Kumar, N.; Alazab, M. Designing authenticated key management scheme in 6G-enabled network in a box deployed for industrial applications. *IEEE Trans. Ind. Inform.* 2020, 17, 7174–7184.

-
- S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021.
- M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 2022.
- M. R. Servati and M. Safkhani, "ECCbAS: An ECC based authentication scheme for healthcare IoT systems," *Pervas. Mobile Comput.*, vol. 90, Mar. 2023, Art. no. 101753.