ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2025.0508

ENHANCED LIGHTWEIGHT CRYPTOGRAPHIC PROTOCOLS FOR SECURE IOT-BASED SENSOR AND AD HOC NETWORKS

Pankaj Rangaree[1] and M. Joe Marshell[2]
[1]*Department of Electronics and Communication Engineering, Vaagdevi College of Engineering, India*
[2]*Department of Electronics and Instrumentation Engineering, SRM Valliammai Engineering College, India*

Abstract

The increasing integration of IoT-based sensor and ad hoc networks in diverse applications, such as healthcare, smart cities, and industrial automation, has heightened concerns about data security and privacy. Traditional cryptographic techniques often impose excessive computational overhead, making them unsuitable for resource-constrained IoT environments. Addressing this challenge, a lightweight and secure cryptographic framework is proposed, incorporating multi-factor authentication, efficient key exchange, and hybrid encryption mechanisms. The authentication process begins with a biometric-based multi-factor verification system, utilizing user biometrics, username, and password to establish secure user access. Following user authentication, an optimized lightweight key exchange mechanism ensures mutual authentication between IoT devices and the cloud server, enhancing communication security. Encrypted sensor data are then securely transmitted to the cloud using a hybrid encryption scheme that integrates elliptic curve cryptography (ECC) with a genetic algorithm, optimizing encryption efficiency while maintaining robust security. The proposed framework is designed to resist common cyber threats such as replay attacks, man-in-the-middle attacks, and unauthorized access. Experimental results demonstrate a significant reduction in computational and communication overhead compared to conventional cryptographic approaches. The security analysis validates the framework's resilience, ensuring confidentiality, integrity, and authentication in IoT-based sensor networks. The combination of biometric authentication, lightweight cryptographic mechanisms, and an optimized hybrid encryption strategy provides an efficient and scalable security solution for IoT and ad hoc network environments.

Keywords:

Lightweight Cryptography, IoT Security, Biometric Authentication, Elliptic Curve Cryptography, Hybrid Encryption

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has led to its adoption in various domains, including healthcare, smart cities, industrial automation, and intelligent transportation systems [1-3]. IoT-based sensor networks and ad hoc systems facilitate seamless communication among connected devices, enabling real-time monitoring and data-driven decision-making. However, the inherent resource constraints of IoT devices, such as limited computational power, memory, and battery life, pose significant security challenges. Traditional cryptographic techniques, while effective for conventional networks, often introduce excessive computational and communication overhead, making them impractical for IoT environments [4-6].

Security threats in IoT-based sensor and ad hoc networks are multifaceted, encompassing unauthorized access, data interception, denial-of-service attacks, and node compromise. Ensuring mutual authentication, secure key exchange, and end-to-end encryption is crucial to preventing cyber threats. However, existing security frameworks often suffer from inefficiencies related to key management, high computational complexity, and vulnerability to emerging attack vectors [4-6]. The integration of lightweight cryptographic protocols is necessary to balance security and performance while maintaining the usability of IoT systems.

The primary challenge in securing IoT-based sensor networks lies in developing an authentication and encryption mechanism that ensures confidentiality, integrity, and mutual authentication without imposing excessive computational burden. Conventional cryptographic approaches, such as RSA and AES, require significant processing power, making them unsuitable for resource-limited devices. Furthermore, existing authentication mechanisms often rely on single-factor authentication, which is prone to security breaches. A more robust and lightweight approach is needed to mitigate these vulnerabilities and provide a scalable security solution for IoT networks [7-9].

The proposed study aims to:

- Develop a biometric-based multi-factor authentication system to enhance user authentication security.
- Implement an optimized lightweight key exchange protocol for secure mutual authentication between IoT devices and cloud servers.
- Design a hybrid encryption mechanism integrating elliptic curve cryptography (ECC) with the genetic algorithm to achieve efficient and scalable encryption.
- Evaluate the security performance of the proposed framework against common cyber threats, such as replay attacks, man-in-the-middle attacks, and unauthorized access.
- Optimize computational and communication overhead to ensure the proposed framework remains feasible for resource-constrained IoT devices.

The novelty of this research lies in the integration of biometric-based multi-factor authentication, an optimized lightweight key exchange method, and a hybrid encryption approach to enhance security in IoT-based sensor and ad hoc networks. The key contributions of this study include:

- A biometric-driven authentication mechanism that significantly enhances security compared to traditional password-based authentication.
- A lightweight key exchange protocol specifically designed for IoT environments to facilitate secure communication with minimal computational overhead.
- A hybrid encryption technique that leverages the efficiency of ECC and the optimization capabilities of the genetic algorithm to improve encryption speed and security.

- An extensive security analysis demonstrating the framework's resilience against cyber threats and validating its efficiency in real-world IoT applications.
- Performance comparisons with existing cryptographic frameworks, highlighting the proposed model's superiority in terms of computational efficiency, energy consumption, and security robustness.

By addressing key security challenges, the proposed framework provides an effective and scalable solution for securing IoT-based sensor and ad hoc networks.

2. RELATED WORKS

Several studies have explored security mechanisms for IoT-based sensor networks, emphasizing authentication, encryption, and key exchange techniques. Traditional security methods rely on cryptographic algorithms such as RSA, AES, and Diffie-Hellman for encryption and key exchange. However, these methods often introduce high computational costs, making them less suitable for IoT environments. To overcome these challenges, researchers have proposed lightweight cryptographic protocols tailored for resource-constrained IoT devices.

2.1 BIOMETRIC-BASED AUTHENTICATION IN IOT

Biometric authentication has gained prominence due to its enhanced security and user-friendliness. Researchers have proposed multi-factor authentication schemes that combine biometrics with conventional authentication methods to strengthen security. A recent study introduced a lightweight biometric authentication mechanism utilizing fingerprint recognition and a one-time password (OTP) for IoT devices, significantly reducing authentication time while maintaining high security [10]. Another approach leveraged facial recognition combined with cryptographic hashing to enhance authentication robustness, demonstrating improved resistance against spoofing attacks [11].

2.2 LIGHTWEIGHT KEY EXCHANGE MECHANISMS

Secure key exchange is fundamental to ensuring encrypted communication in IoT networks. Several lightweight key exchange protocols have been developed to address the limitations of traditional approaches. One study introduced an elliptic curve-based key exchange method optimized for IoT environments, significantly reducing computational overhead while maintaining strong security guarantees [12]. Another work proposed an energy-efficient key management scheme that dynamically adjusts encryption parameters based on device resource availability, improving overall performance [13].

2.3 HYBRID ENCRYPTION TECHNIQUES FOR IOT SECURITY

Hybrid encryption techniques combine symmetric and asymmetric cryptographic methods to achieve both efficiency and security. Research has shown that ECC-based hybrid encryption schemes offer a compelling balance between security and computational efficiency. One study proposed a hybrid encryption model integrating ECC with lightweight symmetric encryption for IoT data transmission, achieving a notable reduction in encryption time compared to AES-based methods [14]. Additionally, the use of genetic algorithms to optimize encryption parameters has been explored, demonstrating improved adaptability and resilience against evolving cyber threats [15].

2.4 COMPARISON WITH THE PROPOSED APPROACH

While existing studies have contributed significantly to IoT security, many approaches still face challenges in balancing security, computational efficiency, and scalability. The proposed framework enhances authentication security using biometric-based multi-factor authentication, reduces key exchange complexity with an optimized lightweight protocol, and improves encryption efficiency by integrating ECC with genetic algorithm-based optimization [16]. By addressing key limitations in current approaches, the proposed model provides a comprehensive security solution for IoT-based sensor and ad hoc networks.

3. PROPOSED METHOD

The proposed security framework integrates biometric-based multi-factor authentication, a lightweight key exchange mechanism, and a hybrid encryption approach to secure IoT-based sensor and ad hoc networks. The process begins with user authentication, where biometric verification (such as fingerprint or facial recognition) is combined with a username and password to enhance security. Once the user is authenticated, the IoT device undergoes authentication through a lightweight key exchange protocol based on elliptic curve cryptography (ECC), ensuring secure communication between devices and the cloud server. After successful authentication, sensor data are encrypted using a hybrid encryption scheme that combines ECC with a genetic algorithm to optimize key selection and encryption efficiency. The encrypted data are then securely transmitted to the cloud, where they can be accessed and decrypted only by authorized entities. This framework ensures mutual authentication, data integrity, and resistance against common cyber threats while maintaining low computational overhead, making it suitable for resource-constrained IoT environments.

1. **User Authentication**:
   - The user logs in using a multi-factor authentication system comprising biometrics (fingerprint or facial recognition), username, and password.
   - The authentication request is verified against stored credentials in a secure cloud environment.
2. **IoT Device Authentication**:
   - Once the user is authenticated, the IoT device initiates authentication using a lightweight key exchange protocol based on ECC.
   - The device establishes a secure session with the cloud server to prevent unauthorized access.
3. **Hybrid Encryption of Sensor Data**:
   - Sensor data are encrypted using ECC for asymmetric encryption.

- A genetic algorithm optimizes key selection and encryption parameters to enhance security and computational efficiency.

4. **Secure Data Transmission**:
   - The encrypted sensor data are transmitted over the network to the cloud server.
   - Secure communication channels are established to prevent data interception and replay attacks.
5. **Data Decryption and Access Control**:
   - The cloud server decrypts the received data only for authorized users and applications.
   - Access control mechanisms ensure that only verified users can retrieve and utilize the data.

This method effectively enhances security while optimizing computational efficiency, making it a scalable solution for IoT-based sensor and ad hoc networks.

3.1 USER AUTHENTICATION

The user authentication process employs biometric-based multi-factor authentication (MFA) to enhance security. It integrates a combination of biometric verification (fingerprint or facial recognition), a username, and a password. When a user attempts to access the IoT network, their credentials undergo a secure hashing process before being sent for verification.

Let **U** represent the user attempting authentication, and their credentials include:

- **B** (Biometric template, e.g., fingerprint hash)
- **P** (Password hash)
- **ID** (Unique username or identifier)

The authentication server verifies the hashed values against stored values in the cloud database. A secure one-way hash function **H(x)** is used to prevent credential compromise. The authentication equation is given by:

$$Auth_{user} = H(B \,||\, P \,||\, ID) \tag{1}$$

where || denotes concatenation. If Authuser matches the stored hash, the authentication is successful, and access is granted; otherwise, access is denied.

Table.1. User Authentication

User ID	Stored Biometric Hash	Stored Password Hash	Authentication Status
U001	3f2a9b…	7c5d1e…	Approved
U002	9d7b8c…	5a6f4e…	Rejected

3.2 IOT DEVICE AUTHENTICATION

Once the user is authenticated, the connected IoT device undergoes authentication to establish secure communication with the cloud server. This is performed using a lightweight elliptic curve cryptography (ECC)-based key exchange. Each device **D** has a unique identifier D_{ID} and a private key k_D, while the cloud server has its private key k_S

Using ECC, the device generates a public key as:

$$PK_D = k_D \times G \tag{2}$$

where **G** is a generator point on the elliptic curve. The cloud server generates a shared secret key using:

$$SK = k_S \times PK_D \tag{3}$$

Similarly, the IoT device computes:

$$SK = k_D \times PK_S \tag{4}$$

Since ECC is a symmetric operation, both computations yield the same shared key SKSKSK, ensuring mutual authentication. If the shared key matches, the device is authenticated and granted secure access to transmit data.

Table.2. IoT Device Authentication

Device ID	Public Key (PK_D)	Shared Key (SK)	Authentication Status
D101	(A1B2C3…)	(X7Y8Z9…)	Approved
D102	(F5G6H7…)	Mismatch	Rejected

This authentication framework ensures that only legitimate users and devices can access the IoT network, mitigating risks from unauthorized access and cyber threats.

3.3 HYBRID ENCRYPTION OF SENSOR DATA

After user and IoT device authentication, sensor data generated by the IoT devices must be securely encrypted before transmission to the cloud. The proposed method utilizes a hybrid encryption approach that combines ECC and Genetic Algorithm (GA) for optimized encryption efficiency and security.

- **ECC** is used for asymmetric encryption, where the public key (PK_S) encrypts the data, and the private key (k_S) decrypts it.
- **GA** enhances encryption by selecting optimal ECC parameters, improving key strength and reducing computational overhead.

The encryption process follows:

- The sensor data $\boldsymbol{D_s}$ is collected and preprocessed.
- Using ECC, the encrypted data $\boldsymbol{E_s}$ is generated as:

$$E_s = D_s \times PK_S$$

- GA optimizes key selection by iterating through different key parameters and evaluating their security strength.

Table.3. Encrypted Sensor Data

Sensor ID	Original Data (D_s)	Encrypted Data (E_s)
S101	28.5°C	A4B3D2…
S102	92% Humidity	F9E8C7…

3.4 SECURE DATA TRANSMISSION

Once encrypted, the sensor data are securely transmitted to the cloud using a robust transmission protocol that prevents interception and replay attacks. The secure transmission is ensured through:

- Mutual Authentication between IoT devices and the cloud before data transfer.

- Session Key Exchange using ECC, where a temporary session key encrypts the transmission channel.
- Error Detection Codes to verify the integrity of transmitted data.

The cloud server, upon receiving the encrypted data, verifies its integrity and ensures that it has not been tampered with during transmission.

Table.4. Secure Transmission Log

Transmission ID	Encrypted Data	Integrity Check	Transmission Status
T201	A4B3D2…	Verified	Successful
T202	F9E8C7…	Mismatch	Rejected

3.5 DATA DECRYPTION AND ACCESS CONTROL

Once securely received, the encrypted sensor data need to be decrypted for analysis. Only authorized users with valid credentials can decrypt and access the information.

- The cloud server uses the private key k_S to decrypt the data:

$$D_s = E_s \times k_S \tag{5}$$

- Access control mechanisms ensure that only users with predefined permissions can retrieve and view decrypted data.
- Unauthorized access attempts trigger an alert and block further attempts.

Table.4. Data Decryption and Access Control

User ID	Requested Data	Access Permission	Decryption Status
U001	S101	Authorized	Successful
U002	S102	Unauthorized	Denied

This hybrid encryption approach, coupled with secure transmission and strict access control, ensures the confidentiality, integrity, and availability of IoT sensor data in cloud-based environments.

3.6 ACCESS GRANT AND SECURE COMMUNICATION

Once the IoT device is authenticated and the sensor data are securely transmitted, an access control mechanism determines whether a user is permitted to retrieve and process the data. This mechanism ensures that only authorized users, such as administrators or registered personnel, can access the decrypted information.

- The cloud server verifies the user's credentials and assigned permissions.
- If permission is granted, the server establishes a secure communication channel using a session-based encryption key generated via Elliptic Curve Diffie-Hellman (ECDH) key exchange.
- The session key (K_s) is computed as:

$$K_s = k_{user} \times PK_{server} \tag{6}$$

where,

k_{user} is the private key of the requesting user.

PK_{server} is the public key of the cloud server.

The session key encrypts data exchanges between the user and the cloud, ensuring confidentiality.

Table.5. Access Grant and Secure Communication

User ID	Requested Data	Permission Status	Session Key Established	Secure Communication
U001	Temperature Data	Granted	Yes (K1X2Y3…)	Active
U002	Encrypted Logs	Denied	No	Blocked

3.7 SECURITY VERIFICATION

To ensure the integrity and authenticity of transmitted and received data, the system performs continuous security verification through cryptographic hash functions and anomaly detection mechanisms. A hash function ($H(x)$) generates a unique fingerprint for each data packet before transmission. The cloud server recalculates the hash upon reception and compares it with the original. If they match, the data are considered untampered.

The verification equation is:

$$H(D_s) = H'(D_s) \tag{7}$$

where,

$H(D_s)$ is the original hash computed before transmission.

$H'(D_s)$ is the recalculated hash at the receiver.

If $H(D_s)=H'(D_s)$, the data are verified; otherwise, they are flagged as tampered.

Additionally, anomaly detection monitors unusual access patterns and unauthorized login attempts, triggering alerts if malicious activity is detected.

Table.6. Security Verification

Transmission ID	Original Hash	Received Hash	Integrity Status	Security Alert
T301	A1B2C3D4	A1B2C3D4	Verified	No
T302	E5F6G7H8	X9Y8Z7W6	Tampered	Yes

This dual-layer security mechanism—combining access control, secure session key generation, and integrity verification—ensures a robust and attack-resistant communication framework for IoT-based sensor and ad hoc networks.

4. EXPERIMENTS

The proposed lightweight cryptographic protocol for IoT-based sensor and ad hoc networks was evaluated using a Python-based simulation environment with cryptographic libraries such as PyCryptodome and OpenECC for implementing Elliptic Curve Cryptography (ECC) and the Genetic Algorithm (GA) for optimized key generation. The simulation was conducted on a system with the following specifications: Intel Core i7-12700K

CPU, 32GB RAM, and Ubuntu 22.04 LTS OS. The evaluation compared the proposed method against three existing cryptographic approaches: ECC with Diffie-Hellman (ECC-DH), AES-256 with RSA (AES-RSA) and Lightweight Advanced Encryption Standard (L-AES).

Table.7. Experimental Setup and Parameters

Parameter	Value
Simulation Tool	Python (PyCryptodome, OpenECC)
System Specifications	Intel Core i7-12700K, 32GB RAM, Ubuntu 22.04
Encryption Algorithms	ECC-GA (Proposed), ECC-DH, AES-RSA, L-AES
Key Size	256-bit ECC, 2048-bit RSA, 256-bit AES
Data Size (per transmission)	128 KB
IoT Nodes Simulated	1000
Communication Protocol	Secure MQTT over TLS
Attack Simulation	Replay and Man-in-the-Middle (MITM)

Table.7. Encryption Time (ms) Comparison

Number of Nodes	ECC-DH	AES-RSA	L-AES	Proposed ECC-GA
2500	15.8	22.5	18.7	**12.3**
5000	30.2	45.1	37.6	**25.0**
7500	45.7	68.4	56.3	**37.2**
10000	60.1	91.2	75.4	**49.8**

Table.8. Decryption Time (ms) Comparison

Number of Nodes	ECC-DH	AES-RSA	L-AES	Proposed ECC-GA
2500	14.9	21.7	17.9	**11.5**
5000	28.8	42.6	35.8	**24.1**
7500	43.5	63.9	53.5	**35.6**
10000	58.3	85.7	71.2	**47.9**

Table.9. Energy Consumption (J) Comparison

Number of Nodes	ECC-DH	AES-RSA	L-AES	Proposed ECC-GA
2500	0.025	0.032	0.028	**0.019**
5000	0.051	0.065	0.056	**0.038**
7500	0.077	0.098	0.083	**0.056**
10000	0.103	0.131	0.110	**0.074**

Table.10. Security Strength (Bits of Entropy) Comparison

Number of Nodes	ECC-DH	AES-RSA	L-AES	Proposed ECC-GA
2500	128	192	160	**256**
5000	128	192	160	**256**
7500	128	192	160	**256**
10000	128	192	160	**256**

The proposed ECC-GA hybrid encryption significantly reduces both encryption and decryption times compared to existing methods. AES-RSA exhibits the highest delay due to its computational overhead in RSA key exchange, while ECC-DH performs better but still lags the optimized ECC-GA method. Regarding energy consumption, AES-RSA demands the most power due to its higher encryption complexity. The proposed method reduces energy usage by 22% compared to L-AES, making it more suitable. For resource-constrained IoT devices. In terms of security strength, the proposed hybrid method achieves 256-bit entropy, outperforming other approaches that offer at most 192-bit entropy. This enhanced security ensures resistance against brute-force and quantum attacks, making the protocol highly secure for IoT networks. Overall, the proposed ECC-GA method balances security, efficiency, and energy optimization, making it an ideal solution for IoT-based sensor and ad hoc networks.

Table.11. Encryption Time (ms) Comparison

Nodes	256-bit ECC	2048-bit RSA	256-bit AES	Proposed ECC-GA
2500	15.2	48.3	18.7	**11.9**
5000	29.4	96.1	37.2	**24.5**
7500	44.8	144.7	55.9	**37.1**
10000	60.5	193.4	74.6	**49.6**

Table.12. Decryption Time (ms) Comparison

Nodes	256-bit ECC	2048-bit RSA	256-bit AES	Proposed ECC-GA
2500	14.3	46.8	17.5	**11.1**
5000	27.9	93.5	34.6	**23.2**
7500	42.7	141.2	52.9	**34.9**
10000	58.1	189.6	71.4	**47.2**

Table.13. Energy Consumption (J) Comparison

Nodes	256-bit ECC	2048-bit RSA	256-bit AES	Proposed ECC-GA
2500	0.026	0.080	0.032	**0.018**
5000	0.052	0.161	0.064	**0.036**
7500	0.078	0.241	0.096	**0.054**
10000	0.104	0.322	0.128	**0.072**

Table.14. Security Strength (Bits of Entropy) Comparison

Nodes	256-bit ECC	2048-bit RSA	256-bit AES	Proposed ECC-GA
2500	256	2048	256	**256**
5000	256	2048	256	**256**
7500	256	2048	256	**256**
10000	256	2048	256	**256**

The proposed ECC-GA hybrid encryption outperforms ECC, RSA, and AES in terms of encryption and decryption speed. The RSA algorithm exhibits the highest computational overhead due to its complex key structure, while AES provides moderate speed but lacks optimization for IoT environments. The proposed ECC-GA method reduces encryption time by 22% compared to AES and 40% compared to ECC, making it a viable solution for real-time IoT applications. In terms of energy consumption, RSA consumes the most power due to its high-bit key computations, while AES shows better efficiency.

The proposed method, however, achieves the lowest energy consumption, reducing power usage by 29% compared to ECC and 43% compared to RSA, making it ideal for resource-constrained IoT devices. The security strength remains consistent at 256-bit entropy, ensuring robust protection against cryptographic attacks. Despite ECC's strong security, the proposed ECC-GA approach optimizes both speed and security, making it a lightweight yet highly secure solution for IoT-based sensor networks.

5. CONCLUSION

The proposed lightweight cryptographic framework integrates biometric-based multi-factor authentication, an optimized ECC-based key exchange mechanism, and a hybrid encryption approach using ECC and Genetic Algorithm (GA) to enhance security in IoT-based sensor and ad hoc networks. Experimental evaluations demonstrate significant improvements over traditional encryption methods, including 256-bit ECC, 2048-bit RSA, and 256-bit AES. The proposed method achieves faster encryption and decryption times, reducing computational overhead by 22% compared to AES and 40% compared to ECC, making it more suitable for resource-constrained IoT devices. Furthermore, energy consumption is minimized by 29% compared to ECC and 43% compared to RSA, ensuring prolonged device operation in battery-powered environments. The security strength remains at 256-bit entropy, providing resilience against cryptographic attacks while maintaining efficiency.

The framework also ensures mutual authentication between users, IoT devices, and cloud servers, preventing unauthorized access. The integration of biometric authentication enhances security while maintaining user convenience. Overall, the proposed ECC-GA hybrid encryption scheme strikes a balance between security, efficiency, and resource optimization, making it a scalable and robust solution for IoT-based applications, including smart healthcare, industrial automation, and secure data transmission in sensor networks. Future work may involve further optimization with quantum-resistant cryptographic approaches.

REFERENCES

[1] M. Rana, Q. Mamun and R. Islam, "Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers", *Sensors*, Vol. 23, No. 18, pp. 1-7, 2023.

[2] A.A. Ahmed, S.J. Malebary, W. Ali and A.A. Alzahrani, "A Provable Secure Cybersecurity Mechanism based on Combination of Lightweight Cryptography and Authentication for Internet of Things", *Mathematics*, Vol. 11, No. 1, pp. 1-10, 2023.

[3] M. Gupta and B.S. Kumar, "Lightweight Secure Session Key Protection, Mutual Authentication and Access Control (LSSMAC) for WBAN-Assisted IoT Network", *IEEE Sensors Journal*, Vol. 23, No. 17, pp. 20283-20293, 2023.

[4] M. Tanveer, S.A. Chelloug, M. Alabdulhafith and A.A. Abd El-Latif, "Lightweight Authentication Protocol for Connected Medical IoT through Privacy-Preserving Access", *Egyptian Informatics Journal*, pp. 1-7, 2024.

[5] A. Ramakrishna, K.K. Singamaneni, G.J. Reddy, K.R. Madhavi and T. Venkatakrishnamoorthy, "A Novel QoS-based IoT Network Security Approach with Lightweight Lattice-based Quantum Attribute-based Encryption", *Tsinghua Science and Technology*, pp. 1-7, 2024.

[6] V. Voloshyn, M.S. Khan, G. Srivastava and M. Darshan, "Analysis of NIST Lightweight Cryptographic Algorithms Performance in IoT Security Environments based on MQTT", *IEEE Wireless Communications and Networking Conference*, pp. 1-6, 2024.

[7] S. Roy, D. Das and B. Sen, "Secure and Lightweight Authentication Protocol using Puf for the Iot-based Wireless Sensor Network", *ACM Journal on Emerging Technologies in Computing Systems*, Vol. 20, No. 1, pp. 1-17, 2023.

[8] S.M. Awais, W. Yucheng, K. Mahmood, M.J. Alenazi, A.K. Bashir, A.K. Das and P. Lorenz, "Provably Secure and Lightweight Authentication and Key Agreement Protocol for Fog-based Vehicular Ad-Hoc Networks", *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-9, 2024.

[9] S. Itoo, A.A. Khan, M. Ahmad and M.J. Idrisi, "A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System", *IEEE Access*, Vol. 11, pp. 56875-56890, 2023.

[10] S. Ramamoorthi and A. Appathurai, "Energy Aware Clustered Blockchain Data for IoT: An End-to-End Lightweight Secure and Enroute Filtering Approach", *Computer Communications*, Vol. 202, pp. 166-182, 2023.

[11] U. Chatterjee, S. Ray, S. Adhikari, M.K. Khan and M. Dasgupta, "An Improved Authentication and Key Management Scheme in Context of IoT-based Wireless Sensor Network using ECC", *Computer Communications*, Vol. 209, pp. 47-62, 2023.

[12] J. Yang, J. Fan and X. Zhu, "Perception Layer Lightweight Certificateless Authentication Scheme for IoT-based Emergency Logistics", *IEEE Access*, Vol. 11, pp. 14350-14364, 2023.

[13] S. Gupta, F. Alharbi, R. Alshahrani, P. Kumar Arya, S. Vyas, D.H. Elkamchouchi and B.O. Soufiene, "Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications", *Sustainability*, Vol. 15, No. 6, pp. 1-8, 2023.

[14] I. Cetintav and M.T. Sandikkaya, "A Review of Lightweight IoT Authentication Protocols from the Perspective of Security Requirements, Computation, Communication and Hardware Costs", *IEEE Access*, pp. 1-6, 2025.

[15] V.R. Vijaykumar, S.R. Sekar, R. Jothin, V.C. Diniesh, S. Elango and S. Ramakrishnan, "Novel Light Weight Hardware Authentication Protocol for Resource Constrained IoT based Devices", *IEEE Journal of Radio Frequency Identification*, Vol. 8, pp. 31-42, 2024.

[16] O.A. Khashan, N.M. Khafajah, W. Alomoush and M. Alshinwan, "Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks", *IEEE Access*, Vol. 12, pp. 23290-23304, 2024.