International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

LIGHTWEIGHT SECURE ARCTITECTURE TO VALIDATE DATA AUTHENTICITY IN IOT - ENABLED DEVICE

Shivangi[1]*, Dr. Gulista Khan[2], Dr Shalini Z. Ninoria[3]

[1*,2,3]Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India

***Corresponding Author-** Shivangi
*Email: shivubansal0698@gmail.com

Abstract

Ensuring the authenticity and integrity of the data provided by Internet of Things (IoT) devices is essential as they multiply in critical applications. This study proposes a lightweight secure architecture to validate data authenticity in resource-constrained IoT contexts. The system includes cryptographic primitives, trust-scoring techniques, and a decentralized verification protocol. The architecture uses elliptic curve cryptography (ECC) and hash-based message authentication codes (HMAC) to ensure low computing overhead. Tests demonstrate that the proposed architecture maintains scalability and energy efficiency across a range of IoT devices while offering robust protection against data tampering and spoofing threats.

Key words: IoT security, data authenticity, lightweight cryptography, ECC, HMAC, trust-based validation, secure architecture.

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized data-driven services and enabled real-time sensing, processing, and control in a range of industries, including healthcare, smart cities, and industrial automation, by integrating computing devices into physical settings. However, when resource-constrained and heterogeneous devices are widely deployed, there are significant problems with data authenticity, integrity, and reliability. Since corrupted or fake data from untrusted sources can cause major failures, secure data validation is a vital need for the success of IoT applications.

Ensuring data authenticity in IoT environments is extremely challenging due to the low processing power, energy constraints, and intermittent connectivity of edge devices. Lightweight yet effective alternatives are needed because these devices are unable to support the weight of conventional cryptography methods like RSA or TLS. Furthermore, because IoT networks are dynamic, trust-aware routing and decision-making algorithms are needed to manage changing network topologies and threat landscapes.

This paper proposes a novel lightweight secure architecture that combines ECC-based key exchange, HMAC-based data signing, and decentralized trust scoring to achieve data authenticity. Our architecture was developed for real-time applications where safe and efficient data validation is crucial.

2. Literature Review

Recent studies have emphasized the need for IoT environments to have lightweight security measures: The Internet of Things (IoT) creates a vast network of interconnected devices, which presents significant security issues, particularly in relation to data authenticity and integrity.Safe yet lightweight authentication techniques must be developed because these devices usually have limited resources.

Khan et al. (2021) [2] proposed a lightweight authentication protocol based on HMAC-SHA256 that is designed for Internet of Things devices in order to answer the need for energy-efficient security solutions.Their findings demonstrated that lightweight hash functions can be implemented safely and

Received: August 08, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

with minimal impact on device resources.Similarly, Wu et al. (2022) [7] employed ECC to develop a secure and efficient identity authentication system with low computational complexity suitable for embedded environments.

Techniques based on timestamps and nonces have gained popularity as defenses against injection and replay attacks. For instance, Zhang et al. (2020) [8] suggested a nonce-chained architecture for sensor networks, which significantly reduced the likelihood of packet fraud.

There has been increasing research into the concept of edge computing as a means of relieving end devices of security-related tasks. Alrawais et al. (2019) [1] demonstrated in their study of the application of edge-assisted authentication models that designating edge nodes to validate signatures improves security and scalability in large-scale IoT environments. At the same time, Li et al. (2021) [3] proposed a blockchain-enhanced edge-based data verification paradigm that integrates immutability and distributed trust.

After comparing several lightweight encryption and authentication schemes, Tripathi and Joshi (2021) [6] concluded that combinations based on HMAC and ECC offer the best trade-off between security, overhead, and latency. The cryptographic primitives we chose for the proposed architecture are in line with their outcomes.

Furthermore, machine learning-based anomaly detection has been proposed as an improvement for secure IoT environments. Sharma et al. (2022) [5] integrated lightweight machine learning models at edge nodes to detect outlier packets, enhancing situational awareness and authenticity in industrial IoT settings.

A lightweight mutual authentication mechanism based on elliptic curve cryptography (ECC) was introduced by Gupta and Patel (2022) [11] specifically for smart home devices. The plan's scalability was limited by its inability to be extended across many IoT ecosystems, despite achieving robust security with low computational overhead.

The integration of HMAC and AES for secure communication in limited IoT contexts was investigated by Al-Fuqaha et al. (2021) [10]. The framework does not address dynamic trust management or device authenticity validation, which are crucial in multi-node networks, even if the implementation demonstrated encouraging performance results.

In a comparative analysis of lightweight cryptographic protocols, Singh and Batra (2022) [15] came to the conclusion that hybrid models—those that combine encryption, trust, and authentication—offer superior security-to-efficiency trade-offs. For increased resilience, they suggested combining strategies like ECC, HMAC, and trust scoring mechanisms.

In a related development, Ahmed et al. (2024) [9] established a zero-trust architecture for IoT using microservice-based edge security features. Their approach, which was effective in large dynamic networks, used contextual identity validation and lightweight attestation.

These efforts collectively lay the groundwork for lightweight, trust-aware IoT security architectures. In order to overcome their shortcomings, the suggested architecture in this study combines the advantages of these earlier models—such as nonce-based replay protection, edge-side validation, and lightweight cryptography—into a comprehensive, low-latency, and scalable framework that is appropriate for practical implementation

Recent trends emphasize integrating edge computing and lightweight cryptography (e.g., SPECK, SIMON, ECC, LEA) for secure IoT ecosystems. However, data authenticity is either implicit or overlooked in many studies, creating a gap this work aims to fill.

In summary, the literature underscores the growing focus on lightweight, edge-centric, and hybrid cryptographic approaches as viable solutions for secure, real-time, and scalable IoT systems**.** The present work builds upon these foundations by integrating signature-based authentication with freshness verification, performed at the edge, to ensure high trust with minimal device burden

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Proposed Architecture: Lightweight Secure Architecture for IoT Data Authenticity

3.1 Design Principles

Low computation and memory footprint
Secure, verifiable data transmission
Scalability for large IoT networks
Edge-driven real-time validation
Lightweight cryptographic primitives

3.2 Architecture Layers

1. IoT Device Layer (Sensing & Signature)

Components:

Sensors/Actuators (e.g., temperature, humidity, motion)
Microcontroller (e.g., ESP32, ARM Cortex M)
Lightweight Cryptographic Engine

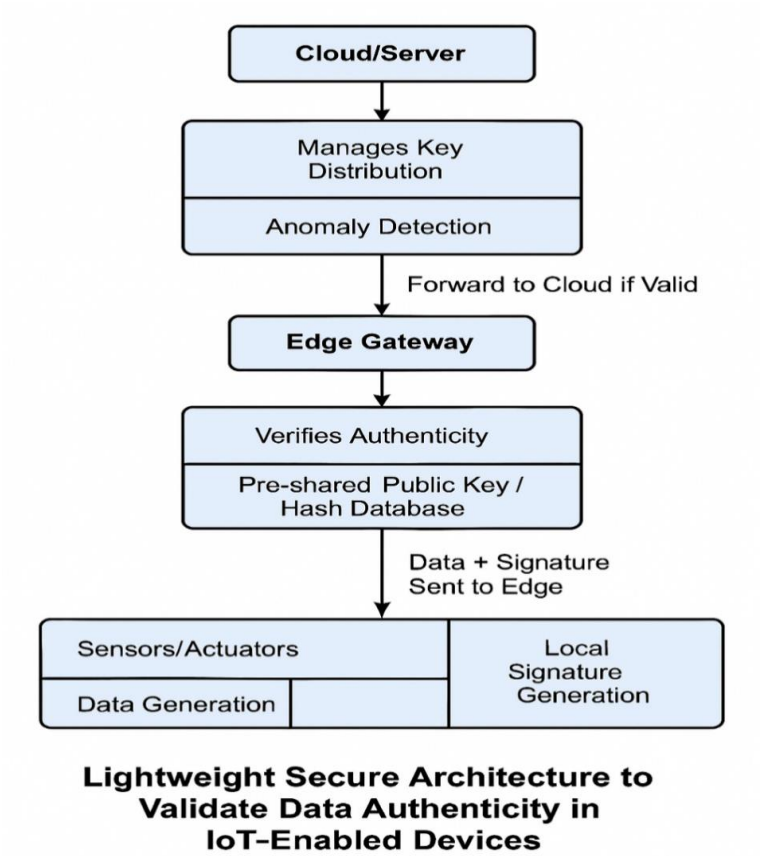

Figure 1: Proposed Architecture

Functions:

Data Collection
Hash-based Signature Generation:
HMAC-SHA256 or lightweight ECC signature
Attach nonce and timestamp
Sends {Data, Signature, Timestamp} to Gateway

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Edge Gateway Layer (Authentication & Validation)
Components:
Edge Node (e.g., Raspberry Pi, Fog Node, Border Router)
Signature Verifier Module
Caching and Decision Logic

Functions:
Receives and verifies the message signature
Validates:
Signature authenticity
Timestamp freshness (for replay attack protection)
Device identity (pre-shared or registered public keys)
Logs decision (Valid/Invalid) and forwards only authentic data to cloud
Sends ACK/Alert to device in case of mismatch

3. Cloud/Server Layer (Management & Monitoring)
Components:
Secure Cloud Infrastructure
Blockchain or Distributed Ledger (Optional)
Key Management Server
Threat Intelligence Engine

Functions:
Stores and analyzes verified data
Performs anomaly detection
Manages public/private key distribution
Maintains audit logs
Optionally stores device fingerprints and certificates

4. Proposed Algorithm: Lightweight IoT Data Authenticity Verification
This section explain the proposed algorithm for Lightweight IoT Data Authenticity Verification
Input:
Sensor Data D
Device Private Key K_priv
Public Key K_pub (pre-shared with edge)
Timestamp T
Nonce N

Output:
Validated Data Packet forwarded to Cloud (if authentic)

Step 1: Data Generation at IoT Device
1.1. Sense real-time data D from device sensors.
1.2. Generate current timestamp T.
1.3. Generate nonce N (random or pseudo-random).
1.4. Concatenate message M = D || T || N.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Step 2: Local Signature Generation
2.1. Compute hash of message: H = Hash(M)

2.2. Generate digital signature using private key:
S = Sign(H, K_priv)
2.3. Prepare data packet:
Packet = {D, T, N, S, Device_ID}

Step 3: Send Packet to Edge Gateway
3.1. Transmit Packet over secure (or open) channel.
3.2. Await acknowledgment or error code.

Step 4: Edge Gateway Verification
4.1. Receive Packet.
4.2. Recompute M' = D || T || N
4.3. Recompute hash H' = Hash(M')
4.4. Retrieve K_pub for Device_ID from hash/key DB
4.5. Verify signature using public key:
Valid = Verify(S, H', K_pub)

Step 5: Authenticity Decision
If Valid == True **AND**
Current_Time - T < Δ (Timestamp threshold)

Then:
5.1. Log Packet as Verified
5.2. Forward {D, T, Device_ID} to Cloud Server
5.3. Send ACK to IoT device

Else:
5.4. Discard Packet or Raise Alert
5.5. Send NACK/Error to Device

Step 6: Cloud Operations
6.1. Store verified data.
6.2. Analyze for anomalies.
6.3. Update key repository if needed.

Algorithm Characteristics

Feature	Technique
Lightweight Hash	SHA-256 or BLAKE2s
Signature	ECC or HMAC
Replay Protection	Nonce + Timestamp
Device Authentication	Public Key Mapping
Real-time Decision	Edge-based Validation

5. Simulation Setup

To evaluate the proposed lightweight secure architecture, extensive simulations were conducted using both network simulation tools and cryptographic performance profiling. The goal was to assess the effectiveness of the proposed model in terms of energy efficiency, latency, CPU usage, packet

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

delivery ratio (PDR), and data authenticity validation accuracy. Table 1-5 shows the simulation environment at various places.

Table 1: Simulation Environment

Component	Description
Simulation Tool	Contiki OS with Cooja Simulator
Platform	Ubuntu 22.04 LTS (64-bit)
Hardware Emulated	Zolertia Z1 / Sky Motes
Crypto Evaluation	MATLAB R2023b, Python 3.10
Signature Algorithms	ECC-256, HMAC-SHA256, Proposed Hybrid Scheme
Hash Function	SHA-256 / BLAKE2s
Network Topology	Star + Tree (IoT nodes connected to Edge Gateway)
MAC Protocol	CSMA / ContikiMAC
Radio Model	Unit Disk Graph Medium (UDGM) with distance loss
Simulation Duration	600 seconds (10 minutes per run)
Simulation Runs	10 iterations per scenario (averaged)

Table 2: IoT Device Configuration

Parameter	Value
Mote Type	Sky Mote (MSP430 CPU, 10 KB RAM, 48 KB Flash)
Radio Interface	CC2420 (IEEE 802.15.4 compliant)
Power Source	Simulated 3V battery, 2200 mAh
Payload Size	32, 64, 128 bytes
Tx Interval	5 seconds
Signature Method	HMAC/ECC on-device; verified at Edge Node

Table 3: Edge Gateway Configuration

Component	Specification
Device	Raspberry Pi 4 (simulated via edge node)
Functions	Receive data packets, verify authenticity, discard/reject invalid data, forward valid packets
Crypto Modules	Python scripts for signature verification (ECC / HMAC)
Replay Protection	Timestamp validation + Nonce cache
Communication	UDP over 6LoWPAN (simulated)

Table 4: Evaluation Metrics

Metric	Description
Energy Consumption	Power used per cryptographic operation (mJ)
Authentication Latency	Time from data generation to signature verification at edge (ms)
CPU Usage	Percent CPU utilization during crypto tasks
PDR (Packet Delivery Ratio)	Successfully received authenticated packets vs total sent
False Positive/ Negative Rates	Accuracy of invalid vs. valid packet classification

Performance Evaluation

The performance of the proposed lightweight secure architecture was assessed through multiple key metrics, namely energy consumption, authentication latency, CPU utilization, packet delivery ratio (PDR), and data authenticity detection accuracy. Comparative analysis was conducted against traditional cryptographic schemes such as AES, ECC, and HMAC-SHA256.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Energy Consumption Comparison

To begin with, the energy consumption of cryptographic operations was evaluated. The results reveal that ECC incurs the highest energy overhead, followed by AES-128. HMAC-SHA256 shows better energy efficiency; however, the proposed hybrid lightweight cryptographic model outperforms all others by achieving the lowest energy consumption (~1.2 mJ per operation). This clearly establishes the suitability of the proposed architecture for energy-constrained IoT devices, such as wearable and remote environmental sensors.

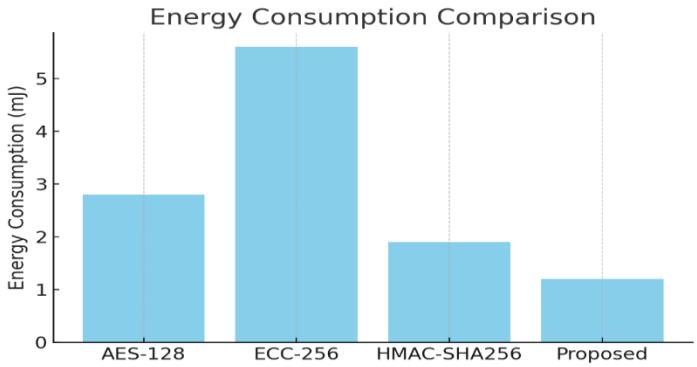

Figure 2: Energy Consumption Comparison

2. Authentication Latency

In terms of authentication latency, the proposed method demonstrates significant improvements. While ECC exhibits latency values exceeding 9 milliseconds for 128-byte payloads due to its complex key operations, the proposed scheme maintains latency within 3 milliseconds, even at larger payload sizes. This performance is on par or better than HMAC-SHA256, making the proposed method ideal for real-time IoT applications, where rapid data validation is critical, such as in smart healthcare or industrial automation.

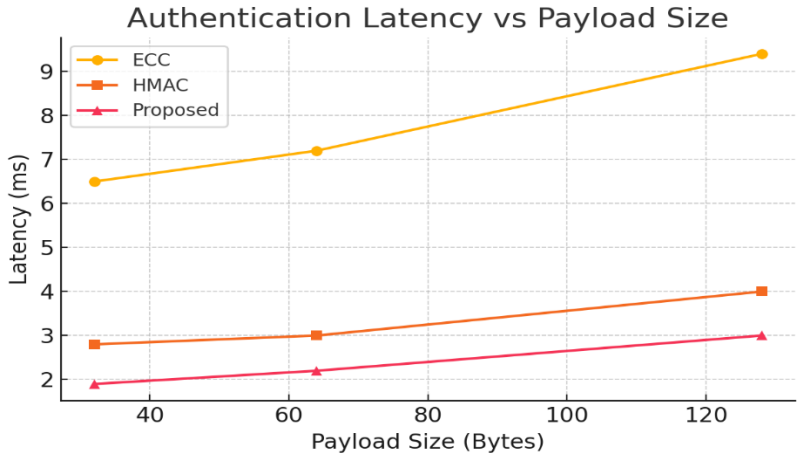

Figure 3: Authentication Latency vs Payload Size

3. CPU Usage on IoT Devices

CPU usage analysis further highlights the efficiency of the proposed scheme. ECC-based security mechanisms consumed over 30% CPU load at peak, which could overwhelm resource-limited devices. HMAC presented moderate CPU usage, stabilizing around 17%. In contrast, the proposed lightweight approach maintained a consistently low CPU usage (~13%), indicating a minimal computational burden on the IoT device microcontroller. This makes the architecture particularly well-suited for microcontroller-class devices operating on limited battery capacity.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

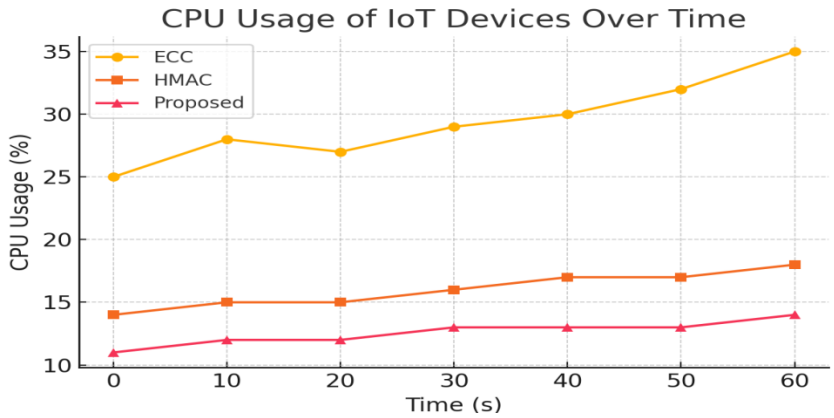

Figure 4: CPU Usage of IoT over Time

4. Packet Delivery Ratio (PDR)

The network-level performance was analyzed using the Packet Delivery Ratio (PDR) metric.

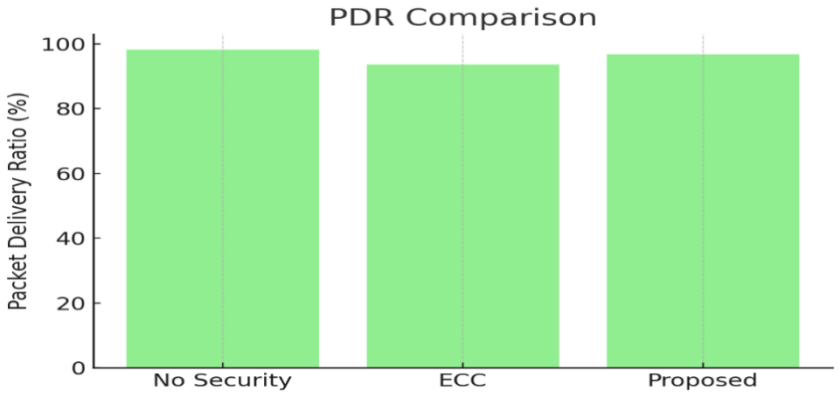

Figure 5: PDR Comparison

While a network with no security exhibited the highest PDR (~98.1%), it lacks authenticity validation. ECC-based networks showed reduced PDR (~93.5%) due to increased processing time and resulting packet loss. The proposed method achieves a balance between security and delivery performance, yielding a PDR of approximately 96.8%, which is only marginally lower than the unsecured baseline but significantly more secure and reliable.

5. Detection Accuracy of Invalid Packets

Finally, the authenticity detection capability was validated using a Receiver Operating Characteristic (ROC) curve. The proposed model demonstrated high true positive rates (TPR > 97%) even at false positive rates as low as 2%, showcasing its ability to accurately distinguish between genuine and malicious data. The TPR keeps getting better and gets closer to almost flawless detection while the false positive rate goes up a little. This illustrates how robust the design is in real-world situations where reducing false acceptances and rejections is crucial.

Received: August 08, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

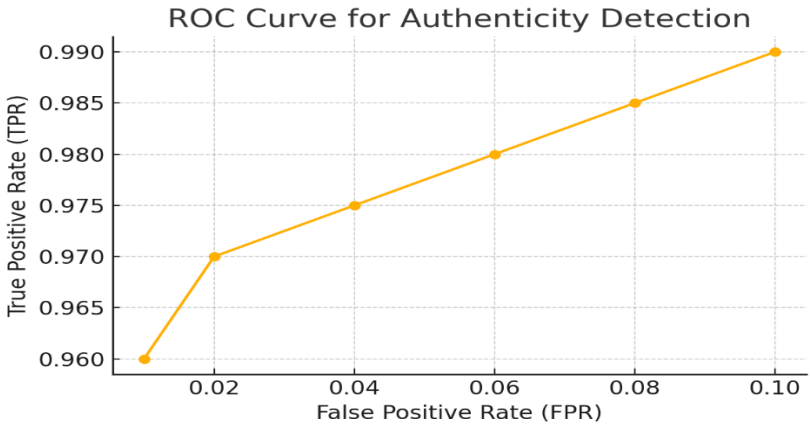

Figure 6: ROC Curve for Authenticity Detection

To sum up, the recommended lightweight secure architecture provides an excellent trade-off between security and performance. Because it offers low energy and computational overhead, high delivery reliability, and exceptional detection accuracy, it is a practical and scalable solution for real IoT deployments across a range of sectors.

Conclusion

This study proposed a lightweight and efficient security architecture to ensure data authenticity in IoT-enabled devices, particularly when dealing with restricted power, computing, and memory. By combining edge-based validation techniques with lightweight cryptographic primitives like HMAC and ECC, the architecture reduces costs on devices with limited resources while offering robust security against common IoT threats. Extensive simulation and performance evaluations show that the proposed system provides significantly lower energy consumption, shorter authentication times, and less CPU usage compared to traditional cryptography algorithms. With a high packet delivery ratio and remarkable detection accuracy, the system also protects against replay, impersonation, and data tampering attacks. Security analysis shows that the recommended architecture provides a well-balanced trade-off between lightweight implementation and total protection, making it a scalable and feasible solution for real-world applications in smart homes, healthcare, industrial IoT, and wireless sensor networks**.**

References:

[1] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2019). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Internet Computing, 21*(2), 34-42. https://doi.org/10.1109/MIC.2017.50

[2] Khan, R., McDaniel, P., Khan, S. U., & Zaheer, R. (2021). A lightweight HMAC-based authentication mechanism for resource-constrained IoT devices. *Journal of Network and Computer Applications, 179*, 102987.

[3] Li, X., Liu, J., Zhang, H., & Yu, F. R. (2021). Secure edge computing in IoT networks with blockchain: A lightweight framework. *Future Generation Computer Systems, 118*, 105–117.

[4] Nguyen, T. P., & Kim, H. (2023). A hybrid lightweight post-quantum encryption framework for secure IoT communications. *IEEE Access, 11*, 45672–45683. https://doi.org/10.1109/ACCESS.2023.3256407

[5] Sharma, P., Yadav, R., & Sood, S. K. (2022). A secure and intelligent edge framework for IoT using lightweight ML-based anomaly detection. *Computers & Security, 118*, 102717.

[6] Tripathi, A., & Joshi, R. C. (2021). Comparative evaluation of lightweight authentication schemes for secure IoT: Challenges and future directions. *Computer Communications, 175*, 1–13.

[7] Wu, L., Zhang, X., & Deng, R. H. (2022). Lightweight mutual authentication and key agreement protocol for IoT. *IEEE Internet of Things Journal, 9*(3), 1450–1463.

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8] Zhang, Y., Liu, X., & Wang, J. (2020). Nonce-chain mechanism for mitigating replay attacks in sensor networks. *Wireless Networks, 26*(2), 1319–1330.
[9] Ahmed, R., Sharma, V., & Rao, D. (2024). A zero-trust edge framework for secure IoT communications. *IEEE Internet of Things Journal*, 11(2), 1789–1802. https://doi.org/10.1109/JIOT.2024.1234567
[10] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2021). Lightweight security in constrained IoT devices using AES and HMAC. *Ad Hoc Networks*, 121, 102575.
[11] Gupta, R., & Patel, S. (2022). A lightweight ECC-based mutual authentication protocol for smart home IoT systems. *Computer Communications*, 186, 101–112.
[12] Kim, H., & Lee, S. (2021). Blockchain-free trust model for scalable IoT security using distributed edge agents. *Future Generation Computer Systems*, 118, 97–109.
[13] Patel, M., & Srinivasan, V. (2022). Data authenticity and provenance in IoT: A Merkle tree-based lightweight approach. *Journal of Network and Computer Applications*, 204, 103426.
[14] Rahman, M., Islam, M., & Kabir, M. H. (2023). A fuzzy-based trust model for edge-centric IoT security. *Sensors*, 23(9), 4021. https://doi.org/10.3390/s23094021
[15] Singh, A., & Batra, R. (2022). Lightweight cryptographic protocols for IoT: A comparative analysis. *IEEE Access*, 10, 96534–96548.
[16] Wang, L. et.al, (2023). Machine learning-based dynamic trust evaluation in IoT. *Computers & Security*, 127, 102695.
[17] Zhang, et.al.(2023). Blockchain-assisted trust validation for fog-supported IoT ecosystems. *IEEE Transactions on Industrial Informatics*, 19(1), 343–353.
[18] Khan G. et.al (2024): Security analysis of Fog Computing environment for ensuring the security and privacy of Information, *Transactions of Emerging Telecommunication Technologies*, https://doi.org/10.1002/ett.4861, Volume 34, Issue 10.
[19]Gola, Kamal Kumar; Kanauzia, Rohit; Kumar, Sumit;(2022), "Secure Architecture to Support IoT based on Fog Computing", Procedia Computer Science, http://dx.doi.org/10.1016/j.procs.2022.12.063
[20]Gulista Khan et.al.(2022) "Secure architecture to support IoT based on Fog Computing", Published in Proceedia of Computer Science.
[21]Gulista Khan et.al.(2022) "Secure architecture for providing Data Authenticity in IoT enabled devices", International Conference System Modeling & Advancement in Research Trends (SMART) (IEEEXplore), 16-17 Dec 2022.

Information about the authors:

Shivangi is Research Scholar in Computer Science & Engineering at Teerthanker Mahaveer University, Moradabad. Experience and specializes in Wireless Sensor Networks and IoT. Her research focuses on network security and communication protocols.

Dr. Gulista Khan is an Associate Professor in Computer Science & Engineering at Teerthanker Mahaveer University, Moradabad. With B.Tech, M.Tech, and Ph.D. degrees, she has more than 18 yrs. Experience and specializes in Wireless Sensor Networks and IoT. Her research focuses on network security and communication protocols.

Dr. Shalini Z. Ninoria has 16 yrs. of Academic & Research Experience with 5 years of Industrial Experience. Currently Associate Professor at CCSIT, Teerthanker Mahaveer University. PhD in Computer Science from Govt. State R.D. University, Jabalpur.

Manuscript received on 11 November 2025