International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Security Framework for Authentication and Integrity Verification in IoT-WSN Healthcare Applications

E. Nandhinipriya[1], Dr. R. Manikandan[2], Dr. K. Kamali[3]

[1]Assitant Professor, Department of Computer Science, Annamalai University. Chidambaram, Tamilnadu, India
Corresponding Author Email: *enandhinipriyaphd[at]gmail.com*

[2]Assistant Professor, Department of Computer Science, Annamalai University, Chidambaram, Tamilnadu, India
Email: *rmkmanikandan1111[at]gmail.com*

[3]Associate Professor, Department of Computer Science, Annamalai University. Chidambaram, Tamilnadu, India
Email: *kamaliaucse2006[at]gmail.com*

Abstract: ***Rapid adoption of Internet of Things (IoT) has introduced critical problems, particularly related to security and privacy. The heterogeneous characteristics of IoT makes authentication difficult since ensuring both efficiency and security simultaneously remains challenging. This paper proposes a security framework for authentication and integrity for IoT-WSN Healthcare applications. The proposed framework employs a three-layer IoT architecture that includes the IoT layer, Edge layer, and Cloud layer. It consists of two phases. In phase-1, Two-factor authentication is performed in which device registration is done initially, followed by device ID based authentication. In phase-2, Hash based data integrity checking is performed using the hashing technique, Spongent. Experimental results have shown that the proposed framework attains improved throughput and reduced energy consumption, when compared to other schemes.***

Keywords: Internet of Things (IoT), Security, Authentication, Integrity, Spongent

1. Introduction

The Internet of Things (IoT) is an emergent technology that connects sensors, physical devices, and equipment over the Internet, allowing seamless data exchange and communication. By 2025, it is projected that more than 75 billion devices will be connected globally, with healthcare being one of the main beneficiaries. In healthcare, IoT facilitates personalized treatment, remote monitoring, and efficient service delivery, ultimately enhancing patient outcomes and revolutionizing care models [1]. IoT applications in healthcare comprise telemedicine for virtual consultations, mobile apps and wearable devices for vital sign tracking, and safe patient portals for data communication and sharing. [2].

However, the rapid adoption of IoT has introduced critical problems, particularly related to security and privacy. The widespread deployment of sensor nodes in unsupervised environments necessitates robust mechanisms for safeguard sensitive data and devices against malicious attacks and unauthorized access. The interdependence of security and privacy is essential to maintain trust and integrity in IoT systems, making privacy-preserving security approaches crucial [3]. Key challenges comprise the large-scale and heterogeneous nature of IoT networks that complicates management and oversight. Limited computational resources leave IoT devices highly susceptible to both physical and cyber threats. [4].

The heterogeneous characteristics of IoT makes authentication difficult since ensuring both efficiency and security simultaneously remains challenging. Inadequate authentication over wireless communication channels can affect data integrity, making authentication a vital method to validate the legitimacy of nodes and preserve trustworthy data exchange [5]. Authentication is seen as the first line of defense in IoT security for protecting against threats like man-in-the-middle (MITM), denial of service (DoS), replay attacks, forgery, and password guessing. However, several existing authentication protocols did not have robustness, leaving exposures that attackers exploit [6].

Conventional authentication mechanisms often fail to adapt to the resource constraints of IoT devices, including limited memory, processing power, and energy capacity, making lightweight yet robust solutions vital. Effective authentication and privacy approaches are vital for maintaining trust, ensuring compliance, and safeguarding sensitive healthcare information within IoT-WSN environments [7].

The main objective of this research work is:
To develop a security framework with authentication for IoT-WSN Healthcare applications.

2. Related Works

A lightweight hybrid cryptographic framework [8] is proposed that integrates Verifiable Random Functions (VRF), Authenticated Encryption with Associated Data (AEAD), and the Elliptic Curve Digital Signature Algorithm (ECDSA). While designed for resource-constrained IoT environments, the framework ensures robust data authentication, integrity, confidentiality, and non-repudiation with less computational overhead. AEAD (AES-GCM or ChaCha20-Poly1305) integrates integrity verification and encryption in a single process,

outperforming conventional AES-CTR with HMAC by minimizing processing time and storage requirements. VRF offers verifiable randomness to reinforce resistance against replay attacks, whereas ECDSA provides lightweight digital signatures with lower overhead when compared to RSA. Benchmark results prove that the proposed framework lessens CPU load, encryption time, and memory consumption when compared with the conventional methods, making it highly appropriate for IoT applications like sensor data protection, secure messaging, and distributed access control.

A novel data integrity methodology [9] is proposed for IoT applications depending on a two-phase protocol with sequence sharing and data exchange. In the first stage, node pairs utilize a chaotic model for securely exchanging identity information and generating a common sequence, while supporting authentication and timing for packet validation. The second stage guarantees packet integrity. The method is assessed across several scenarios and compared with conventional integrity protocols. Experimental results prove that it lessens energy consumption and packet overhead, is efficient, cost-effective, removes third-party auditors, and is robust against diverse threats, making it appropriate for practical IoT applications.

A trust-aware hybrid framework [10] is proposed that combines CNN, LSTM, and VAE for analysing temporal, spatial, and latent features of physiological signals in healthcare IoT (H-IoT). A Trust-Aware Controller (TAC) dynamically produces trust scores depending on context entropy, anomaly probability, and historical patterns, implementing access through threshold-based logic and quarantine mechanisms. Assessments on benchmark and proprietary datasets under attack scenarios attained 96.1% classification accuracy and 94.3% F1-score, while outperforming baselines by 12%–18%. Edge deployment on Raspberry Pi and Jetson Nano maintain latency below 160 ms. The framework ensures robust, scalable, and adaptive security for next-generation H-IoT ecosystems.

A secure and adaptive framework for edge-based data aggregation (SAFED) is proposed [11] that consists of IoT nodes, Edge Devices, a Trusted Authority, a Public Cloud, and a Control Center. Data from IoT nodes is digitally signed, encrypted, authenticated by edge devices, and collected before being transmitted to the cloud. The Control Centre decrypts aggregated data as required. SAFED utilizes efficient cryptographic methods, while ensuring fault tolerance, reducing communication and computation costs, and improving energy efficiency and overall system performance.

A blockchain-based data integrity authentication technique [12] is proposed to improve security and efficiency within cloud computing. Blockchain reinforces cloud security, ensures secure operations, and avoids threats or unauthorized access. The method incorporates data integrity authentication for safeguarding cloud storage and ensuring only legitimate users gain access. Cuckoo filters and Merkle Hash Trees (MHT) are employed for improving authentication. The approach aims to strengthen both data protection and user authentication within the cloud environment. Its efficiency is assessed using various performance metrics, such as authentication, processing, consensus, and storage overhead, confirming its potential for secure cloud operations.

2.3 Research Gaps

In spite of significant progressions, several research gaps remain in proposing a comprehensive security framework for privacy protection and authentication within IoT-WSN healthcare applications. Initially, most lightweight cryptographic algorithms solve resource constraints but fail to preserve strong real-time performance essential in healthcare monitoring systems. Secondly, while ensuring data integrity, blockchain confronts challenges of bandwidth usage, energy consumption, and usability, restricting its practical adoption in resource-constrained IoT-WSN environments.

3. Proposed Methodology

3.1 System Model

The proposed framework employs a three-layer IoT architecture that includes the IoT layer, Edge layer, and Cloud layer, as shown in Figure 1. The lowest layer is the IoT layer that consists of highly distributed and latency-sensitive IoT nodes that require real-time data processing. The intermediate Edge layer comprises edge devices that offer storage and processing resources for IoT nodes, serving as a bridge between IoT devices and the cloud. These edge devices allow computation, location awareness, and data storage closer to the network's edge, thus minimizing latency. At this level, data from IoT nodes is aggregated before being sent to the uppermost layer.

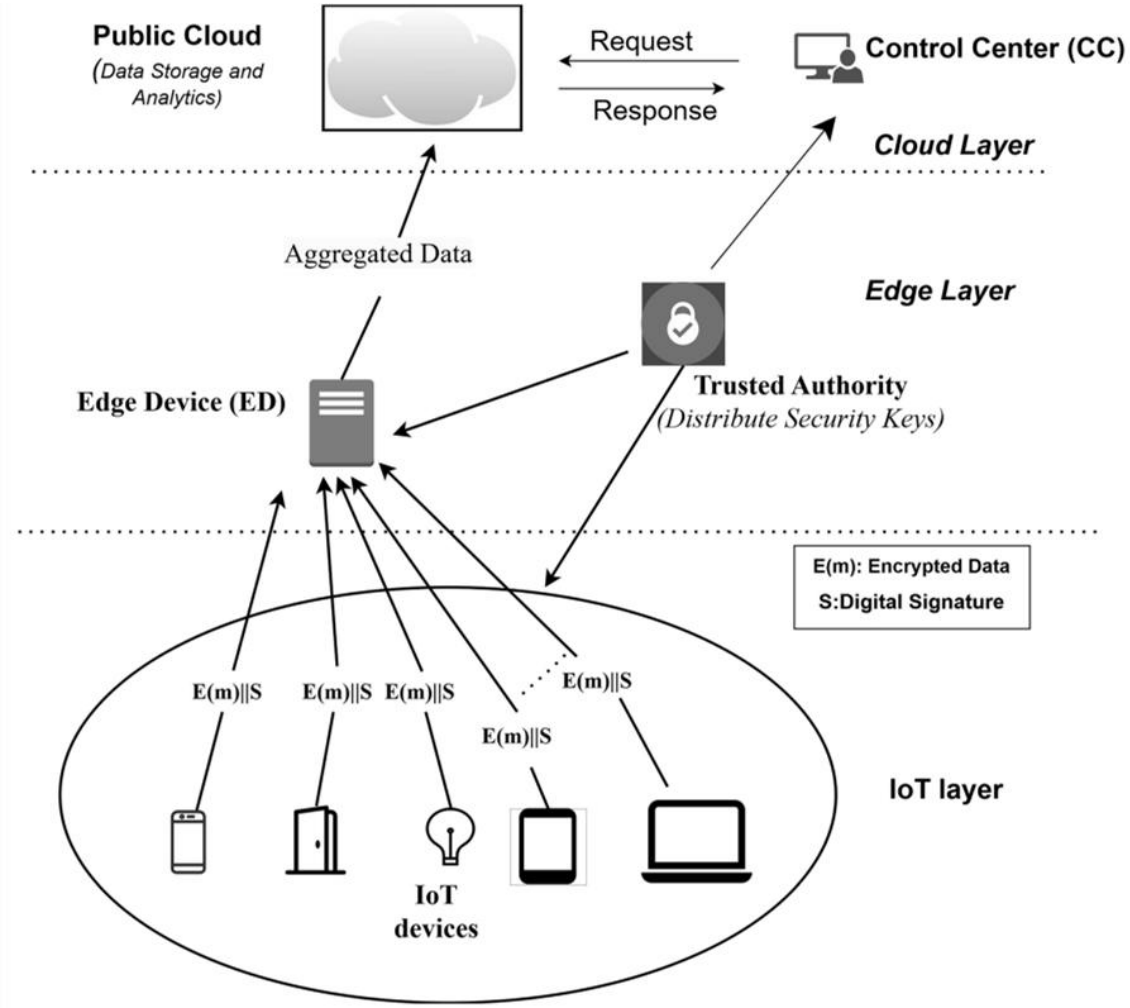

Figure 1: System Model

The Cloud layer has the public cloud and a control centre. The public cloud stores collect data for analysis, whereas the control centre handles access to this data based on operational requirements.

The proposed framework includes the following entities:

1) **Trusted Authority (TA):** A reliable component accountable for creating cryptographic keys for digital signatures and encryption. By distributing necessary security parameters to users, TA initializes the system. After this setup, it does not participate in following processes, while ensuring independent system operation.
2) **IoT Nodes (N):** Smart devices in an IoT network that gather data and execute cryptographic functions like digital signatures and encryption before sending the data to the edge device.
3) **Edge Device (ED):** The framework's central element that aggregates data from IoT nodes and safely forwards it to the public cloud. The ED ensures confidentiality, integrity, and authentication of the aggregated data with greater computational and storage capabilities than IoT nodes but fewer than cloud servers.
4) **Public Cloud (PC):** The PC acts as the storage hub for aggregated data sent by EDs, providing virtually unlimited storage capacity. Its main features comprise scalability to fulfil dynamic storage requirements, improved durability and availability via secure multi-location storage, and support for managing huge volumes of data. For instance, in a smart city scenario, a public cloud service like Amazon Web Services (AWS) can be utilized for storing and analysing traffic sensor data, enabling real-time insights for efficient urban management.
5) **Control Center (CC):** The CC serves as an authorized utility provider in the framework, mainly significant within smart grid applications. With direct access to the cloud, it recovers collected data forwarded by EDs. The CC then executes decryption through its private keys for reconstructing the original data, ensuring secure management. This allows the CC to monitor performance, find anomalies, and optimize resource allocation. For example, within a smart grid, the CC can analyse energy consumption trends to enhance distribution efficiency and maintain reliable system operations.

It is assumed that,

- Both ED and PC are considered as semi-trusted entities that obey with the protocol but may try to access IoT node readings.
- IoT nodes are expected to be homogeneous, indicating that they are identical in data generation rate, data type, and resource capacity. For example, within a smart grid, all smart meters are designed for recording and transmitting electricity usage data with uniform communication and processing capabilities.

- IoT node users are regarded as honest; therefore, IoT nodes are tamper-proof.
- External attackers may compromise ED or PC; nevertheless, the individual IoT node readings' confidentiality remains intact.
- An attacker may insert false data into the network; though, such anomalies can be recognized and filtered at the ED.

3.2 Security Framework with Authentication

In this paper, a security framework with authentication and data integrity for IoT Healthcare applications is proposed.
It consists of two phases:

- **Two-factor authentication**: In this phase, device registration is done initially, followed by device ID based authentication.
- **Hash based Data Integrity checking:** For checking the integrity of sensed data, a lightweight hashing technique, Spongent is applied.

3.2.1 Data Integrity using Spongent Hashing technique

Spongent is **not** a public–key algorithm like RSA. It is a lightweight cryptographic hash function (a family of sponge-based hashes) designed for constrained devices such as IoT and RFID. So when we talk about a Spongent-based digital signature, it is usually in the context of hash-and-sign schemes. A sponge construction absorbs an input message into an internal state and then squeezes out a digest of fixed length. It has different variants like Spongent-128, Spongent-160, Spongent-256. It provides collision resistance, pre-image resistance, and is suitable for resource-limited devices.

A. Signature Creation Process

(i) **Message preparation**

The signer takes the original message M.

(ii) **Hashing with Spongent**

Apply Spongent to M to compute a digest h.

$$h = \text{Spongent}(M) \quad (1)$$

(iii) Sign the hash

- Use a hash-based signature scheme like XMSS or SPHINCS).
- With a private signing key SK, generate the signature S.

$$S = \text{Sign}(SK, h) \quad (2)$$

B. Signature Validation Process

(i) Hash the received message

The receiver computes the digest h' of the received message M using the same Spongent variant**.**

$$h' = \text{Spongent}(M) \quad (3)$$

(ii) Verify the signature

Using the signer's public key **(PK)**, verify that the signature S corresponds to the digest h'.

$$\text{valid} = \text{Verify}(PK, h', S) \quad (4)$$

(iii) Decision

- If verification succeeds, the message is authentic and unmodified.
- Otherwise, reject it.

C. Illustration

Signer (with private key):

$$M \rightarrow \text{Spongent}(M) = h \rightarrow \text{Sign}(SK, h) = S \rightarrow \text{Send}(M, S) \quad (5)$$

Verifier (with public key):

$$\text{Receive}(M, S) \rightarrow \text{Spongent}(M) = h' \rightarrow \text{Verify}(PK, h', S) \quad (6)$$

3.3.1 Two-factor Authentication for Data Protection and Privacy

The optimized resource allocation and secure exchange of information within this infrastructure are attained using RSA. This helps in mitigating breaches and adversarial threats in processing systems. Preventive and defensive security mechanisms are used to minimize vulnerabilities during data processing and ensure data protection and user privacy. User and service provider authentication depends on the parameters (U_{rq}, s_d, S_F),. New security measures are generated dynamically for reinforcing privacy when location exploration suggests a loss or breach of user data.

The steps involved for generating new privacy measures in authentication are:

1) Define variables m and n for representing user requests and responses, while ensuring $m \neq n$, thus providing data protection under variable conditions and explorations.
2) Validate the security factor as:
$$SF = m * n \quad (7)$$
3) Calculate authentication as:
$$U_{rq}(s_d) = (m - 1)(n - 1) \quad (8)$$
4) Calculate the new privacy measure (NPM) as:
$$N_{PM}Z \equiv 1(\text{mod}(U_{rq}(s_d)) \quad (9)$$

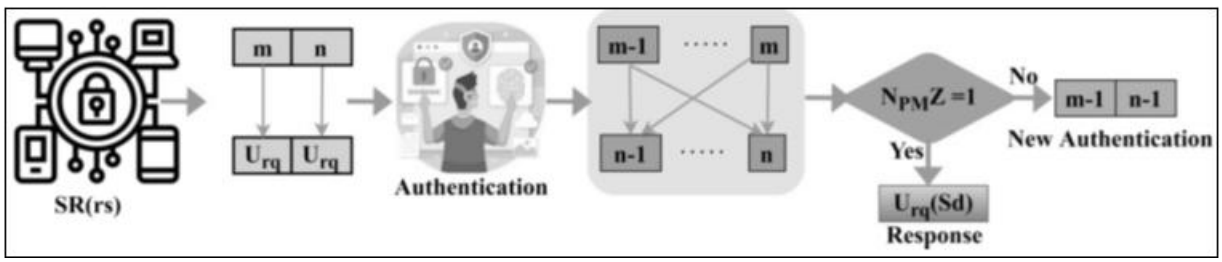

Figure 2: Security Implementation

4. Experimental Results

In this section, the results corresponding to signing and hashing of datasets are presented. The proposed Spongent algorithm is compared with RSA and other light weight algorithm U-Quark.

Figure 3 and 4 show the results of throughput for Hashsize 128 and 64, respectively.

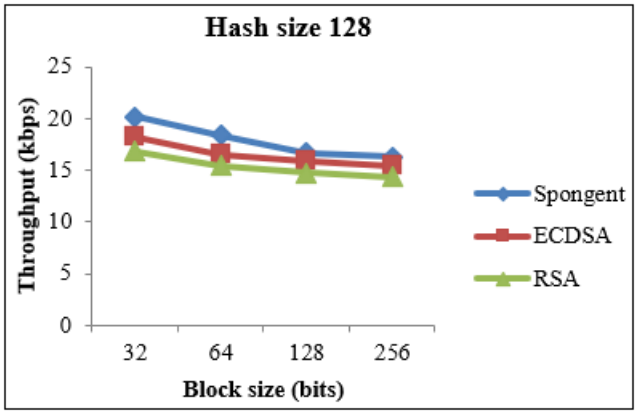

Figure 3: Throughput (Hash size 128)

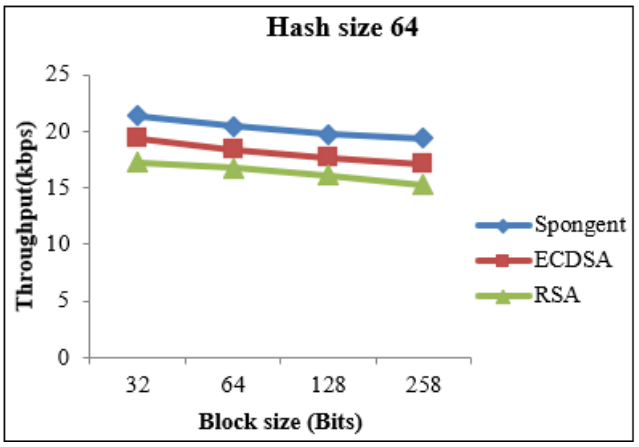

Figure 4: Throughput (Hash size 64)

From Figure 3, the throughput of Spongent is 5% higher than ECDSA technique and 9% higher than RSA method.

From Figure 4, the throughput of Spongent is 7% higher than ECDSA technique and 12.7% higher than RSA method.

Figure 5 and 6 show the results of energy consumption for Hashsize 128 and 64, respectively.

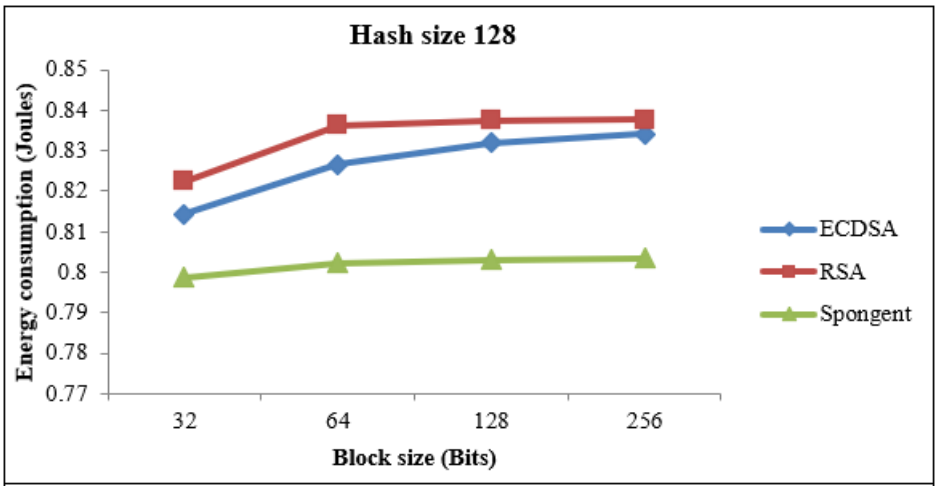

Figure 5: Energy consumption (Hash size 128)

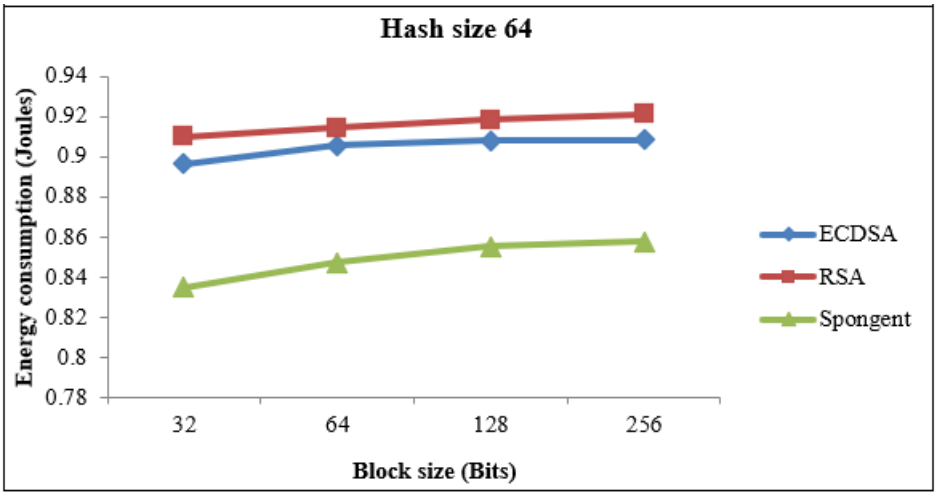

Figure 6: Energy consumption (Hash size 64)

From Figure 5, the energy consumption of Spongent is 3% lesser than ECDSA and 3.7% lesser than RSA.

From Figure 6, the energy consumption of Spongent is 6% lesser than ECDSA and 7% lesser than RSA.

5. Conclusion

This paper proposes a security framework for authentication and integrity for IoT-WSN Healthcare applications. The proposed framework employs a three-layer IoT architecture that includes the IoT layer, Edge layer, and Cloud layer. It consists of two phases. In phase-1, Two-factor authentication is performed in which device registration is done initially, followed by device ID based authentication. In phase-2, Hash based data integrity checking is performed using the hashing technique, Spongent. Experimental results have shown that the proposed framework attains improved throughput and reduced energy consumption, when compared to other schemes.

References

[1] I. H. Memon, Y. Jiaoyun, M. T. Hassan, and A. Ning, "The role of the Internet of Things (IoT) and Wireless Sensor Network (WSN) in healthcare," *Int. J. Eng. Trends Technol.*, vol. 67, no. 7, pp. 92–96, 2019.

[2] T. Jabeen, I. Jabeen, H. Ashraf, N. Z. Jhanjhi, A. Yassine, and M. S. Hossain, "An intelligent healthcare system using IoT in Wireless Sensor Network," *Sensors*, vol. 23, p. 5055, 2023, doi: 10.3390/s23115055.

[3] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in IoT," *e-Prime - Adv. Electr. Eng., Electron. Energy*, vol. 4, p. 100158, Jun. 2023.

[4] A. Wakili and S. Bakkali, "Privacy-preserving security of IoT networks: A comparative analysis of methods and applications," *Cyber Secur. Appl.*, vol. 2, 2025.

[5] J. S. Yalli, M. H. Hasan, L. T. Jung, and S. M. Al-Selwi, "Authentication schemes for Internet of Things (IoT) networks: A systematic review and security assessment," *Internet Things*, vol. 30, 2025.

[6] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions," *Sensors*, vol. 25, p. 1649, 2025, doi: 10.3390/s25061649.

[7] A. J. Andrew and J. Karthikeyan, "Privacy-preserving Internet of Things: Techniques and applications," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6, Aug. 2019.

[8] H. Verma and N. M. Dubba, "Hybrid data integrity verification for real-time IoT systems using AEAD and VRF with ECDSA," *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 34s, 2025.

[9] M. A. Alkhonaini, F. A. Alenizi, Y. H. Jazyah, and S. Lee, "A two phase spatiotemporal chaos based protocol for data integrity in IoT," *Sci. Rep.*, vol. 14, p. 8629, 2024.

[10] N. Naik, N. Surendranath, S. A. B. Raju, C. Madduri, N. Dasari, V. K. Shukla, and V. Patil, "Hybrid deep learning-enabled framework for enhancing security, data integrity, and operational performance in healthcare Internet of Things (H-IoT) environments," *Sci. Rep.*, vol. 15, p. 31039, 2025.

[11] Z. Naaz, G. Joshi, and V. Sharma, "SAFED: Secure and adaptive framework for edge-based data aggregation in IoT applications," *Discover Internet Things*, vol. 5, p. 42, 2025, doi: 10.1007/s43926-025-00143-3.

[12] A. Ramachandran, P. Ramadevi, A. Alkhayyat, and Y. K. Yousif, "Blockchain and data integrity authentication technique for secure cloud environment," *Intell. Autom. Soft Comput.*, vol. 36, no. 2, 2023.