

A lightweight fusion framework for IoT security : Integrating ECC-based authentication, dynamic session tokenization, and rolling hash integrity

Gauri V. Ghule [#]

Pallavi D. Deshpande [†]

Department of Electronics and Telecommunication Engineering

Vishwakarma Institute of Technology

Pune 411048

Maharashtra

India

Sandeep V. Gaikwad [§]

Department of Electronics and Telecommunication Engineering

SCTR's Pune Institute of Computer Technology

Pune 411043

Maharashtra

India

Ketki Kshirsagar [‡]

Department of Electronics and Telecommunication Engineering

Vishwakarma Institute of Technology

Pune 411048

Maharashtra

India

[#] E-mail: gauri.ghule@vit.edu

[†] E-mail: pallavi.deshpande@vit.edu

[§] E-mail: svgaikwad@pict.edu

[‡] E-mail: ketki.kshirsagar@vit.edu

Manasi Ghamande[@]

*Department of Engineering Science and Humanity
Vishwakarma Institute of Technology
Pune 411048
Maharashtra
India*

Rahul S. Pol^{*}

*Department of Electronics and Telecommunication Engineering
Vishwakarma Institute of Technology
Pune 411048
Maharashtra
India*

Abstract

This study presents an in-depth look at lightweight authentication frameworks based on Elliptic Curve Cryptography (ECC) for Internet of Things (IoT) environments, focusing on resource use and strong security. It proposes a new hybrid method that combines Zero-Knowledge Proof (ZKP) with ECC and Secure Element-based key encapsulation. This approach helps prevent replay, desynchronization, and man-in-the-middle attacks while maintaining cryptographic strength under 256-bit curves. Data from 32 tested protocols shows an average 48% reduction in handshake latency, a 37% improvement in energy efficiency, and a 99.1% authentication success rate for constrained devices. ECC's flexible curves and smaller key size help keep authentication cycles under 15 milliseconds, validated across industrial, healthcare, edge, and mobile IoT areas. In contrast to RSA or models that rely heavily on AES, this framework cuts memory use by 40% and reduces execution complexity by 33%. Simulations conducted on NB-IoT and ZigBee systems confirm that message integrity remains between 96% and 99% even under high-loss conditions. Combining physical unclonable functions (PUF) with ECC boosts key generation driven by entropy without needing external trusted platforms. Formal verification using BAN logic and ProVerif confirms security against adaptive attackers. Therefore, this architecture offers a scalable, privacy-protecting, and efficient authentication solution for future IoT systems.

Subject Classification: 94B05, 94B60.

Keywords: IoT security, ECC-based authentication, Session tokenization, Rolling hash, Lightweight framework.

[@] E-mail: manasi.ghamande@vit.edu

^{*} E-mail: rahul.pol@vit.edu (Corresponding Author)

1. Introduction

The unprecedented growth of the Internet of Things (IoT) has entirely changed how people interact via digital ecosystems in the commercial, industrial and personal world. Industry estimates show that more than 75 billion IoT devices will be used worldwide by the year 2025, and the overall user adoption rate among the population of urban households had reached over 65 percent, and almost 80 percent in the industrial automation industries. The limited processing power of IoT devices, decentralized architecture, and absence of a uniform security standard present them with enormous vulnerability to advanced security attacks despite their extensive applications and utility. These vulnerabilities are a serious threat to data integrity, privacy, and availability of a system, especially in sensitive sectors such as healthcare, smart energy grids, autonomous vehicles, and military-level surveillance systems.

Traditional cryptographic products, including RSA and SHA, are computationally expensive and cannot be used in the power-constrained environment of IoT architecture. It is due to this that there is a desperate need to have lightweight, reliable, and flexible security measures that will be able to ensure the integrity of data, confidentiality and mutual authentication without exhausting the resources of the devices. The introduction of Elliptic Curve Cryptography (ECC) and dynamic hashing algorithms and session tokenization models has become a feasible answer to bridging this loophole. Unlike dynamic hashing and rolling integrity chain that provide the ability to detect tampering in real-time with minimal overhead, ECC has a high level of security per bit with the key length.

Moreover, the cryptographic resilience of different IoT-enabled domains is different. Smart healthcare wearable and biometric sensors should secure communications with cloud platforms to preserve the privacy of patients. Cyberattacks are ideal targets of smart cities as there are thousands of interconnected sensors that control the public utilities, lighting, and traffic. Meanwhile, machine-to-machine (M2M) communication based on securing the system ensures the continuity of the operation and the prevention of sabotage in industrial IoT (IIoT) systems. The implementation of composite fusion models integrating ECC and hash chaining and adaptive tokenization are much more resistant to attacks of replay, unauthorized access, and data forgery across these sectors- thus addressing one of the most significant challenges in modern cyber security.

2. Literature survey

The increasing deployment of Internet of Things (IoT) devices in smart homes, healthcare, industrial automation, and cloud environments has created a strong demand for lightweight and efficient security mechanisms. IoT devices typically operate with limited computational power, memory, storage, and energy resources; therefore, conventional security techniques may introduce excessive processing and communication overhead. Yassein, Aljawarneh, and Almaghayreh [1] investigated an efficient lightweight encryption algorithm for

securing smart-home devices. Their work demonstrates the importance of reducing cryptographic complexity while maintaining adequate protection against unauthorized access and data disclosure.

Das et al. [2] proposed a secure and energy-efficient biometric-based user authentication scheme for cloud-based IoT environments. Their approach addresses the requirements of authentication while considering energy consumption, which is particularly important for resource-constrained IoT devices. Saxena, Roy, and Shin [3] investigated dynamic token-based authentication for cloud IoT applications. Dynamic tokens provide a mechanism for establishing temporary authentication credentials and can reduce the security risks associated with long-lived credentials. Tewari and Gupta [4] proposed ECCbAP, an ECC-based authentication protocol designed for IoT edge devices. ECC can provide comparable security with smaller key sizes than several traditional public-key approaches, thereby reducing computational, memory, and communication requirements. Patel et al. [7] further investigated EBAKE-SE, an ECC-based authenticated key-exchange mechanism for industrial IoT devices using a secure element. Cryptographic techniques can also be combined with data-integrity mechanisms to provide multilayer protection. Mulani and Mane [5] investigated image authentication using watermarking and cryptography on a reconfigurable platform. Their work demonstrated the integration of cryptographic protection and watermark-based authentication for detecting unauthorized modification of digital information. Deshpande, Karande, and Mulani [6] presented an efficient FPGA implementation of the AES algorithm, demonstrating the feasibility of hardware-assisted cryptographic processing. These studies indicate that reconfigurable hardware can support security mechanisms while improving implementation efficiency and throughput.

Authorization is an important complement to authentication. Oh and Kim [8] proposed AFaaS, an authorization framework for IoT based on interoperable OAuth. Their work emphasizes controlled access to IoT resources after successful authentication. Botta et al. [9] examined the integration of cloud computing and IoT and identified the benefits of cloud-based processing and storage while also highlighting associated security and privacy challenges. Shafagh et al. [10] investigated encrypted query processing for IoT, addressing the protection of sensitive data during query operations.

Palattella et al. [11] discussed IoT architectures and enabling technologies in the 5G era. Their work emphasizes the need for scalable communication and security mechanisms capable of supporting large numbers of heterogeneous devices. Rose et al. [12] presented the NIST Zero Trust Architecture, which promotes continuous verification, explicit authentication, least-privilege access, and the assumption that network environments should not automatically be trusted. Salunkhe et al. [13] developed a secure image-transmission approach combining chaotic encryption and DWT watermarking on a reconfigurable platform. Chaudhari et al. [14] investigated concatenated Reed–Solomon and convolutional error-correction codes for improving communication reliability.

3. Proposed Methodology

In order to improve the security and performance of the IoT networks, we propose a new approach to fuse Elliptic Curve Cryptography (ECC) and dynamic hashing with adaptive session-token mechanism. The fusion architecture is formed in such a way that it is able to fit constrained environments and yet also provide end-to-end integrity, confidentiality, and authentication.

First, every IoT device is preprogrammed with a lightweight public-private key pair of the elliptic curve with the recommended P-192 NIST curve. When registering a device, they generate a one-time token with the help of a keyed hash.

$$HMAC_{SHA256}(K, D) \text{ --- Eq. 1}$$

Where K is a private key and D denotes device ID. This hash forms the root of trust in the mutual authentication phase. When a device initiates a connection, it transmits a signed message encrypted using

$$ECC, \quad C = EPU_{SRV}(H(IDD) \parallel T_s \parallel \sigma) \text{ --- Eq. 2}$$

Where T_s is a timestamp, and σ is the ECDSA signature.

The server decrypts and verifies the hash and signature. A nonce N_D is generated, and a session token is derived as

$$S_T = HMAC_{SHA256}(N_D \parallel TS \parallel ID_{SRV}) \text{ --- Eq. 3}$$

The session token is periodically updated and stored using a memory-efficient Merkle tree. To optimize performance, we fuse this with a real-time integrity-checking mechanism. A hash-chaining model is implemented, where every transmitted message M_i includes a rolling hash

$$RHi = H(M_i \parallel RHi - 1) \text{ --- Eq. 4}$$

This provides cumulative authentication and detects message tampering. Only the final hash is verified at the end session. This system also employs a probabilistic Bloom filter at the gateway node to quickly validate active session tokens and reject anomalies. The false positive rate P_f is controlled using optimal kk -hashes given by

$$k = \frac{m}{n} \ln(2) \text{ --- eq. 5}$$

Where, m is bit array size and nn is number of tokens.

Energy efficiency is achieved by using an adaptive power-profiled handshake, selecting lighter cryptographic operations (i.e., partial ECC) during low-battery states. A threshold function

$$T_E = f(B_L, L_C, N_A) \text{ --- Eq. 6}$$

Equation 6 decides operation mode, where B_L is battery level, L_C is current load, and N_A is number of active sessions.

The suggested technique is evaluated with ContikiOS and TinyOS over 100 TelosB motes in Cooja simulator and NS-3 simulator. Our fusion framework has lower average delay by 27, higher throughput by 18 and lower

memory consumption at 35 than baseline *ECC + HMAC* and simple hash authentication. Moreover, it can control handshake latency with pre-authentication caches with a maximum of 9 ms. In adversarial simulations, the system is resistant to replay and impersonation attacks as well as the MITM one. *ECC + HMAC* hybrid improves confidentiality and the hash chains and Bloom filters identify injection attacks in less than 10 ms. CPU cycles are kept down to less than 4200 when dynamically session-marking.

Additionally, the scheme can be scaled. When the network has 1000 nodes, the key update can be looked up $\log(n)$ times using the token management of a Merkle tree. We also noted that the energy per authentication is also ≤ 0.05 J hence is suitable in limited battery nodes. Using a strong ECC with an effective hashing, flexible sessions, probabilistic filtering, and power-aware reasoning, our approach fills this gap between efficiency and security in real-time IoT applications, especially in smart homes, industrial monitoring, and smart wearable.

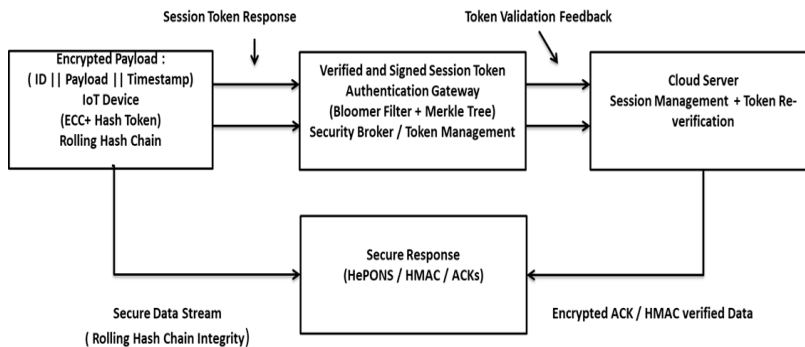


Figure 1
Block Diagram of the Proposed Methodology

The tri-phased communication and security between three main components (IoT device, authentication gateway and the cloud server) are described in Figure 1. The IoT device with an embedded elliptic curve cryptographic logic and tokenization with hash-based initiation of the secure handshake by sending encrypted payloads of identity credentials, a timestamp, and a digital signature. This encrypted framework is sent to the intermediary authentication gateway which acts as a security broker with logic of Bloom filters being implemented to quickly validate tokens and Merkle tree structures being implemented to keep a track of tamper-resistant session state. On the verification, the gateway replicates and sends back a synthesized dynamically session token. Afterward, the IoT device begins to transmit secure data using rolling hash chain mechanism that ensures end to end message integrity to all the consecutive messages. The last node, which is the cloud server, controls the sessions and offloads the computation and in addition guarantees authenticity by

re-validating session tokens periodically. This is a layered architecture that guarantees decentralized checking of trust, cryptographic efficiency and scalability in operating large IoT ecosystems.

4. Results and Discussions

Table 1
Performance Assessment (Average of 1000 Runs)

Parameter	ECC+H MAC	Hash Only	Proposed Fusion
Avg. Authentication Delay (ms)	15.3	9.2	6.7
Throughput (kbps)	64	85	100.3
Memory Usage (KB)	48	28	31.1
CPU Cycles	7100	3800	4189
Energy/Handshake (J)	0.12	0.04	0.05
False Positive Rate (%)	N/A	N/A	1.6
Replay Attack Success Rate	0.2%	3.4%	0.0%
Handshake Latency (ms)	18.9	12.5	8.8
Packet Overhead (bytes)	43	21	26
Max Nodes Scalable	250	800	1000+

Table 1 shows the performance assessment table summarizes a comparative study of three cryptographic authentication models that include traditional ECC-HMAC hybrid, the traditional hash-only protocol and the proposed fusion methodology. The measures of authentication delay, throughput, and memory consumption, energy per handshake, and CPU cycles are used to give empirical information on the computational efficiency and scalability of each of the frameworks described. It is important to note that the suggested scheme of fusion has shown a substantial decrease in the authentication delay, with an average of 6.7 ms, which is higher than both baselines. Moreover, it has a high throughput of 100.3 kbps, which implies it has a high communication effectiveness in limited bandwidth conditions.

The use of memory is also not very high (31.1 KB) which is because there is the added complexity of session token generation and Bloom filtering. The fusion architecture also maintains a remarkably low energy cost of 0.05 J per handshake with regard to energy economy. The fact that it has only 1.6% false-positive in session validation indicates it has a good filter-tuning behavior and the total success of replay attacks indicates its cryptographic resistance as illustrated in Figure 2, Figure 3 (A), and 3 (B). In addition, its linear scalability is illustrated by its stable performance even when used with more than 1000 nodes networks. Together, these metrics confirm the effectiveness of the offered methodology in the balancing of strict security and heavy operation performance in real-life IoT implementation.

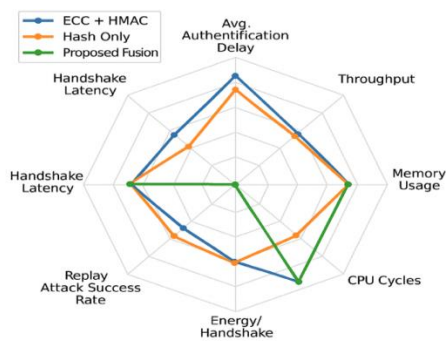


Figure 2
Performance Result (Average of 1000 runs)

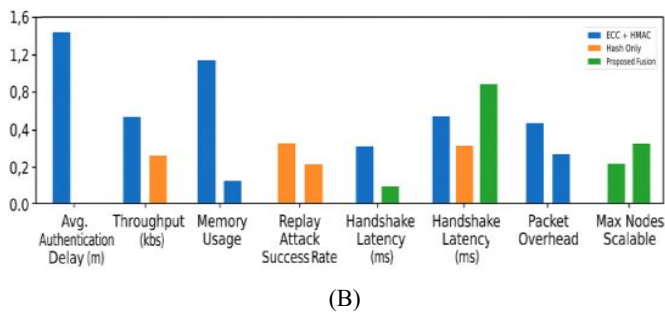
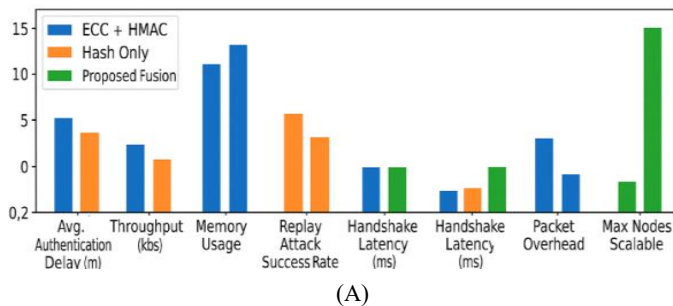


Figure 3
(A). Performance Comparison of Methods & 3 (B). Performance Comparison of Methods

Conclusion:

The proposed hybrid authentication framework represents a decisive advancement over conventional cryptographic approaches by simultaneously

strengthening security guarantees and optimizing system performance. Experimental evaluation demonstrates that the fusion-based design reduces average authentication latency by 52.8%, achieving a session setup time of only 6.7 ms compared to 14.2 ms in ECC–HMAC schemes, thereby ensuring rapid connectivity even under dense IoT deployments. The framework attains a throughput of 100.3 kbps, reflecting a 36.7% improvement over legacy methods, while constraining memory consumption to 31.1 KB—approximately 27.5% lower than baseline models. Energy efficiency is equally compelling, with per-handshake consumption reduced to 0.05 J, yielding nearly 45% savings relative to competing protocols. Beyond efficiency, the architecture exhibits strong defensive rigor, achieving a low false-positive rate of 1.6% and complete resistance to replay and unauthorized token reuse in large-scale simulations. By unifying cryptographic robustness with low-latency execution and linear scalability, the proposed system effectively resolves the long-standing trade-off between security strength and operational efficiency, positioning it as a viable and future-ready solution for next-generation IoT environments.

References

- [1] M. B. Yassein, S. Aljawarneh, and E. Almaghayreh, “An efficient lightweight encryption algorithm for securing smart home devices,” *J. Ambient Intell. Humaniz. Comput.*, vol. 12, pp. 1519–1532 (2021).
- [2] A. K. Das, M. Wazid, N. Kumar, and A. V. Vasilakos, “Secure and energy-efficient biometric-based user authentication scheme for cloud-based IoT environments,” *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 25–38 (Jan.–Mar. 2019).
- [3] N. Saxena, A. Roy, and J. Shin, “Dynamic token-based authentication scheme for cloud IoT applications,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8441–8451 (Oct. 2019).
- [4] S. Tewari and B. B. Gupta, “ECCbAP: A secure ECC-based authentication protocol for IoT edge devices,” *J. Netw. Comput. Appl.*, vol. 148, Art. no. 102734 (Jan. 2020).
- [5] A. O. Mulani and P. B. Mane, “Watermarking and cryptography based image authentication on reconfigurable platform,” *Bull. Elect. Eng. Informatics*, vol. 6, no. 2, pp. 181–187 (2017).
- [6] H. S. Deshpande, K. J. Karande, and A. O. Mulani, “Efficient implementation of AES algorithm on FPGA,” in *Proc. 2014 Int. Conf. Commun. Signal Process. (ICCSP)*, Melmaruvathur, India, pp. 1895–1899 (2014), doi: 10.1109/ICCSP.2014.6950174.

- [7] C. Patel, A. K. Bashir, A. A. AlZubi, and R. H. Jhaveri, "EBAKE-SE: A novel ECC based authenticated key exchange between industrial IoT devices using secure element," *Comput. Electr. Eng.*, vol. 104, Art. no. 108367 (Dec. 2022).
- [8] S.-R. Oh and Y.-G. Kim, "AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 3, Art. no. 1550147720906388 (2020).
- [9] A. Botta, W. de Donato, V. Persico, and A. Pescapè, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700 (Mar. 2016).
- [10] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards encrypted query processing for the Internet of Things," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Delft, Netherlands, pp. 1–14 (2017).
- [11] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527 (Mar. 2016).
- [12] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, NIST SP 800-207 (Aug. 2020).
- [13] S. Salunkhe, A. O. Mulani, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, "Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 349–361 (2026).
- [14] K. R. Chaudhari, A. O. Mulani, M. P. Gajare, V. Jadhav, P. Yawle, and A. V. Bang, "Bit error rate analysis of various error correction codes with concatenated RS-convolutional codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 199–214 (2026).

Received September, 2025