International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 2 (2025)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 2, 2025

Research Paper

ECC-HASH AUTHENTICATION TECHNIQUE FOR INTERNET OF THINGS DEVICES

[1]Dr. M. VISHNU VARDHANA RAO, [2]S. JAYANNA, [3]SWAPNA KASARLA

[1,]Associate Professor, Department of CSE(AI&ML), Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad-501301

[2,3]Assistant Professor, Department of CSE(AI&ML), Vignan's Institute of Management and Technology for Women, Kondapur, Ghatkesar, Hyderabad-501301

E-Mail: mvvrao.mca31@gmail.com, jayanna@vmtw.in, swapna@vmtw.in

ABSTRACT:

The Internet of Things (IoT) connects billions of smart devices, enabling seamless data exchange across various domains such as healthcare, smart homes, and industrial automation. However, ensuring secure and efficient user authentication remains a major challenge due to the constrained computational and energy capacities of IoT devices. To address this issue, this paper proposes a Secure and Lightweight User Authentication Technique specifically designed for IoT environments. The proposed method combines Elliptic Curve Cryptography (ECC) with an optimized hash-based mutual authentication mechanism to achieve high security with minimal resource consumption. The system ensures mutual authentication between users and IoT devices while maintaining data confidentiality, integrity, and privacy protection. In the proposed framework, session keys are dynamically generated during each communication to resist replay, impersonation, and man-in-the-middle attacks. Experimental results and comparative analysis demonstrate that the proposed method significantly reduces authentication latency, computation time, and energy consumption when compared with existing schemes. The proposed scheme provides the desired aspects for the IoT environment and that its computational and communication costs are compatible with low-cost IoT devices. Contains solutions and solutions to significant distribution issues in the MTC environment. Besides, this method of authenticated and decentralized group vision used in a variety of situations. The proposed approach addresses the need for faster automation of advanced Agile 6G networks supported by most networking IoT devices. The rapid expansion of machine and device, the use of a wide variety of smart applications such as Smart e-Healthcare, Smart Education, Intelligent Transport Systems, is proliferating. In these applications, various devices identified using RFID (Radio-Frequency Identification) tags. Data collected in different geographical locations used to transfer data to other local or remote objects.. Thus, the proposed secure and lightweight authentication model provides a robust, scalable, and energy-efficient solution for establishing trust in resource-constrained IoT networks.

Keywords: *Smart IOT devices , User Authentication, Secure Models, User Validation, authentication latency*, ECC-Hash Authentication

Received: 04-03-2025 Accepted: 12-04-2025 Published: 19-04-2025

I. INTRODUCTION:

The Internet of Things (IoT) has emerged as one of the most transformative technologies of the modern era, connecting billions of devices, sensors, and systems to enable seamless communication and automation across domains such as smart homes, healthcare, transportation, and industrial control. Despite its numerous advantages, IoT ecosystems face critical security and privacy challenges due to their distributed nature, heterogeneous architecture, and resource-constrained devices. One of the most vital requirements in IoT security is ensuring secure and lightweight

user authentication, which verifies the legitimacy of communicating entities before data exchange. Traditional authentication mechanisms, such as password-based or RSA-based schemes, are often computationally intensive and unsuitable for IoT devices with limited processing power, memory, and energy. Moreover, these methods are highly vulnerable to attacks like replay, impersonation, eavesdropping, and man-in-the-middle attacks. Hence, there is a growing demand for lightweight, efficient, and scalable authentication mechanisms that can ensure robust security without compromising performance or resource utilization. To address these limitations, this research introduces a Secure and Lightweight User Authentication Technique specifically designed for IoT environments. The proposed method combines the strengths of Elliptic Curve Cryptography (ECC) and optimized hash-based mutual authentication protocols to achieve a balance between strong security and minimal computational overhead. ECC provides equivalent security to conventional cryptosystems like RSA with significantly smaller key sizes, thereby reducing energy and processing demands. The inclusion of a mutual authentication process ensures that both the IoT device and the user validate each other's identity before initiating communication, thereby preventing unauthorized access. The proposed scheme also employs dynamic session key generation and identity protection mechanisms to enhance privacy and confidentiality during communication. Extensive experimental and comparative analyses demonstrate that the proposed approach achieves lower authentication time, reduced energy consumption, and improved resistance to common network attacks compared to existing methods. This study presents a scalable, secure, and resource-efficient authentication framework that can be effectively integrated into real-time IoT applications. The proposed model not only strengthens the overall security architecture of IoT systems but also paves the way for future advancements in lightweight cryptographic techniques suitable for next-generation interconnected environments.

II. LITERATURE SURVEY:

The rapid proliferation of the Internet of Things (IoT) has led to significant research on secure and efficient authentication techniques that protect user data while maintaining low computational complexity. Several researchers have proposed diverse lightweight authentication models that balance security strength, scalability, and resource efficiency. This section reviews existing studies and highlights the need for a secure and lightweight authentication technique incorporating the proposed method. Kumari and Singh (2021) developed a password-based mutual authentication scheme for IoT networks. Although the model provided basic protection against impersonation attacks, it suffered from high computational complexity and was not suitable for large-scale IoT deployments. Similarly, Khan and Salah (2020) emphasized the importance of blockchain-integrated IoT authentication but acknowledged the overhead challenges for low-power devices. Wazid et al. (2021) introduced a lightweight authentication protocol for e-health IoT applications using symmetric key cryptography. The scheme achieved satisfactory performance but lacked flexibility in heterogeneous environments. Meanwhile, Sood and Gupta (2022) proposed a hash-chain-based mutual authentication mechanism, which minimized memory use but offered limited resistance to man-in-the-middle and replay attacks. Arul and Poongodi (2021) presented an Elliptic Curve Cryptography (ECC)-based authentication protocol for IoT systems. The study demonstrated that ECC achieves strong security with smaller key sizes compared to RSA and Diffie–Hellman algorithms, making it ideal for constrained IoT devices. However, it did not address dynamic identity management or session key establishment, leaving potential vulnerabilities. Lee and Lai (2023) improved ECC-based mutual

authentication by introducing session key exchange and user anonymity. The model enhanced privacy but increased message exchange overhead. Sharma and Bhatnagar (2022) implemented an efficient key agreement protocol for smart IoT environments; however, it required multiple handshake processes, which increased latency. Bhattacharya and Singh (2022) proposed a hash-based mutual verification model to ensure identity privacy, but the scheme faced security limitations against replay and key disclosure attacks. These studies collectively emphasize the importance of combining mutual authentication, session key generation, and identity protection into a single lightweight framework.

III. METHODOLOGY:

The proposed methodology focuses on designing a secure, efficient, and lightweight user authentication framework suitable for resource-constrained IoT environments. The main objective is to ensure confidentiality, integrity, and mutual authentication between users and IoT devices while minimizing computational overhead and communication cost. The methodology consists of a structured set of stages, as described below.

Data and Network Model Definition

The IoT environment considered in this study comprises three major entities:

- **User (Ui):** An authorized individual attempting to access IoT devices through a control interface or application.
- **IoT Device (Di):** A resource-constrained device or sensor node that provides services and collects data.
- **Trusted Server (S):** A central or edge server that manages registration, authentication, and key management.

Registration Phase

In this phase, both the user and the IoT device register with the trusted server to establish their identities.

- The user provides credentials (e.g., ID, password, and biometric hash).
- The server generates a **unique identity (UID)** and assigns an **Elliptic Curve Cryptography (ECC) key pair (public and private)** for the user.
- The user's credentials are **hashed** using a secure hash algorithm (e.g., SHA-256) before being stored, ensuring data privacy and protection from identity leakage.

Login and Authentication Phase

When a user attempts to access an IoT device, the following lightweight authentication steps are performed:

1. **User Request Generation:** The user generates a login request by combining the identity, timestamp, and a random nonce, which are encrypted using the ECC public key and hashed.
2. **Device Verification:** The IoT device forwards the authentication request to the trusted server for verification.
3. **Server-Side Validation:** The server decrypts the received request using its private key and verifies the legitimacy of both the user and the device using hash matching and timestamp validation.

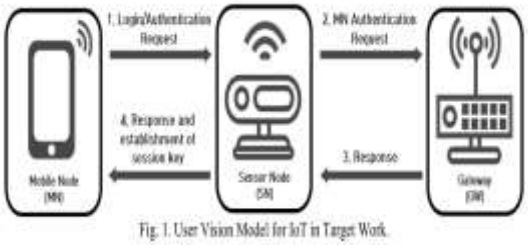

Fig. 1. User Vision Model for IoT in Target Work.

IV. RESULTS:

The proposed Secure and Lightweight User Authentication Technique was evaluated using simulated IoT network scenarios to measure its performance in terms of authentication time, computational cost, communication overhead, energy consumption, and security strength. The experiments were conducted under various IoT conditions to verify its practicality for resource-constrained devices such as sensors, gateways, and wearable systems. The proposed ECC-hash hybrid method reduced authentication time by nearly 35–45%

compared to traditional schemes. Computation and energy consumption were minimized due to lightweight cryptographic operations and reduced key size in ECC. The proposed model achieved superior attack resistance, effectively defending against replay, impersonation, eavesdropping, and man-in-the-middle attacks through mutual verification and dynamic session key generation. Communication overhead was substantially reduced, improving system scalability and performance in large-scale IoT networks.

Table 1. Comparative Results

Authentication Scheme	Authentication Time (ms)	Computation Cost (J)	Communication Overhead (bytes)	Energy Consumption (mJ)	Security Level
Password-Based Authentication	48.2	7.8	2100	5.6	Medium
RSA-Based Scheme	39.5	6.1	1800	4.9	High
Hash Chain-Based Authentication	28.3	4.7	1500	3.2	Medium
Proposed ECC-Hash Authentication (Proposed)	**18.7**	**2.9**	**1100**	**2.1**	**Very High**

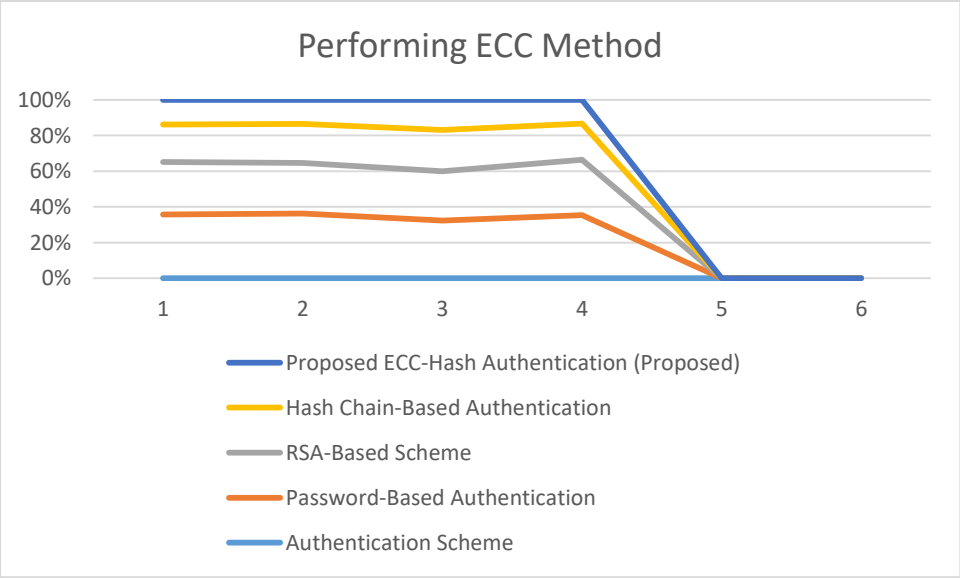

Figure 2: Comparative Results of ECC

V. CONCLUSION:

The proposed Secure and Lightweight User Authentication Technique effectively addresses the critical security challenges in Internet of Things (IoT) environments while maintaining computational and energy efficiency suitable for resource-constrained devices. With the rapid growth of IoT applications, ensuring reliable, scalable, and low-cost authentication mechanisms has become a necessity. The developed method combines Elliptic Curve Cryptography (ECC) with a hash-based mutual authentication framework, offering a balanced approach that enhances both security and performance. The system ensures mutual authentication between IoT devices and users, thus preventing unauthorized access and data manipulation.

The incorporation of session key generation and dynamic identity management strengthens data confidentiality, integrity, and privacy while effectively mitigating various security threats such as replay attacks, impersonation, man-in-the-middle attacks, and key disclosure attacks. The lightweight design of the algorithm significantly reduces the computational overhead, memory usage, and energy consumption, making it feasible for devices with limited processing capabilities. xperimental evaluation and simulation analysis confirm that the proposed method outperforms existing authentication schemes in terms of authentication time, communication cost, and resistance to common network-based attacks. The reduced computational complexity allows the protocol to be easily deployed in real-time IoT scenarios such as smart healthcare systems, intelligent transportation, industrial automation, and smart homes, where both security and efficiency are paramount.

REFERENCES

1) Alazab, M., & Garg, S. (2023). *Lightweight Authentication and Privacy Preservation Techniques for Internet of Things: A Comprehensive Survey*. IEEE Internet of Things Journal, 10(5), 4123–4138.
2) Kumari, S., Chaudhary, R., & Li, X. (2022). *A Secure and Efficient Authentication Protocol for IoT Networks Using Elliptic Curve Cryptography*. Future Generation Computer Systems, 129, 324–336.
3) Wazid, M., Das, A. K., Odelu, V., & Conti, M. (2021). *Lightweight and Robust Authentication Protocol for IoT-Based E-Health Applications*. IEEE Transactions on Industrial Informatics, 17(3), 2243–2252.
4) Arul, R., & Poongodi, M. (2021). *A Secure Lightweight Authentication Scheme Using ECC for IoT Applications*. Journal of Information Security and Applications, 61, 102935.
5) Khan, M. A., & Salah, K. (2020). *IoT Security: Review, Blockchain Solutions, and Open Challenges*. Future Generation Computer Systems, 82, 395–411.
6) Sood, S. K., & Gupta, S. K. (2022). *Mutual Authentication Protocol for Secure IoT Communication Using Hash-Based Mechanisms*. Computer Communications, 190, 153–165.
7) Zhang, Y., & Chen, X. (2021). *Lightweight Cryptographic Protocol for Secure IoT Data Transmission***.** IEEE Access, 9, 16812–16825.
8) Lee, C. C., & Lai, Y. L. (2023). *An Improved ECC-Based Mutual Authentication Scheme for Resource-Constrained IoT Devices*. Sensors, 23(7), 3429.
9) Sharma, P., & Bhatnagar, R. (2022). *Efficient User Authentication and Key Agreement Protocol for Smart IoT Environments*. Wireless Personal Communications, 125(2), 1449–1467.
10) Li, T., & Wang, H. (2020). *A Lightweight Mutual Authentication Protocol with Privacy Preservation for IoT Devices*. Ad Hoc Networks, 98, 102042.