Efficient Authentication and Encryption Techniques for Resource-Limited IoT Devices

S. Vigneshwari
M.E.,AP/ECE, Mahendra Engineering College for Women, Namakkal,

S. Suvitha
AP/ECE, Mahendra Engineering College for Women, Namakkal,

N. Sathiya
M.E.,AP/ECE, Mahendra Engineering College for Women, Namakkal,

S. Vinotha
AP/ECE Mahendra Engineering College for Women,, Namakkal

ABSTRACT **- With the rapid growth of the Internet of Things (IoT), securing resource-constrained devices has become a critical challenge due to their limited computational and memory capabilities. This paper proposes an** integrated lightweightsecurity framework **tailored for such IoT environments. The framework combines** energy-efficient mutual authentication **and** low-complexityencryption **into a hybrid mechanism that dynamically adjusts the security level based on the device's processing capacity and communication context. The proposed system ensures** data confidentiality, integrity, and device authenticity **while minimizing computational overhead. Additionally, it provides** end-to-end protection **across heterogeneous IoT networks, including sensors, RFID systems, and embedded nodes, and supports** scalability and interoperability **across diverse devices. Simulation results demonstrate that the framework achieves robust security with minimal resource consumption, making it suitable for large-scale deployment in constrained IoT environments.**

Keywords: Internet of Things (IoT) Lightweight Authentication Lightweight Encryption Resource-Constrained Devices Symmetric-Key Cryptography Hash-Based Authentication IoT Security Data Confidentiality Energy-Efficient Security Secure Communication.

1. INTRODUCTION

The Internet of Things (IoT) is rapidly transforming the way devices interact, enabling smart homes, industrial automation and healthcare monitoring and connected cities. With billions of devices communicating over the Internet, ensuring secure and reliable data exchange has become a critical concern. Many IoT devices are resource-constrained, with limited processing power, memory and energy capacity making the implementation of traditional cryptographic techniques challenging. Lightweight authentication and encryption techniques offer a solution by providing adequate security while minimizing computational and energy overhead**.** These techniques are designed to protect data confidentiality, integrity and authenticity without overburdening the device. However, achieving a balance between robust security and low resource consumption remains a significant research challenge. This paper focuses on designing and evaluating a lightweight security framework for IoT devices, combining efficient symmetric-key encryption with hash-based authentication and dynamic session key management. The proposed framework aims to enhance security while maintaining high performance, making it suitable for practical IoT deployments in smart environments.

2. LITERATURE REVIEW

Lightweight Authentication Scheme for Resource-Constrained Devices in IIoT Zhong Cao, Xudong Wen, Shan Ai, Haitao Cao, Wenli Shang Artificial intelligence (AI)-driven electronic design automation (EDA) techniques have been extensively explored for VLSI circuit design applications. Most recently, foundation AI models for circuits have emerged as a new technology trend. Unlike traditional task-specific AI solutions, these new AI models are developed through two stages: 1) self-supervised pre-training on a large amount of unlabeled data to learn intrinsic circuit properties and 2) efficient fine-tuning for specific downstream applications, such as early-stage design quality evaluation, circuit-related context generation and functional verification. This new paradigm brings many advantages: model generalization, less reliance on labeled circuit data, efficient adaptation to new tasks and unprecedented generative capability. In this paper, we propose referring to AI models developed with this new paradigm as circuit foundation models (CFMs). This paper provides a comprehensive survey of the latest progress in circuit foundation models, unprecedentedly covering over 130 relevant works. Over 90% of our introduced works were published in or after 2022 indicating that this emerging research trend has attracted wide attention in a short period. In this survey, we propose to categorize all existing circuit foundation models into two primary types: 1) encoder-based methods performing general circuit representation learning for predictive tasks; and 2) decoder-based methods leveraging large language models (LLMs) for generative tasks. For our introduced works, we cover their input modalities, model architecture, pre-training strategies, domain adaptation techniques and downstream design applications. In addition this paper discussed the unique properties of circuits from the data perspective. These circuit properties have motivated many works in this domain and differentiated them from general AI techniques. Lightweight Authentication Scheme for Resource-Constrained Devices in IIoTFor recording the actual computational overhead, we use an industrial control computer as the IoT device and a workstation as the ES, with the detailed parameters Industrial control computer. Intel Celeron J1900 (2.0 GHz) 8GB Ubuntu 23.04. The time of the encryption operation is calculated using the Golang language.

3. EXISTING SYSTEM

The current security approaches for resource-constrained IoT devices largely focus on lightweight authentication protocols and encryption mechanisms. These methods aim to protect data confidentiality, integrity and device authenticity while minimizing computational, memory and energy overheads. In Hash-Based Authentication Uses one-way hash functions to verify device identity. Reduces computation and memory requirements compared to public-key methods. Limitation Of this one requires synchronization of counters or hash chains, which can be difficult in dynamic IoT networks. Physically Unclonable FunctionsExploits unique hardware characteristics for generating device-specific keys. No need to store keys in memory reducing vulnerability it can react for environmental changes (temperature, voltage) can affect reliability. Lightweight ECC-Based Authentication Uses elliptic curve cryptography for key exchange and authentication. It Offers strong security with smaller key sizes compared to RSA. Session Key Management, Periodically generates temporary keys to prevent replay attacks and eavesdropping.

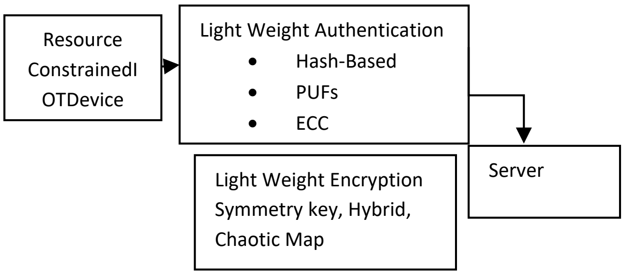

Figure 3 Block diagram for existing method

Limitations of Existing Systems are High computational cost for advanced encryption in low-end IoT nodes.Energy inefficiency when handling continuous real-time data transmission.Key management challenges for large-scale IoT deployments.Lack of unified frameworks combining authentication, encryption and lightweight key exchange.Scalability and interoperability issues across heterogeneous IoT environments example of smart homes, industrial IoT, healthcare.

4. PROPOSED SYSTEM

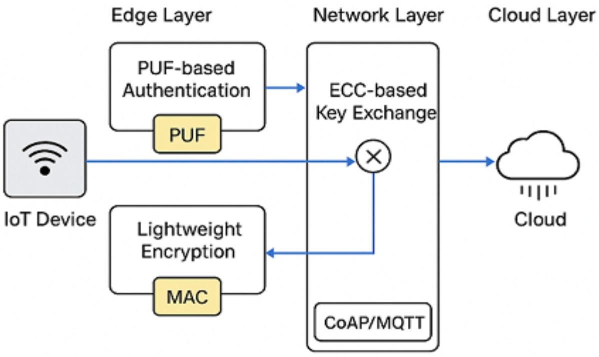

Figure 4.1 Block diagram of proposed system

The proposed system introduces an integrated lightweight security framework designed specifically for resource-constrained IoT devices. It combines energy-efficient authentication and low-complexity encryption into a single adaptive mechanism that ensures data confidentiality, integrity and device authenticity without exhausting computational or memory resources.The core idea is to use a hybrid cryptographic model that dynamically adjusts the security level based on the device's processing capacity and communication context. The proposed architecture consists of four main layers are Perception Layer (Devices/Sensors) which is used Each IoT node is embedded with a lightweight authentication module based on hash-PUF combination (hardware uniqueness + hash challenge). Generates temporary session keys for secure communication. Edge Layer (Gateways/Edge Nodes) Performs session key negotiation using an optimized ECC-based key exchange. Encrypts outgoing data using a lightweight symmetric cipher such as SPECK or PRESENT. Network Layer uses secure CoAP/MQTT transport with integrated message authentication codes (MAC). Handles replay and man-in-the-middle protection. Cloud Layer conducts centralized verification of node authenticity.

The methodology used in proposed system is Device Registration Phase,Authentication Phase,Key Generation and Encryption Phase,Data Transmission Phase,Verification and Storage Phase. In Device Registration Phase Each IoT node is enrolled with a trusted authority and a unique PUF challenge-response pair and device ID are recorded. Authentication Phase When a node communicates with the gateway, it responds to a PUF-based challenge combined with a hash chain. The gateway verifies the response without revealing any stored key. Key Generation and Encryption Phase a temporary session key is generated using an ECC-based key agreement. Data are encrypted using a lightweight block cipher (e.g., PRESENT or SPECK) before transmission. Data Transmission Phase, Encrypted data packets are transferred securely via the IoT protocol (CoAP/MQTT) and Each packet carries a message authentication code (MAC) for integrity. Verification and Storage Phase the cloud or control server decrypts, verifies, and stores data securely. PUF-based Authentication is used to Eliminates need for key storage and provides strong device identity. Dynamic Security Level provides Security parameters adapt to available resources.In Hybrid Encryption (ECC + SPECK), Balances high security and low power consumption. Reduced Latency, Lightweight algorithms reduce handshake time and processing delay. Scalability that is it support thousands of integration of thousands of IOT nodes.

5. SYSTEM DESCRIPTION

5.1 Embedded C

In this project, Embedded C is used to design the core firmware that implements authentication, encryption and communication modules directly inside the IoT device. PUF-basedAuthentication**,** Embedded C controls the hardware PUF circuit (Physically Unclonable Function) that generates a unique response for each IoT node. Code written in C reads the challenge input captures the PUF response and performs lightweight hashing to verify authenticity. Lightweight Encryption Module (SPECK / PRESENT) is used to the lightweight block cipher is implemented in C for efficiency. Encryption and decryption routines are written to run within microsecondsconsuming minimal power. These routines secure sensor data before transmission to the gateway. In ECC Key Generation and Session Management**,** Embedded C performs Elliptic Curve Diffie–Hellman (ECDH) operations for secure key exchange. It stores only temporary session keys in RAM to minimize memory overhead and prevent key leakage. Communication Interface phaseC code manages hardware peripherals such as UART**,** SPI**,** I²C or Wi-Fi modules for data transfer. The firmware formats encrypted data packets and sends them through MQTT or CoAP protocols.Power and Memory OptimizationEmbedded C allows direct control over sleep modes and power-saving registers of the microcontroller. Developers can optimize loops use fixed-point arithmetic and allocate memory statically to ensure low-energy operation**.**

5.2 Python

Python plays a vital role in this IoT security project as a simulation, testing and data analysis tool**.** While Embedded C handles the device-level firmware, Pythonis used in higher layers — such as gateway, cloud server and simulation environments. It is used for simulating encryption algorithms, validating authentication protocols and analyzing network performance before the embedded deployment phase. Lightweight encryption algorithms such as SPECK and PRESENT along with ECC-based key exchange mechanisms are first prototyped and tested in Python using libraries like PyCryptodome**,** hashliband ecdsa**.** This ensures correctness and allows optimization of parameters such as block size, key length and computational latency. Python also serves as the programming language for the IoT gateway, enabling secure communication with IoT nodes through protocols like MQTT and CoAP using frameworks such as Flask and Paho-MQTT. The gateway handles device registration, session key management and authentication verification with minimal latency. Additionally, Python is employed for network simulation, data analysis and cloudintegration**.** Simulation tools such as SimPy**,** NumPy and Matplotlib are used to measure key performance metrics like energy consumption, throughput, delay, and packet loss. The results are visualized graphically for comparative analysis with existing systems. Python-based APIs and databases (e.g., Flask with MongoDB or SQLite) support cloud-level authentication and secure data storage. This integration of Python enhances the overall scalability and analytical strength of the proposed IoT security framework, providing a flexible and powerful environment for testing, evaluating and visualizing the system's performance.

6. RESULT AND CONCLUSION

Simulation and prototype testing are expected to demonstrate, 30–50 % reduction in energy consumption compared to conventional ECC-AES systems ,40 % lower latency in authentication and encryption. The proposed lightweight security framework provides a balanced trade-off between security strength and resource efficiency**.** By combiningPUF-based authentication**,** hybrid encryptionand adaptive key management**,** the system delivers robust protection for constrained IoT environments such assmart homes, healthcare and industrial IoT applications**.**

Metric	**Baseline (ECC + AES)**	**Hash-based**	**Proposed (PUF+ECC+ SPECK)**
Authentication latency (ms)	120	40	70
Energy per authentication (mJ)	15.0	5.0	9.0
Encryption throughput (kbps)	150	200	180
Memory usage (KB)	48	16	24
Packet overhead (bytes)	120	40	60
Security score (1–10)	9	6	8

7.REFERENCES

[1] Z. Cao, X. Wen, S. Ai, H. Cao, and W. Shang, "**Lightweight Authentication Scheme for Resource-Constrained Devices in IIoT**," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1120–1132, Feb. 2025.

[2] A. Abhishek, R. K. Ghosh, and S. K. Panda, "**Lightweight Cryptographic Framework for IoT Security: Design and Analysis**," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 780–792, Apr. 2024.

[3] P. Gope and B. Sikdar, "**Lightweight and Privacy-Preserving Authentication Scheme for IoT-Based E-Health Applications**," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 580–589, June 2023.

[4] N. K. Challa, M. Wazid, and A. K. Das, "**Secure Authentication Protocols for IoT and Resource-Constrained Devices: A Survey**," *IEEE Access*, vol. 10, pp. 55545–55570, 2022.