International Journal of Advanced Culture Technology Vol.11 No.1 343-348 (2023)
DOI https://doi.org/10.17703/IJACT.2023.11.1.343

IJACT 23-3-41

A Research on IoT Security Technology based on Blockchain and Lightweight Cryptographic Algorithms

[1]Sun-Jib Kim

[1]Prof., Dept. of IT, Hansei Univ., Korea
kimsj@hansei.ac.kr

Abstract

As the IoT market continues to grow, security threats to IoT devices with limited resources are also increasing. However, the application of security technology to the existing system to IoT devices with limited resources is impossible due to the inherent characteristics of IoT devices. Various methods for solving related problems have been studied in existing studies to solve this problem. Therefore, this study analyzes the characteristics of domestic IoT authentication standards and existing research to propose an algorithm that applies blockchain-based authentication and lightweight encryption algorithms to IoT equipment with limited resources.

In this study, a key generation method was applied using a Lamport hash-chain and data integrity between IoT devices were provided using a Merkle Tree, and an LEA encryption algorithm was applied using confidentiality in data communication. In the experiment, it was verified that the efficiency is high when the LEA encryption algorithm, which is a lightweight encryption algorithm, is applied to IoT devices with limited resources.

Keywords: *Blockchain, Merkle Tree, IoT, Lightweight Cryptographic Algorithms, Authentication Scheme*

1. INTRODUCTION

The Internet of Things(IoT) represents a new technology in which a large number of devices connect and communicate with each other, producing various services that improve our quality of life and are used in our daily life. The number of IoT devices such as sensors, smart devices, and applications is growing exponentially, and according to Statista, the number of Internet-connected IoT devices is expected to grow significantly to about 75 billion by 2025 [1].

As the IoT market continues to grow, it is expected that cyber security attacks against IoT devices and services will also increase. May cause damage to life, property, etc. Furthermore, due to the characteristic that various devices are connected via a network, it can easily affect other devices [2].

In such systems, security should be an inherent consideration, requiring well-designed security solutions to protect resources from unauthorized access [1]. Additionally, most IoT devices are powered by low-performance hardware and rely on centralized architectures connected to cloud servers through gateways. This centralized architecture suffers from a single point of failure, making it difficult to ensure the integrity of identity management and collected data for a large number of devices.

Manuscript received: January 30, 2023 / revised: March 4, 2023 / accepted: March 15, 2023
Corresponding Author: kimsj@hansei.ac.kr
Tel:+82-31-450-9884, Fax: +82-31-450-5172
Professor, Dept. of IT. Hansei Univ., Korea

Therefore, in this research, we solve the single point of failure problem of IoT systems that rely on the existing centralized architecture, the identity management problem of IoT devices, and ensure the integrity of collected data and the confidentiality of data delivery. try to improve security.

The composition of this paper is as follows. Section 2 presents an analysis of blockchains and cryptography algorithms that have been researched in the past. Section 3 present the logic for IoT security technology research based on blockchains and lightweight cryptographic algorithms presented in this research, and Section 4 presents performance results and conclusions.

2. PRIOR RESEARCH

2.1 IoT Security Certification

Currently, the Korea Internet & Security Agency(KISA) operates an IoT security certification system in Korea, and there is a STANDARD grade that applies 23 core measures required to improve vulnerabilities reported as hacking cases. There is a BASIC grade to which 41 items of comprehensive security measure items of the internationally required level are applied. There is a LITE grade that applies 10 minimum security measures to maintain product security. They are divided into these three inspection classes, and inspections are carried out according to five types of inspection criteria [3].

Table 1 shows a comparison between the three grades according to the type of IoT device. In general, for smaller sensor-layer devices configured with lower-performance hardware, the LITE grade is applied, which consists of minimal action items to maintain security.

Table 1. Feature of Standard, Basic, Lite Level

Rating	Contents	Apply
Standard	√ Comprehensive security measures items at the level of international requirements	√ Suitable for medium to large-sized smart home appliances
Basic	√ Key measures required to improve the reported vulnerabilities of hacking cases, etc. √ Certification: Users, products √ Application of encryption algorithm when storing important information, √ Data in transit protection	√ Suitable for small and medium-sized products low-specification OS
Lite	√ Minimum action items to maintain product security √ Certification: Users, products √ Application of encryption algorithm when storing important information, √ Data in transit protection	√ Suitable for small firmware-based products such as sensors

2.2 IoT Device Authentication Techniques

2.2.1 Blockchain-based IoT Device Authentication Scheme

In the study claimed by Park et al., each sensor device generates a Merkle Tree value using a public key and a group key, which are Lamport hash-chain assigned from the top aggregator. The top-level Aggregator has proposed a method to authenticate each sensor device by verifying the Merkle Tree values generated by each sensor device and storing them in the blockchain [4].

However, in this research, there is no mutual authentication procedure when sending the Merkle Tree values from each sensor device to the Aggregator, which can be subject to man-in-the-middle attacks [5].

In addition, there is no discussion about the procedure for generating blocks in the top-level Aggregator, and if the block generation entity is only the top-level Aggregator, there will be a single point of failure problem despite the use of blockchain technology.

2.2.2 Blockchain-based Lightweight Mutual Authentication Protocol for IoT System

In Choi et al.'s research, mutual authentication is performed using random numbers in sensor devices, the IDs of sensor devices are grouped in the cluster head, and authenticated by comparing with the sensor device IDs stored in the blockchain on the gateway. proposed a blockchain-based authentication technology for low-performance sensor devices. It complements the shortcomings of Park et al.'s work by performing mutual authentication through lightweight computation between sensor nodes, cluster heads, and gateways, but there is no discussion of how to configure the blockchain used by the gateways.

2.2.3 P2P Networking-based IoT Sensor Node Authentication by Blockchain

In this study, we give each IoT sensor node a sequence number according to its distance from the sink node, and use it as a means of verifying and authenticating each node. Since the sink node keeps the sequence number of all nodes, it can check the level of each node and the physical distance from itself, and various by verifying the message in stages, the IoT sensor node is authenticated only by hash calculation. However, this research also focuses only on the IoT sensor node authentication protocol and does not discuss how to configure the blockchain [6].

2.3 Encryption Algorithm

AES is a widely used block encryption algorithm standardized by NIST in the United States, and supports the use of key lengths of 128, 192, and 256 bits based on 128-bit block size. It supports encryption and decryption through 8-bit unit operation within the round function [7].

LEA was proposed by Hong et al., and Feistel structure is applied. There is no theoretical vulnerability due to key scheduling characteristics, and 128, 192, and 256-bit key lengths are supported based on the 128-bit block size. LEA adopts the ARX (Addition Rotation XOR) structure, and the round function of LEA consists only of ARX operations in units of 32 bits. These LEAs are used as block encryption algorithms to provide confidentiality in lightweight environments such as IoT and cloud. It is designed to provide sufficient performance and security while efficiently using computational resources in consideration of IoT devices with lightweight and low-power characteristics [8-9].

RSA is a public key-based representative encryption algorithm that encrypts and decrypts with a pair of public and private keys. It was developed by Ron Rivest, Adi Shamir, and Leonard Adleman. It is a fact-based, encryption/decryption method that enables digital signatures [10].

ECC is a public key cryptosystem proposed by Victor Miller and Neil Koblitz. Even if you know two random points P and Q on an elliptic curve, it is difficult to find a random integer k used as a secret key. was designed with safety in mind. Compared to other encryption algorithms, this has the advantage of providing equal security even with a short key length. To implement the ECC encryption system, it must be composed of a key distribution algorithm and a message encryption algorithm. Accordingly, the public key combined with the random number is shared with each terminal to synchronize and encrypt with a secret key that an attacker cannot infer. Accordingly, the key distribution representative method is the Elliptic Curve Diffie-Hellman (ECDH) algorithm. In the message encryption method, the sender and the receiver proceed with the calculation of the secret key [11].

3. PROPOSED IoT SECURITY TECHNOLOGY

The blockchain and lightweight cryptographic algorithm-based IoT security technology proposed in this research constitutes a mutual trust infrastructure process between users, IoT devices, and service management servers using Lamport hash-chain for the authentication of users and IoT devices, and using the Merkle Tree for the integrity. Provides confidentiality to IoT services by applying a data-lightening cryptographic algorithm in data transfer, aiming to meet the IoT security testing and certification standards of the KISA.

Figure 1 is a Merkle Tree-based IoT device authentication scheme applied in this research by taking the idea from B.J. Park's paper.

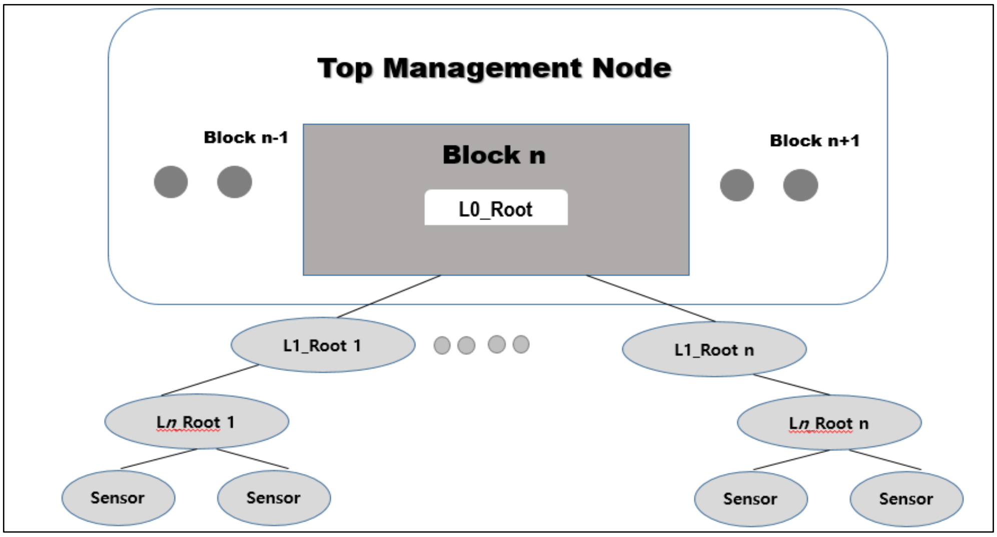

Figure 1. Merkle Tree-based IoT device authentication scheme

Figure 2 is a schematic configuration diagram of the service proposed in this research. In general, a user who owns a wireless device uses the IoT device via a network, and a management server provides database and web-based services. Figure 1 shows the association of components in a proposed network using a Merkle Tree. In the proposed network configuration, the server becomes Root, and the user's device and IoT device act as aggregators.

In the case of the proposed service, there is a central management server that manages services for IoT devices, and an environment is provided in which general users can easily and safely use devices with IoT devices installed through mobile devices.

Basically, it uses trust-based authentication between users, IoT devices, and management servers to generate random keys through the Lamport hash-chain to respond to device authentication and retransmission attacks. Merkle Tree was used to ensure the integrity of the data. The lightweight encryption algorithm LEA was applied to secure the encryption of data transmission.

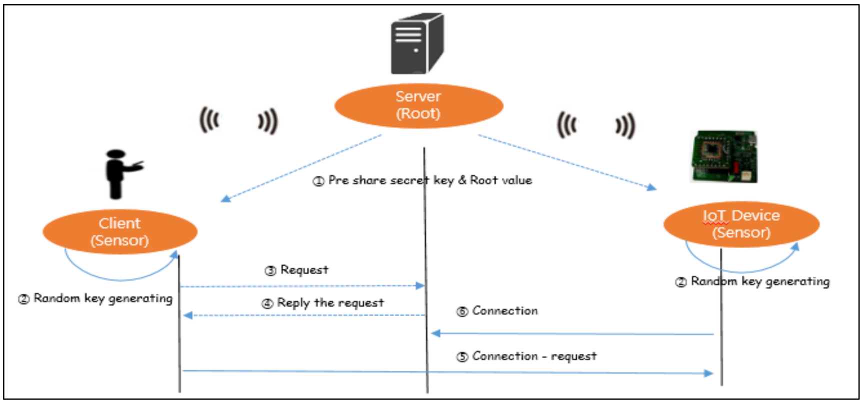

Figure 2. Service structure

The process of implementing service encryption functionality is as follows:
Step 1: Divide the secret key and *Root* hash value in advance based on trust.
Step 2: Use Lamport hash-chain to generate random key values.
Step 3: The client requests the request, a random key, and a hash value of the *Root* value, which is encrypted and transmitted using LEA algorithm.
Step 4: Approve data requests through data integrity and authentication at each stage.

4. RESULTS

The secret key proposed in this research is designed according to the LEA 128-bit encryption method, and can also generate 192 and 256-bit secret keys to enhance the encryption strength, and participate in communication for encryption and decryption. We used the Merkle Tree for device trust relationships.

To compare the performance of the method proposed in this study, the average value of the time performed 30 times on the target item was derived from the ESP 8266 with a CPU performance of Tensilica L106 32bit running at 80Mhz or160MHz. *K-g-t* means the average time to generate a key, *enc-t* is the average encryption time, *dec-t* is the average decryption time, and *ct* is the one-way communication time. As a result, it is necessary to encrypt specific data and send it to the management server for communication or authentication of a specific service, and to receive the response value again. It is expected to take at least twice as much as this measured value.

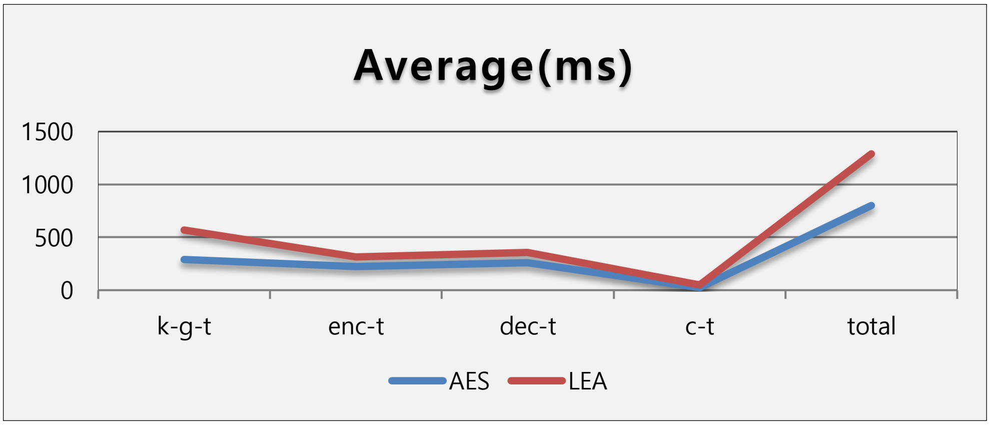

Figure 3. Compare average times for AES & LEA performances(*ms*)

As shown in Figure 3, the conventional method takes about 2.3 times longer to encrypt and 2.7 times longer to decrypt than the method presented in this paper. By limiting and measuring only one IoT device, there was almost no difference between the conventional random method and the method presented in this research, but a reduction effect of about 4% was confirmed. It was confirmed that the time could be shortened by about 40%. It also solves the resource limitation problem of IoT devices by not applying encryption algorithms for private key generation to IoT devices.

5. CONCLUSION

We used LEA for encryption algorithms to meet the IoT security test certification standards of KISA for IoT devices with resource suggestions, and the Lamport hash-chain was used for generating random keys. We also used the Merkle Tree for data integrity between IoT. As a result of the experiment, it was confirmed that the application of LEA on certain IoT devices increased by more than 40%. This means that IoT devices with limited resources can secure confidentiality such as authentication and data encryption

REFERENCES

[1] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security Requirements for the Internet of Things: A Systematic Approach," *Sensors-20-05897*, 2020.

[2] Korea Internet & Security Agency, "IoT Common Security Guide for Security Internalization of ICT Convergence Products and Services," *Jinhan M&B*, 2016.

[3] S. K. Ji, "IoT Security Certification Inspection Standards and Trends in Domestic Certification," *TTA Journal 186*, Special Report, 2019.

[4] B. J. Park, T. J. Lee, and J. Kwak, "Blockchain-Based IoT Device Authentication Scheme," *Journal of The Korea Institute of Information Security & Cryptology,* Vol. 27, No. 2, pp. 343-351, 2017.

[5] W. S. Choi and S. S. Kim, "Blockchain-based IoT Authentication techniques for DDoS Attacks," *Journal of the Korea Society of Computer and information,* Vol. 24, Issue. 7, pp. 87-91, 2019.

[6] S. H. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," *Springer,* Peer-to-Peer Networking and Applications 13, pp. 579-589, 2019.

[7] J. Daemen and V. Rjjmen, "The design of Rijnde l: AES-the advanced encryption standard," *Springer*, 2013.

[8] D. Hong, J. Lee, D. Kim, D. Kwon, K. Ryu, and D. Lee, "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors," *ISA. LNCS,* Vol. 8267, pp. 3-27, 2013.

[9] J. M. Jeong, P. H. Kim, K. Y. Jung, E. J. Yoon, and K.Y. Yoo, "Key Management Method for LEA Lightweight Block Cipher," *Proceedings of Symposium of the Korean Institute of communications and Information Sciences,* pp. 959-960, 2017.

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining Digital Signatures and Public-Key Crypto-systems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[11] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[12] S. J. Kim, "A Study on the Security Management System for Preventing Technology Leakage of Small and Medium Enterprise in Digital New Deal Environment," *The International Journal of Advanced Culture Technology,* Vol. 9, No. 4, pp. 355-362, 2021.