A Study on KSI-based Authentication Management and Communication for Secure Smart Home Environments

Gyeong-Jin Ra[1] and Im-Yeong Lee[2]
[1]Department of Computer Science and Engineering, Soonchunhyang University
Asan, South Korea
[e-mail: rababi@sch.ac.kr]
[2]Department of Computer Software and Engineering, Soonchunhyang University
Asan, South Korea
[e-mail: imylee@sch.ac.kr]
*Corresponding author: Im-Yeong Lee

Received September 30, 2017; accepted December 28, 2017; published February 28, 2018

Abstract

In smart home environment, certificate based signature technology is being studied by communication with Internet of Things(IoT) device. However, block - chain technology has attracted much attention because of the problems such as single - point error and management overhead of the trust server. Among them, Keyless Signature Infrastructure(KSI) provides integrity by configuring user authentication and global timestamp of distributed server into block chain by using hash-based one-time key. In this paper, we provide confidentiality by applying group key and key management based on multi - solution chain. In addition, we propose a smart home environment that can reduce the storage space by using Extended Merkle Tree and secure and efficient KSI-based authentication and communication with enhanced security strength.

Keywords: Smart Home, Internet of Things, Keyless Signature Infrastructure, Block Chain, Extended Merkle Tree, XOR Tree

A preliminary version of this paper was presented at APIC-IST 2017, and was selected as an outstanding paper.
This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (2017-0-00156, The Development of a Secure Framework and Evaluation Method for Blockchain)

http://doi.org/10.3837/tiis.2018.02.021 **ISSN : 1976-7277**

1. Introduction

The smart home is a wired / wireless network that manages the internal devices of the house by communication between the internal IoT device, the user remote controller, and the external device. As shown in **Fig. 1**, IoT devices communicate with the external cloud server through the Internet or through the gateway, and communicate with other devices (such as the user's smartphone) to manage the inside of the house[1]. Therefore, it is essential for smart home messages to communicate securely from the attacker, and personal privacy is the most important item. In addition, low-performance IoT devices can not perform high-level computations, and therefore, it is necessary to find an appropriate relationship between security and efficiency. Therefore, the IoT message standard protocol is an X.509 certificate public key verification environment including Public Key Infrastructure(PKI), MQ Telemetry Transport or Message Queuing Tlemetry Transport(MQTT) using Accoutable Key Infrasturcture(AKI), Constrained Application Protocol(CoAP) and Transport Layer Security(TLS). The PKI's validation updates and manages the public key according to a certificate issued by a trusted third party based on a TTP (Trusted Third Party)[2-3]. However, the TTP has the overhead to handle as the user increases and the single point of failure when the TTP is taken or tampered by the attacker (**Fig. 1**). AKI is a public key verification environment of Acoountable Internet Protocol(AIP) which is a next generation self-authentication protocol, and it reduces the single point error by distributing the burden and responsibility to work on a single PKI to Integrity Log Server(ILS) and Log Validator[4]. However, it does not solve the problem of additional system building and fundamental single points of failure. Recently, the block chain, which is a core technology of bit coin, has attracted attention[5]. The block chain is decentralization and anonymity by the cooperation of the distributed network, so that all the participants can manage the open ledger and trust them. KSI is authenticated through a key generated by a hash chain rather than a key pair generated by PKI based mathematical difficulties[6]. It is also a signature that binds a message and a secret key to create a global timestamp by linking with the global coordinator time and committing it to a block chain to provide integrity. However, since KSI performs only hash operations, it is difficult to provide confidentiality. Therefore, in this paper, we provide confidentiality by encrypting with a group key based on a redundant hash chain and applying key management to protect important user privacy in a smart home. In addition, we propose a smart home environment that provides secure and efficient KSI-based authentication and communication by reducing tree creation and storage space by using Extended Merkle Tree[7].

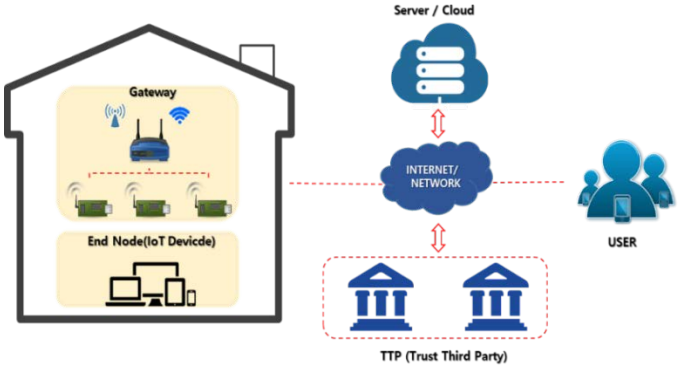

Fig. 1. IoT smart home configuration process and single point of failure threat

2. Related Work

2.1 Public Key Infrastructure (PKI)

PKI is a public key infrastructure, which means all the set of procedures such as procedures, use, storage, cancellation, etc. necessary for roles, policies, generation, management and distribution based on public keys[2]. In order to achieve the trust of the users registered in the general directory, it provides the validity in combination with the digital certificate. It provides the credibility by building the infrastructure through CA (Certificate Authority), RA (Registration Authority) and VA (Validation Authority). The digital certificate is also encrypted and managed by a third party to prove the validity of the public key. This gives the user the overall processing that takes place in the digital environment. The purpose of digital certificates is to facilitate the transfer of secure digital information of information about the scope of activities of the network such as e-commerce, Internet banking, and e-mail. The PKI consists of a certificate authority CA in the certificate issuance process that includes a list of trusted public keys, an RA that accepts requests for digital certificates, requests the CA to make a request, and a third party verification authority that verifies and verifies information in a chain. As such, the PKI has a structure for creating, distributing, using, storing, and revoking certificates that bind public key and ownership. Therefore, certificate status registration CRL (Certifitcate Revocation List) and OCSP (Online Certificate Status Protocol) And has a timestamp role with validity over time. Therefore, the use of the public key for authentication and communication between the IoT devices of the smart home is performed by judging the state management and validity of the certificate in order to verify the public key. Therefore, if the number of communication times increases or the number of IoT devices to be managed increases, the overhead to be handled by the TTP and the amount of computation of the device increase. Also, in case of a CA that depends on a single processing service, a single point of failure, a service error, may cause the failure of the IoT device and the failure of the entire smart home[5].

2.2 Accountable Key Infrastructure (AKI)

AKI is a public key verification environment of AIP which is a self - authentication protocol, and it is supplemented with PKI 's "Single point of failure". It consists of ILS and Valiadator other than the CA of the existing authentication scheme. ILS stores the certificate based on the hash tree and effectively manages the certificate and copes with data tampering quickly. Therefore, AKI guarantees the reliability of the certificate even if the threat of the secret key occurs through the distributed structure. In the smart home, the AKI-based authentication and communication design is performed with the home device and the user smartphone, and the ECDSA signature and the TLS are communicated [5]. However, additional ILS and validator construction are required, and TLS and additional systems are not fundamentally decentralized with hybrid structures.

2.3 Block Chain

In a smart home environment, convenience is also important in a limited environment, but privacy is also an important security concern. Therefore, a block-chain-based IoT smart home environment has been proposed to overcome the existing single-point failure and satisfy efficient computation and security[8]. The block chain technology is used to record the same information in a distributed form in the form of a signature, which is shared by all the participants. It provides security technologies such as non-repudiation and digital signature, It

has possible features. Block chaining has three main characteristics: decentralization, anonymity, and irreversibility. One of the noteworthy features is decentralization, which makes it difficult for any institution to take responsibility because all participants make up a book. Therefore, not only do you spread and collaborate overhead over a single central entity, but also reduce single point of failure. Anonymity is a PKI-based public key - a secret key signature that provides an address with a public key instead of an individual's personal identity, and provides proof of identity with a secret key. The last feature is that irreversibly, the transaction in which the participant has occurred is blocked by a certain consensus method, and then the block is added to all the books after the block is formed. The top root value of a hash tree, called the Merkle Tree, is irreversible depending on the nature of the hash, and the whole is changed even if 1 bit is different. Therefore, since it is impossible to forge data without falsifying all the hash values, the merge tree, and the book, there is a tremendous amount of calculation for counterfeiting, which is practically impossible.

2.4 Keyless Signature Infrastructure (KSI)

The global timestamp using KSI computes user authentication and message integrity separately from the signature scheme of PKI based public key structure. In other words, authentication is performed by issuing a certificate with a public key-secret key structure using the irreversibility of the hash chain, and the integrity of the message is generated by the KSI's distributed server using the global timestamp value [6]. It is connected in a block chain to provide strong transparency and accessibility within network services such as the Internet[9]. Therefore, the KSI - based signature system can reduce the computational complexity of IoT device and provide secure authentication and communication environment in smart home environment which is a constrained environment. However, since KSI only uses hash operations, it does not provide confidentiality among the encryption functions provided by the existing PKI. Therefore, in a smart home environment where personal privacy protection is important, it is necessary to construct a new environment that can satisfy confidentiality and various security issues.

2.5 Extended Merkle Tree (XMT)

Extended Merkle Tree is based on XOR Tree and implements the collision resistance by applying bit mask technique to the key. XOR Tree is a technique first appeared in Collison-Resistant Hashig: Towards Making UOWHF(Uninersal Onewayness Hash Function)s Practical in 1987[10]. It constructs a structure of K and a function for resistance to collision attack in a hash function of Mekle-damgard structure as Tree type, The target collision resistance (TCR) was satisfied. The hash function compresses the message without the original Key, and is designed to be robust against collision tolerance. However, for the classification and explanation of the hash function, the function composing the hash function is explained by the key value. The MD (Meklre Damgard) structure does not use a key for a function. It splits the initial message into blocks and compresses it by padding. Second, the Wide Pipe Construnction improved the security characteristics of Second Pre-image Attack and Heard Attack of MD structure. The message is padded by itself and compressed by repeating the input and output using two initial vector values a minute after block by block. We have improved the overall Coliision Resistance of the MD hash function. We then improved the security strength and efficiency of the hash function by halving the key size by Fast Wide Construction, which then uses the output as the next input value[11]. The previous MD Struction, Wide pipe Construction is a basic linear Hash, and Fast Wide Construction is an XOR Hash. XMT is classified as XOR Tree Hash, and XOR Tree Hash has the smallest key

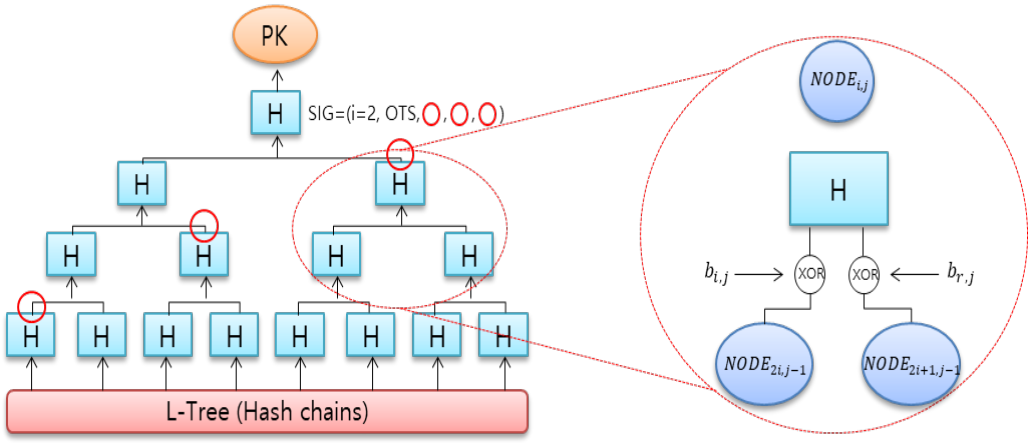

Fig. 2. Extended Merkle Signature and XOR Tree Configuration Method

size.Future research by Merkle Signature Scheme (MSS), Johannes Buchmann et al. It was applied to XMSS (Extended Merkle Signature Scheme). XMT is a method using general Merkle Tree and Bit Mask for high-speed implementation of hash based signature as shown in (**Fig. 2**). Bit mask scheme, which is half the size of the MSS (Mekle Signature Scheme) of the same strength[12]. This has the advantages of reduced signature key length and high speed implementation. He is a candidate for the Internet Engineering Task Force (IETF) final round in 2016. Therefore, XMT has advantages of computation speed and storage size because it can maintain security strength while halving the output of Tree that IoT-Device should generate in smart home environment.

2.6 Double Hash Chain

A double hash chain defends an attack that threatens the integrity of a single hash chain. A single hash chain has the risk of exposing all the values it creates in the future if the hash value is exposed. The dual hash chain arbitrarily selects *Seed* values x and y, and then generates two hash chains of length n using a one-way hash function. The confirmation value of the hash chain generated in the opposite direction. The safety of a system based on a hash function is due to the irreversibility of the hash function. By constructing a hash chain using this hash function and providing a double hash chain using two hash chains, it has higher security than a unidirectional hash chain. In this paper, we use the double hash chain to generate the session key as the confirmation value of the chain.

3. Security Requirements

The security requirements for KSI - based authentication management and communication for the secure smart home environment proposed in this study are as follows.

- **Signer certification**: Anyone can verify the signer of the signature.
- **No forgery**: Only legitimate signers should be able to generate signatures.
- **Reusable**: The signature of the data should not be used as a signature of other data.
- **Can not change**: The contents of the signed data must not be changed.

- **Non-repudiation**: The signer must not be able to deny the fact that he or she has signed it.
- **Data confidentiality**: Only authorized users should be able to access information assets.
- **Data Integrity**: Only authorized users should be able to change information assets.
- System Availability: Must be accessible by authorized users at the appropriate time.
- **Mutual Authentication**: Mutual authentication should be ensured through the smart home device key, and the session key must be agreed.
- In addition, since the hash functions used for authentication management and communication based on KSI have safety based on the hash strength to be used, the following security requirements are required.
- **Efficiency**: The calculation efficiency of the hash function should be good.
- **One-wayness**: Finding x with H (x) = h should be computationally infeasible.
- **Weak collision avoidance**: When x is given, it should be computationally impossible to find y (x) with H (x) = H (y).
- **Strong collision avoidance**: It is computationally impossible to find any (x, y) pair with H (x) = H (y).

Finally, the attacks that can occur in this research environment are as follows.

- **MITM (Man In The Middle) Attack**: On a protocol that does not validate the public key, the intermediary can manipulate the network communication to eavesdrop or manipulate the contents.
- **Replay Attack**: It is possible to impersonate a legitimate user by copying a valid message on a protocol that uses the same key repeatedly, and then retransmitting it later.

4. Proposal Scheme

A device that is difficult to communicate directly with KSI in the smart home communicates using a gateway repeater through signals such as Bluetooth Low Energy (BLE) WiFi. Users who use smart home service control and manage IOT devices in the home through communication with external gateway through a controller like smart phone.

In this paper, we propose a preprocessing process to generate a key for communication and a communication process with IoT Device in a smart home and User Controller through KSI. Proposed scheme 1 is user controll IoT device and smart phone with the gateway. The other proposed scheme 2 is communicatein IoT device and smart phone without the gateway.

4.1 System Parameters

The system coefficients of the proposed scheme are as follows. The participating objects are IoT Device, SmartPhone, Gateway, KSI Sever. These are identified by the unique number, and ID. There is an initial shared secret key for session key distribution and session key distribution between objects, and a secret key, a public key pair, a hash chain, and a hash tree for KSI-to-object communication are generated. Thereafter, there is a time stamp value generated by KSI, and all hash trees are bit masked through the stored XMT.

- ID_{Dev} : Device Serial Number
- $\mathrm{SM_{IMEI}}$: Smartphone IMEI Number
- ID_s : KSI Server identifier
- IV_k : Initial Shared symmetric Key
- Z_i: Device private key generated from SEED
- Z_0 : Last value generated by the private key and hash chain, public value
- r : The hash tree root value generated by the hash chain, the public value
- C_i: Authentication Path sibling node used to efficiently calculate the r value
- S_t: timestamp value of the message generated by the global hash tree
- t_0 : Device public value creation timestamp
- t_n : Message time value with authentication session key, $t_n = t_0 + \mathrm{i}$
- P_n : Device and gateway communication session key
- SK_i : Device and gateway communication session key $SK_i = Z_i \oplus \mathrm{P_{n-i}}$

4.2 Proposed Scheme 1

Proposed scheme 1 is the process of communication with KSI through IOT device which wants to communicate with external user SmartPhone as shown in **Fig. 3**.

4.2.1 Preliminary preparation

1) Key generation for communication with KSI

A device generates hashed values through random SEED and repeats the hashes in one

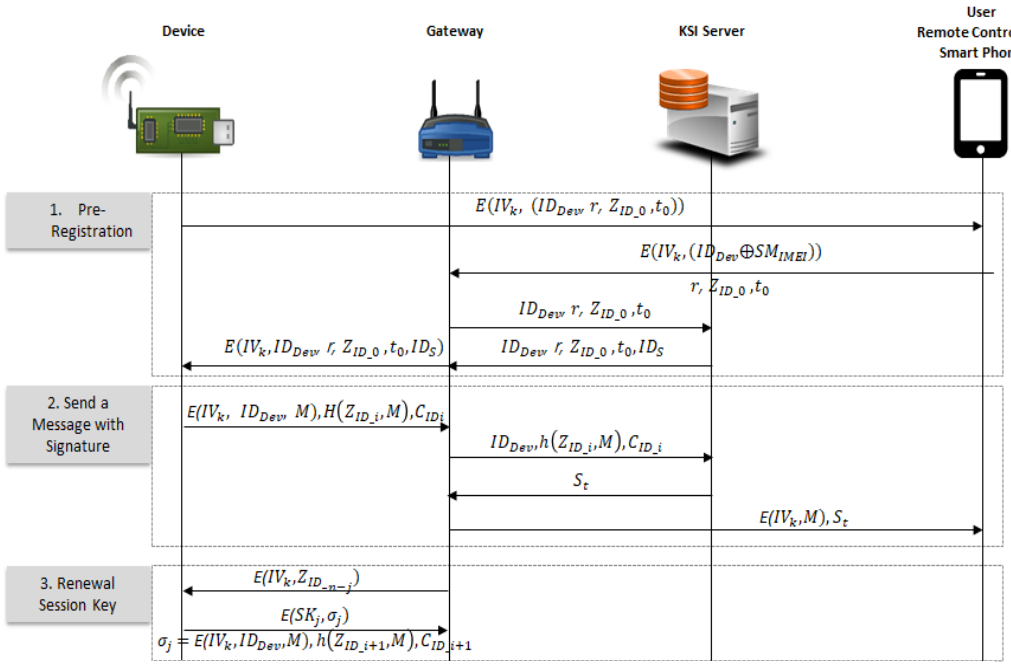

Fig.3. Overall flow chart of proposed scheme 1

direction. Then, we use the root value of the hash tree created by weaving the entire tree using the extended Merkle tree and finally generate the hash value as a public key.

$$Z_i = h(Z_{i+1})$$
$$Z_{i,j} = h((Z_{2i,j-1} \oplus b_{l,j}) || (Z_{2i+1,j-1} \oplus b_{r,j})) \quad (1)$$

2) Key generation for communication with Gateway

The device sends the private key through the Gateway to the KSI using the symmetric key previously shared with the gateway. The session key for communication then computes the session key of the next communication using a double-hash chain operation of a one-time private key used for the KSI authentication of a device and the one-time key of the gateway.

$$SK_i = Z_{i+1} \oplus P_{n-i} \quad (2)$$

4.2.2 Communication with Device-Gateway-Smartphone

1) Device Registration

Step 1. A device that wants to generate a new certificate sends $E(IVk, (ID_{Dev}, r, Z_0, t_0))$ to a smartphone.

Step 2. The SmartPhone decrypts the message received from the device and passes the value of $ID_{Dev} \oplus SM_{IMEI}$ and the value r, Z_0, t_0 to the gateway.

Step 3. The Gateway sends ID_{Dev}, r, Z_0, t_0 to KSI server.

Step 4. The KSI server sends the registered certificate to the Gateway with Server ID, ID_S.

Step 5. The Gateway sends the certificate information $ID_{Dev}, r, Z_0, t_0, ID_S$ to the Device.

2) Sending a message

Step 1. The device sends $E(IV_k, (ID_{Dev}, M))$, $h(Z_i, M), C_i$ to the Gateway, along with the message to be transmitted.

Step 2. The gateway decrypts the received content and transmits only the hash value of the message and the device certificate information to the KSI to obtain the unique global timestamp value of the message along with the authentication of the device.

Step 3. The Gateway forwards the message to the SmartPhone, including the message $E(IV_k, M)$, S_t encrypted with the initial symmetric key and the global timestamp value.

3) Renewal of the session key

Step 1. The Gateway sends $E(IV_k, P_{n-i})$ to the Device which encrypts the private key with its initial symmetric key in its hash chain and updates the session key.

Step 2. The Device calculates the session key using the information received from the Gateway and subsequently performs the communication.

$$\sigma_i = \mathrm{E}(IV_k, ID_{Dev}, M), h(Z_{i+1}, M), C_{i+1}) \quad (3)$$

4.3 Proposed Scheme 2

As shown in **Fig. 4**, the proposed scheme2 is a communication process between KSI and an IoT device that wants to communicate with an external user SmartPhone without gateway.

4.3.1 Preliminary preparation

1) Key generation for communication with KSI

A device generates hashed values through random SEED and repeats the hashes in one direction. Then, we use the root value of the hash tree created by weaving the entire tree using the extended Merkle tree and finally generate the hash value as a public key.

$$Z_i = h(Z_{i+1})$$
$$Z_{i,j} = h((Z_{2i,j-1} \oplus b_{l,j}) || (Z_{2i+1,j-1} \oplus b_{r,j})) \quad (4)$$

2) Key generation for communication with smartphone

The device sends the private key through the Gateway to the KSI using the symmetric key previously shared with the gateway. The session key for communication then computes the session key of the next communication using a double-hash chain operation of a one-time private key used for the KSI authentication of a device and the one-time key of the gateway.

$$SK_i = Z_{i+1} \oplus P_{n-i} \quad (5)$$

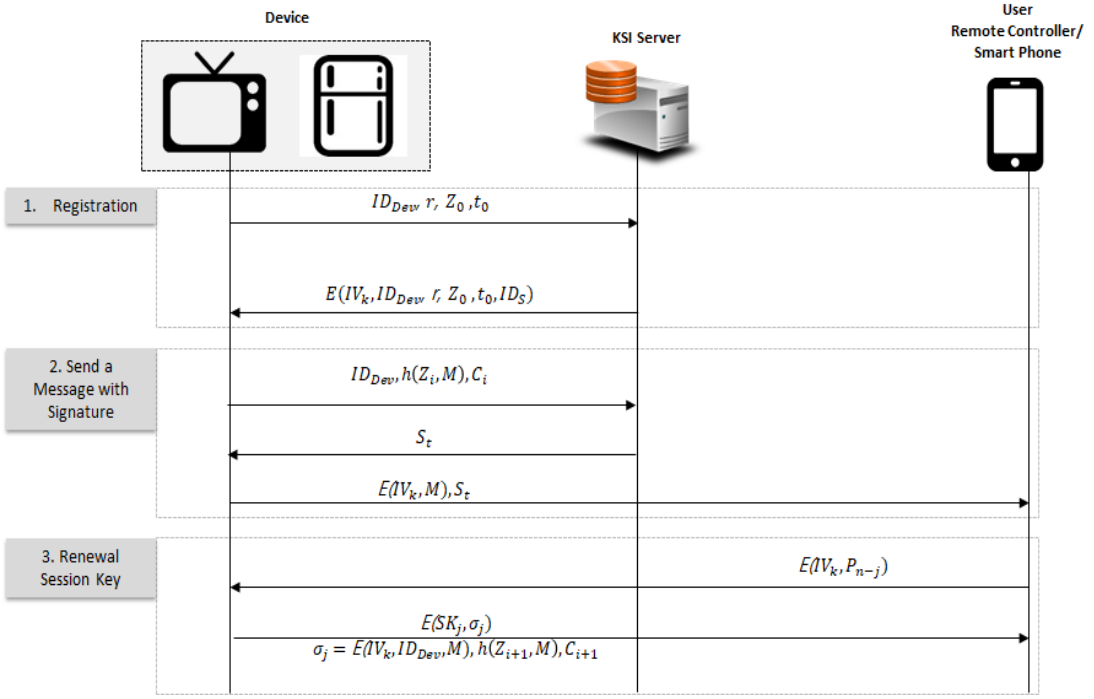

Fig. 4. Overall flow chart of proposed scheme 2

4.3.2 Communication with Device-Smartphone

1) Device Registration

Step 1. A device that wants to generate a new certificate sends $E(IVk\ ,(\ ID_{Dev}, r, Z_0, t_0))$ to a smartphone.

Step 2. The Smartphone decrypts the message received from the device and passes the value of $ID_{Dev} \oplus SM_{IMEI}$ and the value $r, Z_0\ , t_0$ to KSI server.

Step 3. The KSI server sends the registered certificate to the Gateway with Server ID ID_S. and sends the certificate information $ID_{Dev}, r, Z_0, t_0, ID_S$ to the Device.

2) Sending a message

Step 1. The device sends the device certificate information $E(IV_k, (ID_{Dev}, M))\ , h(Z_i, M), C_i$ to KSI server along with the message to be transmitted.

Step 2. The KSI creates the unique global timestamp value of the message along with the authentication of the device.

Step 3. The Gateway sends the message to the SmartPhone, including the message $E(IV_k, M)$, S_t encrypted with the initial symmetric key and the global timestamp value.

3) Renewal of the session key

Step 1. The Gateway sends $E(IV_k, P_{n-i})$ to the Device which encrypts the private key with its initial symmetric key in its hash chain and updates the session key.

Step 2. The Device calculates the session key using the information received from the Gateway and subsequently performs the communication.

$$\sigma_i = \mathrm{E}(IV_k, ID_{Dev}, M), h(Z_{i+1}, M), C_{i+1}^{E(SK_i, \sigma_i)} \tag{6}$$

5. Analysis

5.1 Safety analysis

The security of the proposed scheme is analyzed according to the security requirements in the smart home environment (**Table 1**).

- **Signer authentication**: The proposed scheme enables the signer authentication by verifying the signature with KSI whenever necessary, through the KSI signature information received from the sender.
- **No forgery**: Only users with legitimate information through a hash keychain can generate a signature.
- **Non-reusable**: The signature is signed with a single-use key and is not reusable because it checks the index i value of the global timestamp corresponding to the key and signature.

Table 1. Analysis of Proposed Scheme

	PKI	**AKI**	**KSI**	**Proposed Scheme 1**	**Proposed Scheme 2**
Process of achieve (Message Communication)	3E+3D+2H+ 2C	3E+3D+2H+ 1C	3E+3D+ 1H+2	3E+3D+1H+ 2⊕	1E+1D+1H+ 2⊕
Authentication Management	CA RA	Integrity Log Server Validator	Keyless Server Block chain		
MITM/ Replay Attack	Weak	Defense	Defense	Defense	Defense
Confidentiality	O	X	X	O	O
Quantum-Immune	X	X	O	O	O
Hash Tree Security Strength	-	$2^{\frac{k}{2}}$	$2^{\frac{k}{2}}$	2^{k}	2^{k}
k : Hash Ouput length, E : Encryption D: Decryption, C : ECDSA H :Hash Operation, ⊕: XOR Operation d : Tree Depth O : Offer X : Not Offer					

- **Unchangeable**: Once created, the signature is created at a unique time and is subsequently committed to the block chain.
- **Nonrepudiation**: The signer authenticates and signs the user through a hash keychain, which is the irrelevance of the hash, which is the only private key that is known only to the user.
- **Data confidentiality**: Only the authorized user through the session key in the smart home checks the message and provides confidentiality.
- **Data Integrity**: KSI's global timestamp allows integrity of the data because only authorized users can access the hash keychain.
- **System Availability**: As long as the Internet connection between the KSI server and the IoT device is established, authorized users are always available to provide system availability.
- **Mutual Authentication**: Mutual authentication is possible through session key between smart home devices, and session key can be agreed through multiple hash chains.
- **MITM / Reply Attack**: KSI defends MITM attack by issuing a hash tree-based certificate generated with a pair value based on user's public key and ID of devices. Also, the private key of the hash keychain defends the Reply Attack with a one-time key.
- **Quantum-Immune**: uses a hash key chain and a hash tree-based one-time key to immunize against the vulnerability of the public key-private key of the quantum computing based on existing mathematical difficulties.

- **Security Strength**: Extended Merkle Tree outputs a half of the XOR Tree bit masking, which is equal to the collision resistance of general Merkle Tree. Therefore, the collision resistance according to the same amount of power is doubled according to the birthday paradox hypothesis [12].

5.2 Analysis of efficiency

Analyze the efficiency of signing speed and the overall number of communications (see Figure 5). The proposed encryption algorithm uses SHA-2 and ECDSA (ECC256), and KSI and AES use 128bit. Compared with RSA 3072 X.509 against the same security strength, JAVA JCE based Eclipse Tool was used. The signature generation and communication times were the fastest and signing speed was slowest with X.509 based certificates.

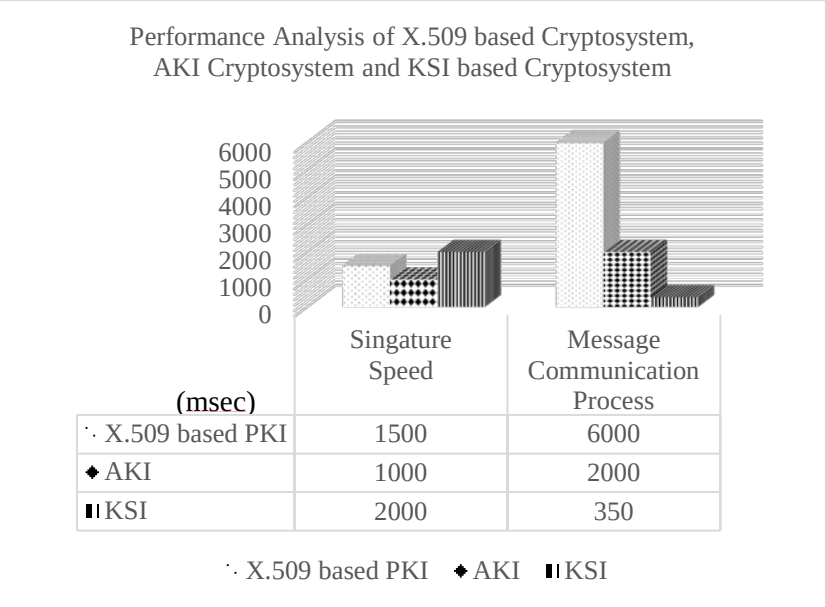

Fig. 5. Proposed sheme analysis graph

6. Conclusion

The smart home is a wired / wireless network that manages the internal devices of the house by communication between the internal IoT device, the user remote controller, and the external device. As shown in Figure 1, IoT devices communicate with other devices (smartphones of users) by transmitting messages to an external cloud server through the Internet or through a gateway, and provide convenience of smart home access through the Internet. However, it is essential that the message of the smart home is directly communicated to the privacy of the user and securely communicated from the attacker. In addition, in the case of low-performance IoT devices, high computation can not be performed, so it is very important to find an appropriate relationship between security and efficiency. Therefore, in this paper, we analyzed the research items applied in the existing smart home environment and analyzed the applicable technology. Therefore, we propose a secure smart home authentication and communication scheme based on KSI using XOR Tree of double hash chain and Extend Merkle Hash Tree. This satisfies the security requirements of digital signatures according to the proposed scheme

analysis, but also eliminates the structure of the existing PKI and AKI TTP based certificate system, and improves the safety and efficiency by defending the vulnerability.

References

[1] T.Mendes, R. Godina, E. Rodrigues, Matias. M, Catalão. J. C, &, J. P, "Smart home communication technologies and applications," *Wireless protocol assessment for home area network resources.* Energies, pp. 7279-7311, 2015. Article (CrossRef Link).

[2] M. Schukat, & P. Cortijo, "Public key infrastructures and digital certificates for the Internet of things," in *Proc. of Signals and Systems Conference (ISSC)*, pp. 1-5, 2015. Article (CrossRef Link).

[3] S. M. Kim, H. S. Choi, & W. S. Rhee, "IoT home gateway for auto-configuration and management of MQTT devices. In Wireless Sensors (ICWiSe)," in *Proc. of IEEE Conference on*, pp. 12-17, 2015. Article (CrossRef Link).

[4] Zhang, X., Hsiao, H. C., Hasker, G., Chan, H., Perrig, A., & Andersen, D. G., "SCION: Scalability, control, and isolation on next-generation networks," in *Proc. of Security and Privacy (SP), IEEE Symposium on*, pp. 212-227, 2011. Article (CrossRef Link).

[5] B.W. Jin, J.O. Park and M.S. Jeon, "A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment," *Journal of IIBC*, Vol.16, No.6, pp.25-31, 2016. Article (CrossRef Link).

[6] A.Buldas, A.Kroonmaa, & R.Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Proc. of Nordic Conference on Secure IT Systems*, pp. 313-320, 2013. Article (CrossRef Link).

[7] G.J. Ra, Y.H. Park, & I.Y. Lee, "A Study on Secure Home System using KSI," in *Proc. of Asia Pacific International Conference on Information Science and Technology*, 2017.

[8] A.Dorri, S. Kanhere, R.Jurdak, & P.Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. of Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on IEEE*, pp. 618-623, 2017. Article (CrossRef Link).

[9] C. Jämthagen, and M. Hell, "Blockchain-based publishing layer for the Keyless Signing Infrastructure," in *Proc. of 13th IEEE International Conference on Advanced and Trusted Computing*, IEEE--Institute of Electrical and Electronics Engineers Inc, 2016. Article (CrossRef Link).

[10] M. Bellare, & P. Rogaway, "Collision-resistant hashing: Towards making UOWHFs practical," in *Proc. of Advances in Cryptology-CRYPTO'97: 17th Annual International Cryptology Conference, Santa Barbara, California, USA*, August 1997. Proceedings, pp. 470, 1997. Article (CrossRef Link).

[11] E.Dahmen, K.Okeya, T.Takagi, & C. Vuillaume, "Digital Signatures Out of Second-Preimage Resistant Hash Functions," *PQCrypto5299*, pp. 109-123, 2008. Article (CrossRef Link).

[12] J. Buchmann, E. Dahmen and A. Hulsing, "XMSS-a practical forward secure signature scheme based on minimal security assumptions," in *Proc. of Post-Quantum Cryptography: 4th International Workshop*, pp. 117-129, 2011. Article (CrossRef Link).

Gyeong-Jin Ra received the B.S.degrees in Depart of Computer Software Engineering from Soonchunhyang University, Korea, in 2011 and 2013, respectively. He is now a M.S. candidate in Department of Computer Science and Engineering from Soonchunhyang University, Korea. His research interests include Block Chain Security, Cryptography, Keyless Digital Signature, etc.

Im-Yeong Lee is corresponding author. He received the B.S. degrees in Department of Electronic Engineering from Hongik University, Korea, in 1981 and the M.S. and Ph.D. degrees in Department of Communication Engineering from Osaka University, Japan, in 1986 and 1989, respectively. From 1989 to 1994, he had been a senior researcher at ETRI (Electronics and Telecommunications Research Institute), Korea. Now he is a professor in Department of Computer Software Engineering from Soonchunhyang University, Korea. His research interests include Cryptography, Information theory, Computer & Network security.