sustainability

MDPI

Article

A Study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment

Namsu Hong, Mansik Kim, Moon-Seog Jun and Jungho Kang *

Department of Computer Science & Engineering, Soongsil University, Seoul 07027, Korea; sucream@ssu.ac.kr (N.H.); mansik@ssu.ac.kr (M.K.); mjun@ssu.ac.kr (M.-S.J.)

* Correspondence: kjh7548@naver.com; Tel.: +82-2-826-6526

Received: 28 March 2017; Accepted: 20 June 2017; Published: 23 June 2017

Abstract: The development of information and communication technology (ICT) has opened the era of the Internet of Things (IoT), in which many devices can connect to the Internet to communicate. Recently, various technologies, such as smart grids, connected cars, and smart farms, have emerged based on IoT, and there is also the smart home, which is the fastest growing market. The smart home is where devices installed for various purposes connect to each other through the Internet so that users can use the service anytime and anywhere. However, while the smart home provides convenience to users, recently the smart home has been exposed to various security threats, such as vulnerability of session/cookies and the use of vulnerable OAuth. In addition, attacks on smart homes by hackers using these vulnerabilities are also increasing. Therefore, in this paper, we propose a user authentication method using the JSON Web Token (JWT) and International Mobile Equipment Identity (IMEI) in the smart home, and solved the problem of unauthorized smart home device registration of hackers by the application of IMEI and JWT technology.

Keywords: IoT; smart home; user authentication; smart home device; security

1. Introduction

The development of the Internet has developed communication between people and things, and recently, the Internet of Things (IoT), which provides convenience to people by enabling communication between various devices, has emerged. Recently, the IoT has been developed due to the development of various smart devices, among which the smart home market is rapidly becoming active. The smart home product market is expected to grow to $130 billion by 2020, and the market value of smart home manufacturing and application makers will account for about $60 billion, according to a statistical research agency, Strategy Analytics. Statista estimates that the US smart home market will increase by 21.05% annually from 2016 to 2020, 5.82% of the US population is using smart home products, and by 2020 approximately 18% of Americans are expected to use smart home products. Recently, users often use smart home products not only in the home, but also outside. Icontrol networks, a company that develops and sells smart home items, conducted a survey of 3000 US and Canadian consumers in 2014 and 2015, and in response to the question, "Why purchase smart home technology?" 90% of smart device buyers cited home security as a reason to avoid accidents that could happen in the home due to theft or carelessness, and 70% said it was for cost saving, including remote control of heating and commissioning of gas valves during commuting. In addition, a survey of consumer preferences for smart devices reported statistics that smart home access from remote locations frequently occurs due to home security and savings, such as 72% for automatic thermostats, 71% for remote front door locks, 65% for indoor surveillance cameras, 65% for outdoor remote control, and 65% for outdoor lighting automatic remote control. In a smart home environment, there are

various smart home devices, such as smart devices and sensors, and each provides a service for the convenience of the user [1]. The user goes through the process of registering the smart home device before using the smart home service. Since registered users can access the smart home via a remote device both inside and outside the smart home, in order to use smart home services securely, user authentication processes, such as session/cookie techniques or OAuth, is performed. However, these techniques are increasingly vulnerable to session hijacking attacks, and the exploitation of user information due to the detection of application programming interface (API) vulnerabilities is increasing [2–4]. Additionally, when registering a new device in a smart home, anyone can easily register it, so a smart home device not authorized by the user can be registered in the smart home by a hacker. Therefore, in this paper, we propose a scheme to authenticate users by using the JWT and IMEI of remote devices, and a scheme where only authorized users can register new smart home devices in a smart home. For the composition of this paper, Section 2 discusses user authentication techniques used in smart homes, smart home security requirements, and existing research; Section 3 describes a user authentication protocol using JWT and IMEI, a new smart home device registration protocol, and an API request and response protocol between the user and smart home device using JWT; in Chapter 4, we implement the proposed protocol; Chapter 5 explains the security and performance evaluation of the proposed protocol; Chapter 6 discusses the important points of this paper; and finally, Chapter 7 provides a conclusion.

2. Related Works

2.1. Smart Home

According to the Korea Association Smart Home (KASH), a smart home is a human-centered smart living environment that enables the convenience of the people, promotion of welfare, and safe living by converging IT into the residential environment. Users can purchase and use their own smart home devices and conveniently control the home. As shown in Figure 1, in the smart home, there are smart home devices composed of various smart devices and sensors, a remote device accessing a smart home, and an access point (AP) connecting smart home devices and a remote device. Smart home devices have different communication and power specifications. A smart home device capable of communicating can communicate directly with the AP, while a device that cannot communicate by itself communicates through another smart home device. In general, smart home devices have the hierarchy structure as shown in Figure 1. The application layer provides the messaging protocol appropriate for communications in the smart home environment, and the user can establish its interface himself. The transport layer provides communication session management and defines the status of the connection with the service layer. The network layer provides the mechanism that enables proper communication among data within the smart home environment. The link layer defines the standards that make physical communication of the device possible. The user can install the dedicated application to the remote device to communicate through the above layers with the smart home device connected to the AP. However, smart home devices have different standards depending on the platform and, therefore, whenever a new smart home device is added, the user has to install a separate application for the new device. Additionally, recently, cases of security threats, such as takeovers of smart home devices and leakage of personal information by hackers threatening users' smart homes, are increasing [5]. Therefore, there is a need to define security requirements for a secure smart home environment.

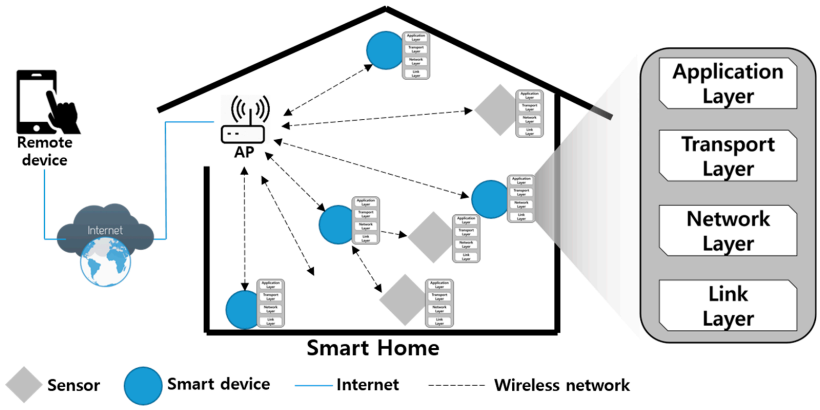


Figure 1. Smart home structure.

2.2. *Security Requirements for a Smart Home*

In the smart home environment for the user's convenience, numerous amounts and types of data are transmitted among a variety of smart devices, IoT gateways, and the users. Then, the data should be applied with security measures to prevent external exposure, be it simply-sensed information, or the voice, image, and the personal information related to the users, directly or indirectly; hence, the security measures should meet the following security requirements.

2.2.1. Privacy

There are various types of smart home devices in the smart home environment, and each of them has different types of in- and output. Although simple data, such as manifold logs, documents, images, animations, and so on, which occur in the smart home devices may not have significant meaning, they may hold the sensitive personal credit or privacy information that should be protected if malicious users analyze their correlation by big data analysis technique [6–8]. Therefore, proper security communication should be established for the user's personal information not to be exposed in the smart home.

2.2.2. Registration of Certified Smart Home Device

The users utilize a variety of smart home devices in the smart home upon their registrations. If the registration process of the device into the smart home is vulnerable, a smart home device that the user does not permit can be registered in the smart home [9]. Even though the registration process of the smart home device is secure, malicious users can access the smart home considering the potential to register the smart home device randomly by the unauthorized users. Consequently, only the authorized users should be able to register their smart home devices in the smart home via a secured process.

2.2.3. User Authentication in Smart Home

The users can access the smart home devices physically when they are in the smart home, however, physical access is difficult when they are out. Hence, the users access the smart home via remote devices [10–12]. Since the personal information of the users in the smart home can be exposed if the unauthorized user approaches the smart home remotely, they should follow the authentication process to block unauthorized users from the smart home. There are login systems using session/cookie; authentication systems using OAuth, in general; three-party password-based authenticated key exchange (3PAKE); biometrics; and so on. However, new authentication methods are required due to the vulnerability against security threats, such as session capture, vulnerable APIs, and so on [13–15].

2.2.4. Security Threats

When the users use the smart home, multiple security threats can occur. Most of the data transmitted in the smart home are delivered mainly by wireless network. If the malicious user counterfeits or modifies the data through the wireless network, which is vulnerable in the smart home, the data synchronization may not be properly performed between the user and the smart home device, and integrity may be affected, such as the occurrence of incorrect responses to the user's request [16,17]. Thus, it should be secure against the attacks of counterfeit data and modification by unauthorized users in the smart home environment [18]. In addition, because the users can utilize all of the services in their smart home by remote devices out of the home, it should be careful not to be infected by malicious code, with respect to malicious users capturing or hacking the remote devices. Furthermore, malicious users should not be able to easily access the smart home system even if the remote devices are stolen, too [19].

2.2.5. Heterogeneous Communication

There can be various types of smart home devices in the smart home. Since each smart home device can use different types of communication, the communication among the smart home devices may not be easy, or even impossible [20]. Hence, the system that supports different types of smart home devices and provides the services should be established to support the users with consistent smart home services.

2.2.6. Low Resources

Various smart home devices in the smart home environment continue to collect information or are on standby to communicate with users. Generally speaking, the smart home devices require miniaturization wherever they are positioned and low enough power to last longer with charging [21–24]. If the smart home device with a relatively low-powered battery performs a calculation with a high degree of complexity, it should be provided with proper security using low power in the smart home environment since the battery in the smart home device would be consumed quickly [25].

2.3. Previous Research on Smart Home

In this chapter, previous studies are reviewed on the user authentications and security in the smart home. Lee [13] proposed the protocol which could exchange the secure session keys between the user and the smart home device by using the pre-shared password for authentication and 3PAKE technique agreed the session key to be used in the communication afterwards. The proposed scheme in [13] were 3PAKE, based on XOR calculation, and based on the Diffie-Hellman method. In the case of the XOR calculation method, it has the potential risk of key exposure during the exchange of keys between the user and the smart home device. The 3PAKE technique based of the Diffie-Hellman method, a heavy calculation method, is not efficient in the smart home environment where weight reduction is required and has the problem of continuous session information exposure once the key is exposed.

In [14], the user access system was proposed using OAuth and realizing middleware to connect the users with the smart home devices for access to various smart home devices in an IoT environment. OAuth has the advantages to enable access to the other smart home devices with a one-time login process, and to resolve problems during the session/cookie usage since it is the access method using a token. Nevertheless, [14] generates a large amount of overhead without consideration of the middleware resource cost in the smart home environment where low power and low amounts of calculation are required. Since some vulnerable points were found in OAuth used in [14], such as token captures, re-transmission, and so on, by multiple analyses and studies, and new points which could not be satisfied with all of the considerations recommended in the OAuth protocol standards were detected, its security is lowered during usage.

The authentication technique by fingerprint recognition in the remote device was proposed in [15] for the users to access the smart home externally. It has middleware for the authentication between the user and the smart home device and the user transmits his or her own fingerprint information to the middleware. The middleware checks the user's authorization and approves the access to the smart home device. Prakash [15] has the advantage of convenience that the users do not have to remember their ID and password separately, while it has the potential of fingerprint information capture by malicious users because the fingerprint information of the users is not processed with the additional coding process, but transmitted he middleware. Additionally, the fingerprint is bio-information that is never changed, hence, serious security issues might occur due to the impossibility of changing once it is captured.

Kang [26] established an infrastructure based on trusted third party (TTP) and a physically-unclonable functions (PUFs)-based smart home environment. The developed technique of the security channel proposed, in [26], to register the service provider, the device of the smart home sensor, and the gateway into TTP and to authorize them mutually. The home gateway was used to resolve the heterogenicity among the smart home devices. All of the smart home devices have PUFs which cannot be copied and these are controlled by the PUF DB in TTP. However, Kang [26] has the problem that unauthorized smart home devices can be registered in the smart home.

3. Proposed Method

3.1. Proposed Smarthome Infrastructure

The proposed smart home environment is shown in Figure 2. The smart home devices in the smart home are connected to the home gateway which integrally manages the smart home devices, and the user accesses the smart home device through the AP. At this time, the user does not access the smart home device directly, but uses the smart home service by accessing it through the authentication system of the home gateway. In the proposed environment, to provide comprehensive smart home services to the user, a middleware layer has been added between the application layer and the transport layer in the home gateway and the smart home device. In doing so, more flexibility is offered to the communication between different devices and remote device and intellectual services can be provided. In addition, the user can access all smart home devices through a single comprehensive application. In the proposed scheme, the user establishes a Transport Layer Security (TLS) session with the home gateway, logs in with the account registered in the home gateway in advance, and receives a JWT to be used in the smart home from the home gateway. When the user accesses the home gateway, the user can authenticate himself/herself and access the smart home by communicating with the JWT and the IMEI issued by the user. Then, the authorized user can register the new smart home device in the home gateway through the proposed technique.

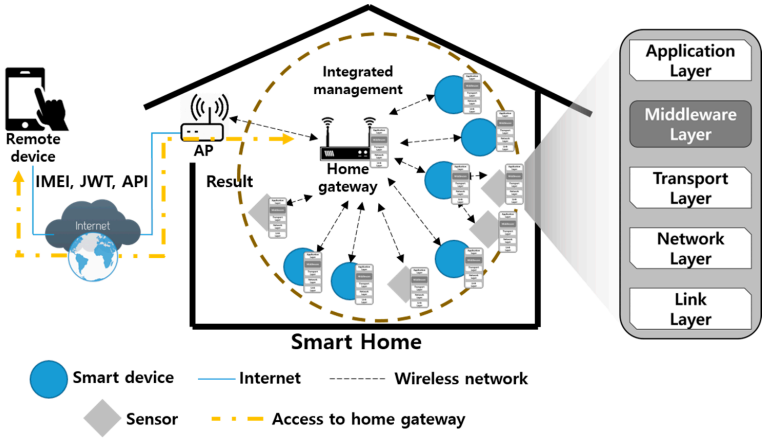


Figure 2. Proposed smart home environment.

3.2. Proposed Scheme

3.2.1. JSON Web Token

JWT is a token authentication system that encodes data in JSON format to base64 with the technique specified in RFC 7519 of IETF [27]. As shown in Figure 3, JWT consists of three sections: header, payload, and signature, and each section is separated by a (dot) operator. The header section specifies the type of token and the hash algorithm to use for the JWT signature. The payload section is where the actual information for the token to be used is stored. The information is a pair of names and values, and can store arbitrary data, such as the token issuer, token expiration time, and user information. The signature section allows the token issuer to sign the token using a hash-based message authentication code (HMAC), RSA, etc., to maintain the integrity of the token. When applying the HMAC, the header and payload section values are encoded in base64, and signatures are applied using hash HMAC using the secret key created in advance. When RSA is applied, the header section and payload section values can be encrypted and signed using the RSA private key of the token issuer. One such value consisting of the three sections is used as a token and it is called JWT. The server issues a JWT to the user and the user receives the service after proving himself/herself using the issued JWT. At this time, if the JWT is delivered over an unsecured network, a hacker can seize the base64-encoded JWT and attempt to modify the payload section to the desired value. However, because the hacker does not know the secret key to be able to hash the header and payload sections, the integrity of the token can be maintained. JWT has the advantage that it can be used not only for user authentication, but also for maintaining data integrity.

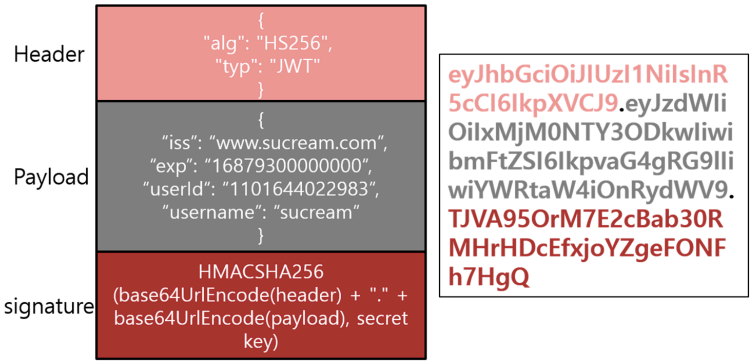


Figure 3. JWT structure.

3.2.2. Proposed Scheme

The proposed protocol is divided into a protocol in which a user authenticates itself where a JWT is issued from a home gateway, a protocol in which a new smart home device is registered only by an authorized user, and a protocol in which a home gateway is accessed using JWT and IMEI. Table 1 shows the parameter values used in the proposed protocol.

Table 1. Proposed protocol parameters.

Notation	Meaning
Client	Client
Home gateway	Home gateway
Smart home device	Smart home device
Session key$_{UG}$	Session key between client and home gateway
G_{pub}	Home gateway's public key
G_{pri}	Home gateway's private key
H(x)	Hash function

Table 1. *Cont.*

Notation	Meaning
ID_x	x's ID
PW_x	x's password
$\oplus$	Exclusive or operator
$IMEI_x$	x's IMEI value
Secret key_x	x's secret key
JWT_x	x's JWT
Base64	Base64 encoding/decoding
▪▪▪▪▪▪▶	Secure communication
R_x	Generated random number for x
$A_{d\text{-}c}$	Generated random key between client and smart home device
API	API requested from client
Result	Result processed by smart home device
$Salt_R$	Random number to cover user's IMEI

Proposed User Authentication Phase

The client must authenticate to the home gateway to access the smart home. In the proposed authentication protocol, as shown in Figure 4, after establishing a TLS connection between the client and the home gateway, if the client transfers the ID, password, and IMEI value to the home gateway, the home gateway authenticates the client and issues the JWT and R_{user} to the client.

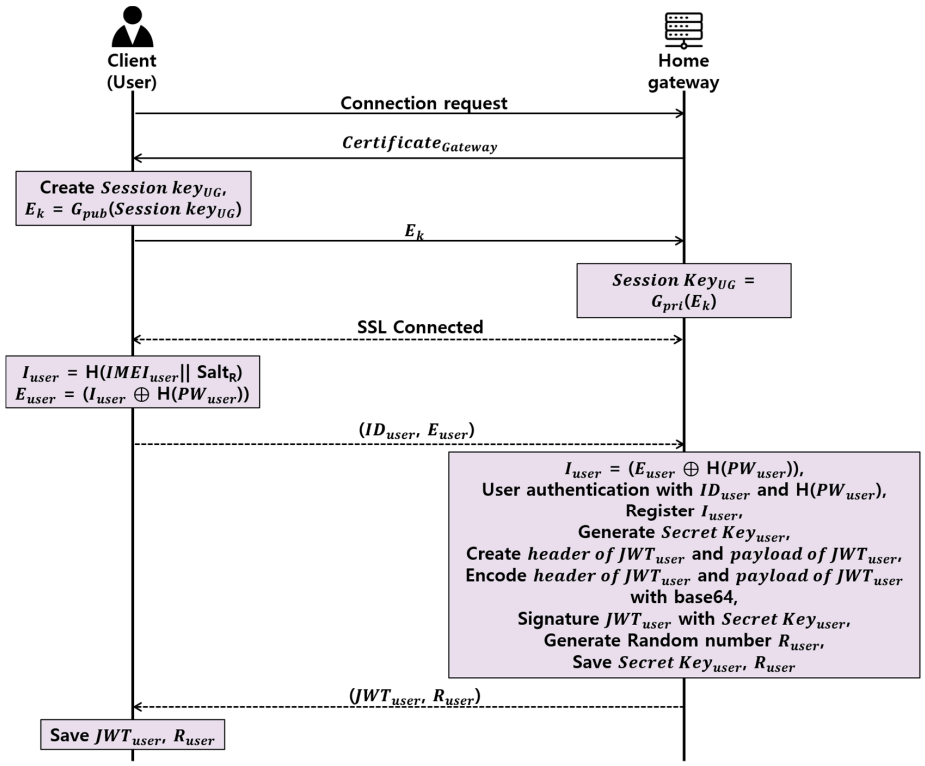


Figure 4. Proposed user authentication protocol.

Step 1. Client and home gateway establishs TLS session through TLS handshake.

Step 2. Client obtains I_{user} by concatenating and hashing randomly generated $Salt_R$ with IME_{Iuser}, which is the device's original value, and subsequently, generates E_{user} through the XOR with the password's hash value, $H(PW_{user})$, and transmits ID_{user} and E_{user} to the home gateway.

Step 3. The home gateway obtains the I_{user} by XORing the $H(PW_{user})$ of the previously-registered client and the E_{user} received from the client.

Step 4. The home gateway authenticates the client via ID_{user} and $H(PW_{user})$, and registers the $IMEI_{user}$ as the IMEI of the client.

Step 5. The home gateway randomly generates a JWT secret key to be issued to the client, and then generates the header field and a payload field of the JWT. At this time, the header field is used to determine whether to use JWT and the signature technique to be used in the signature field. In the payload field, the issuer, the expiration period of the token, the user identification ID, the user name, and the access right of the user are inputted.

Step 6. The home gateway signs the JWT with the secret key using the HMAC method, randomly generates a random number R_{user}, and sends JWT_{user} and R_{user} to the client.

Step 7. The client stores JWT_{user} and R_{user}, which are delivered from the home gateway.

Proposed Register New Smart Home Device Phase

When a new smart home device is registered in a smart home, it must be possible to register it only by an authorized user. The proposed scheme assumes that when a client that has been issued a JWT registers a new smart home device in a smart home, the smart home device can be registered only through the authorization of an authorized client in the same network as the home gateway. As shown in Figure 5, when a new smart home device is connected, it can be registered after receiving confirmation of connection to the client.

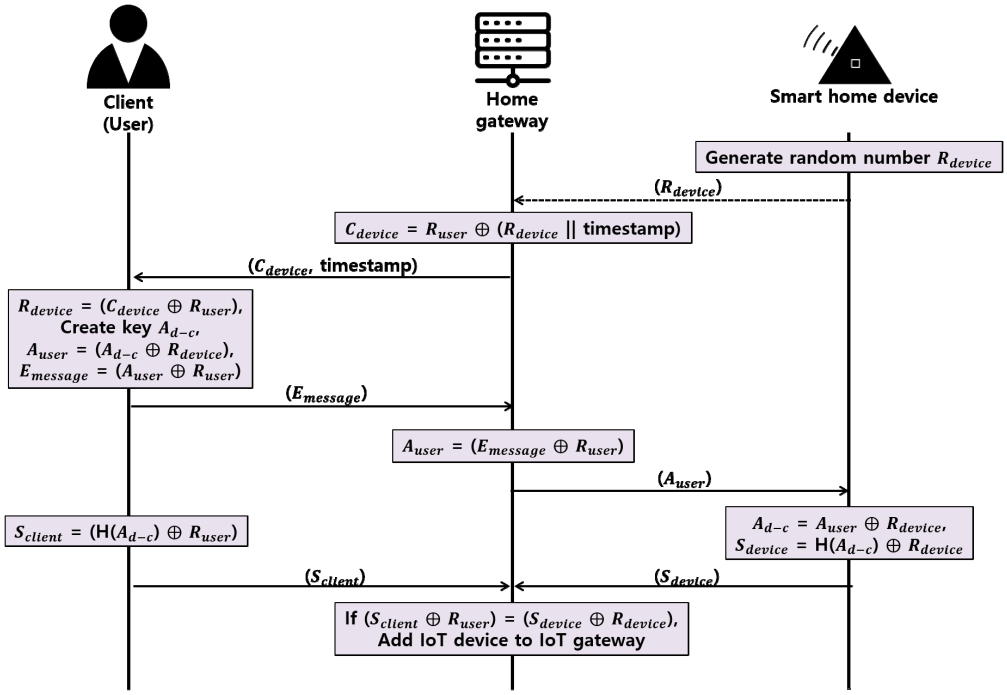


Figure 5. Proposed register new smart home device protocol.

Step 1. The smart home device generates a random number R_{device} and sends it to the home gateway through a secure channel.

Step 2. The home gateway concatenates the timestamp and the R_{device} to prevent a replay attack, then the home gateway creates a C_{device} that XORs the R_{user} shared with the client in the user authentication phase and delivers it to the client.

Step 3. The client XORs the received C_{device} and R_{user} to obtain the R_{device} and generates the random number $A_{d\text{-}c}$. Client XORs $A_{d\text{-}c}$ and R_{device} to create A_{user}, then XORs Auser and R_{user} to deliver $E_{message}$ to the home gateway.

Step 4. The home gateway XORs $E_{message}$ and R_{user} to obtain the A_{user} and delivers the A_{user} to the smart home device.

Step 5. The smart home device XORs A_{user} and R_{device} to obtain $A_{d\text{-}c}$, XORs $H(A_{d\text{-}c})$, which is a hash of $A_{d\text{-}c}$ and R_{device}, generates S_{device}, and delivers S_{device} to the home gateway.

Step 6. The client also XORs the $A_{d\text{-}c}$ hash $H(A_{d\text{-}c})$, and R_{user} to obtain S_{client} and deliver S_{client} to the home gateway.

Step 7. The home gateway compares the acquired $H(A_{d\text{-}c})$ obtained by XORing the S_{client} and S_{device} received from the client and smart home device with R_{user} and R_{device}, respectively, and if the smart home device has the same value, the smart home device is registered in the home gateway, and refused if different.

Proposed Access API Phase

The user must authenticate himself to the home gateway to access the smart home device. As shown in Figure 6, a client sends its own JWT and IMEI issued when requesting the API to the home gateway and authenticates, and the home gateway then requests the client's API to the smart home device and delivers the response to the client.

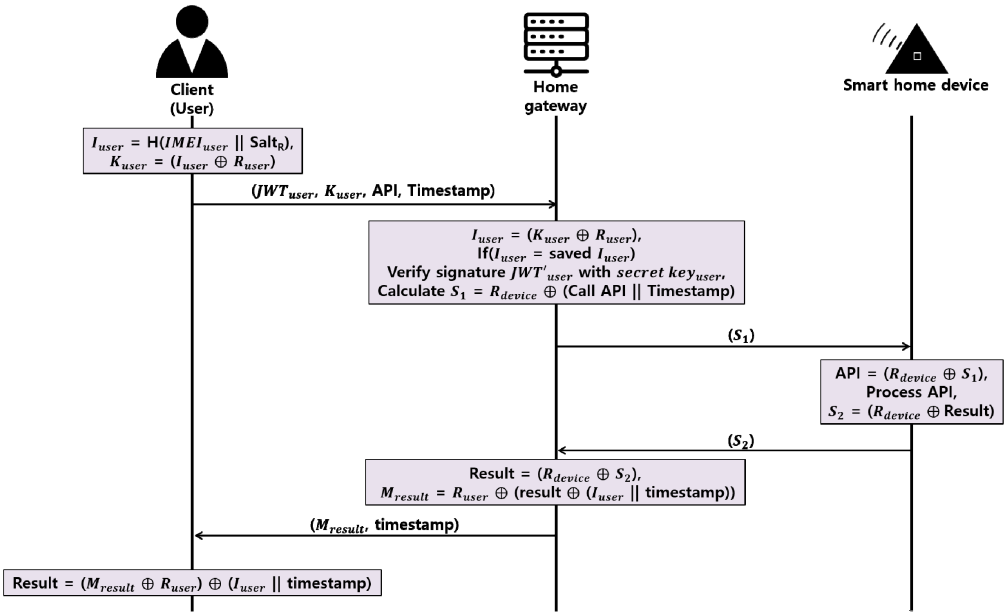


Figure 6. Proposed API access protocol.

Step 1. The client generates I_{user} by concatenating and hashing $IMEI_{user}$ and $Salt_R$ and, subsequently, delivers K_{user} to the home gateway, which is generated through the XOR of R_{user} with this value.

Step 2. The home gateway identifies the authorized client by obtaining I_{user} through the XOR of K_{user} and R_{user} and, subsequently, compares the existing registered client's I_{user}. At this time, the home gateway judges that it is abnormal if it receives different IMEI values from one client to another JWT within a short time.

Step 3. For the JWT received from the client, the home gateway verifies the validity of the token through the HMAC using the secret key that only it knows.

Step 4. The home gateway concatenates the client's API with the timestamp, XORs this value with the R_{device}, creates S_1, and delivers it to the smart home device.

Step 5. The smart home device XORs S_1 and R_{device} to obtain the client's API, and then generates the result after processing the client's request. Then, the S_2 created by XORing result and R_{device} is sent to the home gateway.

Step 6. The home gateway obtains the result by XORing S_2 and R_{device}. The home gateway concatenates the IMEI value and the timestamp of the registered client, XORs the result, and sends the M_{result} value to the client by XORing the value with the R_{user} value again.

Step 7. The client XORs the M_{result} and R_{user} values and XORs the IMEI with the timestamp to obtain the result.

4. Implementation of the Proposed Protocol

The home gateway in the smart home environment proposed in this paper realized as a Raspberry pi3, Raspbian OS, Apache, MySQL, and PHP; and the smart home device realized as each smart home device using an Ardunino uno, temperature sensor, power supply system, camera sensor, and so on, as shown in Figure 7 and Table 2. The client used a Samsung Galaxy Note5 Android 6.0.1. For security of the home gateway, an SSL/TLS authentication letter was issued and applied in StartSSL. The realizations were performed as the step that the client logs into the home gateway with his or her own preregistered account and issued JWT; the step to register the new smart home device by the authorized client; and the step for the client to access to the smart home device and communicate with it.

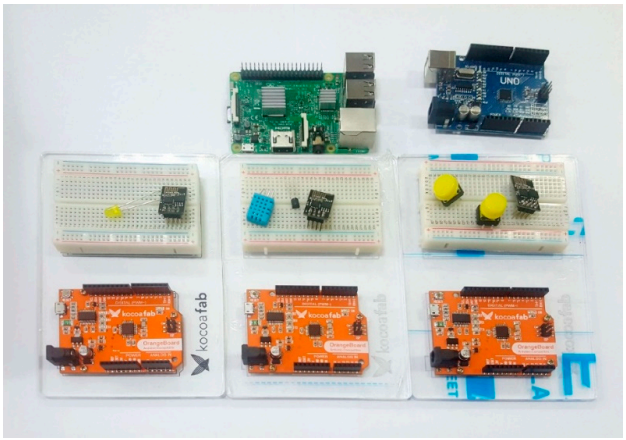


Figure 7. Devices used in the proposed scheme.

Table 2. Specifications of devices.

	Client	**Home Gateway**				**Smart Home Device**		
Name	Samsung Galaxy Note5	Raspberry pi3	Apache2	MySQL	PHP	ESP8266	LED	DHT11
Feature	Android 6.0.1	Raspbian OS JESSIE	Apache/2.4.10 (Raspbian)	15.1 Distrib 10.0.25-MariaDB	PHP 5.6.22-0+deb8u1	WiFi module	Yellow LED	Temperature-humidity sensor

4.1. Login Function

The client performs the login process in the home gateway through the preregistered account in the home gateway, or the login process generating a new account as shown in Figure 8. Then, the connection with the home gateway uses HttpsURLConnection for SSL communication. Providing input of an incorrect account, the login process will be failed. Additionally, the authority of the Android

permission READ_PHONE_STATE was added in the client device to obtain the IMEI value of the client during the login process. In case of a login process with an authorized client, the IMEI value of the client is registered in the home gateway and the JWT is issued from the home gateway.

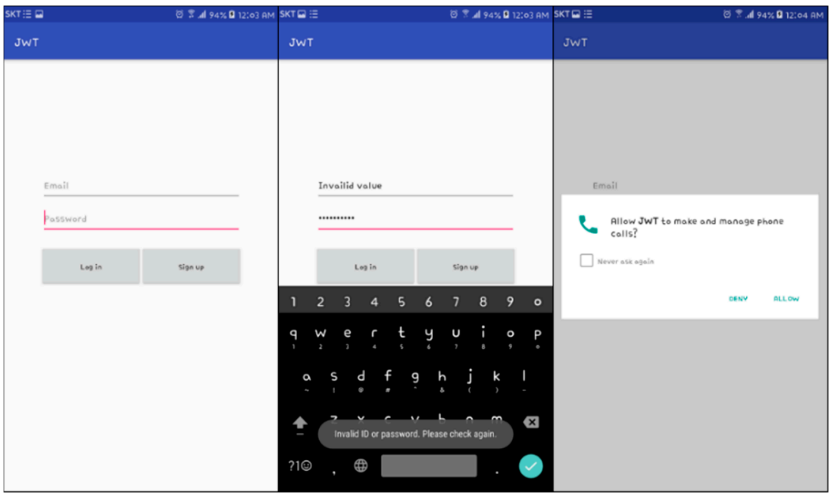


Figure 8. Login page for client access to a smart home.

4.2. Identification and Registration of Smart Home Devices

The client who completes the login process can check the list of the smart home devices connected to the home gateway, as shown in Figure 9 (left, right). If '*add new device*' button is clicked, as in Figure 9(center), any smart home device to try to connect the home gateway would be informed to the client. If the client permits it, the smart home device would be registered in the home gateway. After finish it, the user can utilize the required services depend on the accessibility of the smart home device registered in the home gateway.

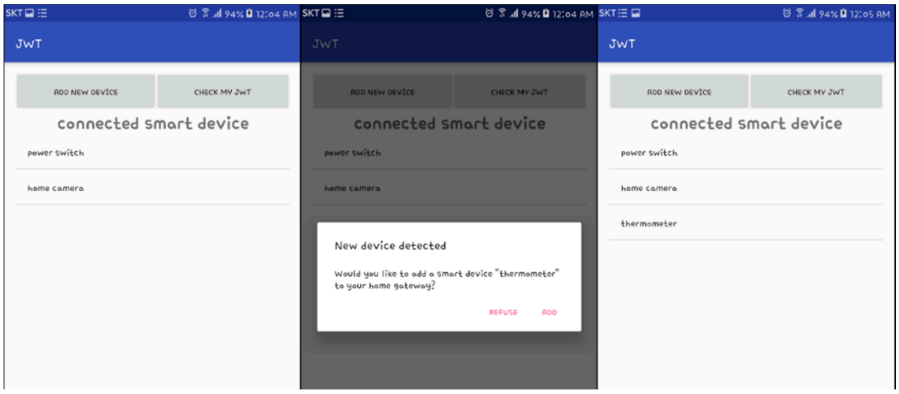


Figure 9. Connected smart home devices in a smart home.

4.3. JWT Validation and Smart Home Device Access

The client can check his or her token issued from the home gateway upon pushing the *check my JWT* button, as shown in Figure 10. The decoded data of the header and payload fields in the JWT can be checked in Figure 10. However, the signature of the client that does not know the secret key cannot be verified since the signature field is developed with the HMAC of the secret key that only knows the home gateway.

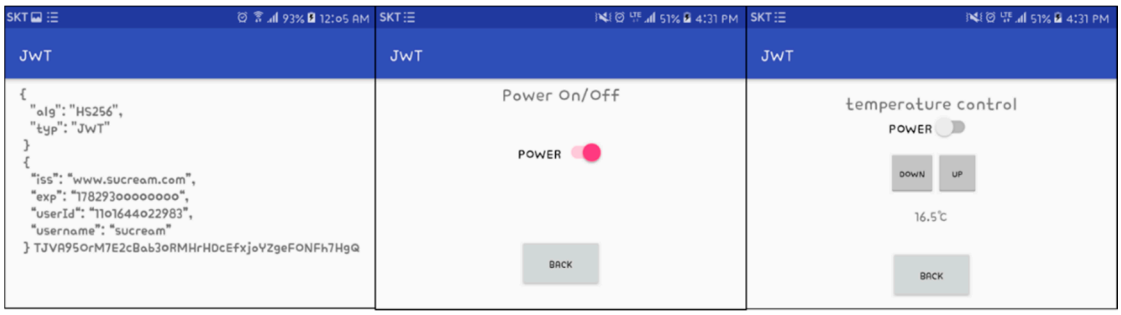


Figure 10. Checking the JWT and control of smart home devices.

5. Security and Performance Analysis

5.1. Secuity Requirement Analysis

The proposed protocol enables remote devices and various smart home devices to communicate through home gateways. Additionally, the registration of the unauthorized smart home devices can be blocked since only the authorized user can register the new smart home device in the smart home. Since the user, the home gateway, and the smart home device communicate using the shared secret code, the leakage of the personal information can be protected. In addition, the home gateway can detect the changes of the client by the verification of the IMEI value even if the malicious user captures the JWT. Therefore, this paper compared and analyzed security requirements with existing papers as Table 3.

Table 3. Comparative security requirement analysis between smart homes.

	Dae-Hwi Lee et al. [13]	Fremantle et al. [14]	Prakash et al. [15]	Kang, Jungho et al. [26]	Proposed Scheme
Privacy	O	O	O	O	O
Secure Smart home device Registration	O	X	X	X	O
User authentication in smart home	O	O	O	O	O
Security threats	O	Δ	Δ	O	O
Heterogeneous communication	X	X	X	O	O
Low resource	X	X	O	O	O

O: Support; Δ: not fully support; X: Not support.

5.1.1. Privacy

In the smart home environment, data should be accessed only by the authorized clients, and those within the smart home should not be exposed to the unauthorized clients. In the proposed protocol the client can deliver his or her own IMEI value and R_{user} value that only the client and the home gateway know upon XOR to the home gateway securely so as to obtain the response to what he or she requests. Since the home gateway sends and receives the pre-shared R_{device} value and the data to the smart home device upon XOR, the user's sensitive data shall not be exposed. Even if the malicious user captures the JWT and requests to the home gateway after amendment, the signature of the JWT cannot be counterfeited because it does not know the secret key. Moreover, the home gateway can detect what the malicious user requests with the user's JWT since the user's IMEI value is checked whenever the user requests.

5.1.2. Registration of a Certified Smart Home Device

A variety of smart home devices in the smart home respond the user's requests by the home gateway. Then, the registration to the home gateway should be possible only for the authorized smart home devices by the user. Fremantle, Prakash and Kang [14,15,26] can register a new smart home device in the smart home, but there is a disadvantage that anyone can register a new smart home device in the smart home because there is no process of identifying the registrant. Therefore, in this paper, the user verifies himself or herself by a login process prior to the registration of the smart home device. After that, if the new smart home device tries to access the home gateway, the home gateway shall make the user acknowledge this and the user shall decide whether he or she adds the smart home device. Later, the user and the smart home device obtain the same $A_{d\text{-}c}$ value by the home gateway and hashes $A_{d\text{-}c}$. Then, the user delivers the hashed $A_{d\text{-}c}$ and R_{user} upon XOR to the home gateway, and the smart home device delivers the hashed $A_{d\text{-}c}$ and R_{device} upon XOR to the home gateway. In the case of two identical values, the home gateway registers the new smart home device and adds it to the user's list of the smart home devices.

5.1.3. User Authentication in the Smart Home

The user authentication process is used to access the smart home externally. In the proposed protocol, the user registers his or her IMEI value after verification of ID and password in the home gateway during the first login process, and obtains the JWT. Even if an improper user captures the user's ID and password, the verification will fail since it has a different IMEI value in the case of an unauthorized device. Therefore, only the authorized users can access to the smart home.

5.1.4. Security Threats

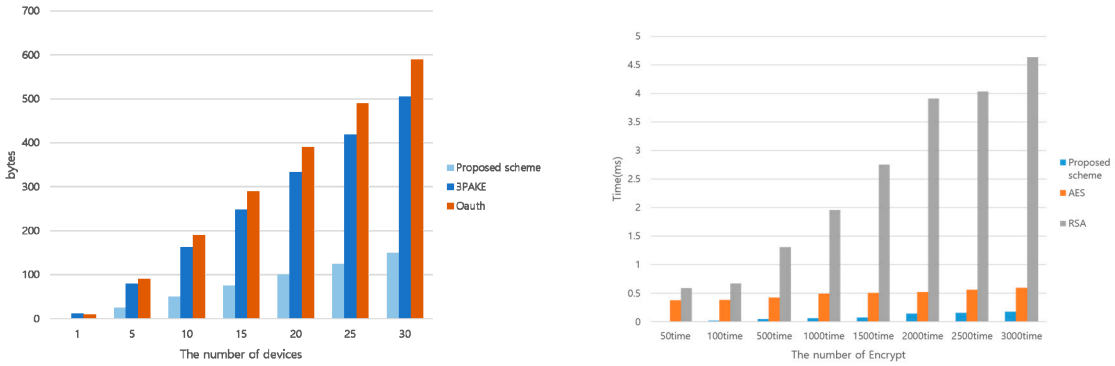
The information used in the smart home should be able to be inquired and amended only by the authorized user. The Diffie-Hellman scheme proposed in [13] has a high computational complexity, and there is a problem that when the session key between a user and a smart home device is exposed, all subsequent session information is exposed. Additionally, the technique proposed in [15] is a method of storing fingerprint information in a DB and comparing them. The method is proposed in [15] and is likely to be easily exposed because the fingerprint of the user is transmitted to the middleware without a separate process. Since biometric information is a unique value that cannot be changed, serious security damage can occur if exposed once. Hence, in this paper, the sending and receiving of information in the smart home is coded so only authorized users can make them able to inquire and amend. The transmitted data between the user and the home gateway are performed with encryption and decryption of R_{user} that only the user and the home gateway know upon XOR, and the transmitted data between the home gateway and the smart home device performed with encryption and decryption of R_{device} upon XOR. The attacker who does not know R_{user} and R_{device} cannot detect the data transmitted in the smart home.

5.1.5. Heterogeneous Communication

The integrated management system is required to recognize each device since various smart home devices in the smart home have different platforms. Lee, Fremantle and Prakash [13–15] did not consider a comprehensive environment for devices using different platforms. In [20], the devices with individually different logic were integrated using XLM, and Intel also enabled communication with the devices with each different logic through their technology. As such, this paper added a middleware layer between the application layer and the transport layer in the home gateway and the smart home device to offer flexibility in communication between different devices, and the user is able to use the comprehensive smart home services through a single application.

5.1.6. Computing Resource Analysis

The smart home device should be considered with low power and weight reduction in the smart home environment. In this paper, secure data transmission was realized between the smart home device and the user with a relatively low level of calculation and resource consumption, taking into account the specifications of the smart home device. Figure 11(left) demonstrates the amount of resource consumption that occurred during the user's authentication process whenever the new smart home devices are registered. In [8]'s proposed scheme using the Diffie-Hellman Key exchange method, the amount of data is increased as the number of the smart home devices is increased. The user should be verified with the effectiveness of the issued token through an external resource authorization serve, whenever new smart home devices are added in the smart home; in [9]'s proposed scheme since it uses OAuth. Therefore, the large amount of resources is consumed as the number of smart home devices is increased. The proposed protocol in this paper is to consume relatively lower resources even if the number of the smart home devices is increased, applying minimal XOR and hash calculations to lower the burden of the smart home devices.



(Left) **(Right)**

Figure 11. Computing resource analysis (**Left**), speeds of encryption and decryption of proposed scheme (**Right**).

In the smart home environment, encryption and decryption processes are frequently used due to processing large amounts of information. In the case of complicated encryption and decryption calculation, each smart home device cannot process the data quickly and timely communication may be difficult. Figure 11(right) shows that it can perform with relatively faster speed when compared with the proposed scheme of encryption and decryption calculation performed by each smart home device, RSA, and AES.

6. Discussion

In this paper, we propose three protocols, which include a user authentication protocol allowing only an authorized user to access the smart home, a protocol allowing only an authorized user to register a new smart home device in a smart home, and a protocol in which an authorized user requests an API to a smart home device securely through a home gateway. When the user logs in to the smart home through the remote device he/she has, he/she inputs the ID and password and the IMEI of the remote device is delivered to the home gateway in conjunction. There is a general characteristic when using the IMEI to authenticate the user's device; it cannot be easily changed once exposed. In this paper, when the user first registers an IMEI value, it concatenates the value of the IMEI with the value of the SaltR and hashes for delivery to the server. Through this, the user does not need to directly expose the IMEI. Even if the user's IMEI is exposed, the user can add a new IMEI value to the home gateway whenever the user wants because the IMEI value is a salted and hashed IMEI value, not the

original IMEI value. Additionally, since the IMEI value of the remote device and the Euser, which is XORed with H (PWuser), is transmitted to the home gateway, there is little possibility of exposing the IMEI of the remote device on the network. Furthermore, if a malicious client attacks through IMEI brute force, it will ask for APIs multiple times. Therefore, if the home gateway detects a different IMEI for one JWT within a short time, it is considered to be a hacker. Since the user's IMEI and password are not exposed on the network, attacks from hackers are difficult. Even if a hacker wishes to perform a complete hijack, it is very unlikely because he must know the user's ID, password, and IMEI values before they can attack. In addition, JWT tampering is also impossible because the secret key to sign the JWT is unknown, even if a hacker attempts to access unauthorized information through JWT tampering. However, in an environment where the remote device's IMEI can be easily leaked, it is recommended that one uses an identification value that can be changed when exposure occurs.

7. Conclusions

In the IoT era where things communicate, the smart home, which combines with the environment in which people live, provides users with various convenient services. However, recently, smart home security threats, such as the vulnerability of sessions threatening the smart home and OAuth vulnerabilities, have appeared, and attacks, such as smart home intrusion, personal information leakage, and privacy exposure are increasing. Therefore, in order to establish a secure smart home, authentication and device registration techniques that can cope with these various security threats should be applied. If a correct security system is not built, the user's personal information may be exposed to a hacker or a serious security problem, such as an unauthorized service being executed, may occur. Session/cookie and OAuth, which were used in existing smart home environments, are vulnerable because hackers can steal user information or disguise themselves as an authorized user. Therefore, in this paper, we proposed a user authentication scheme using JWT and IMEI, and proposed a scheme where only a user authorized to the home gateway can add a new smart home device. The proposed scheme minimizes the computation of data transmission and reception between the user and the smart home device, thereby providing low-power computing of the smart home device and the remote device. Additionally, even if a hacker seizes the JWT through JWT and IMEI, it has proved secure against various attack scenarios by preventing hackers from changing tokens by signing using a secret key.

Author Contributions: Mansik Kim researched relation work; Namsu Hong designed the protocol; Moon-Seog Jun and Jungho Kang performed and analyzed the data; and Namsu Hong and Jungho Kang wrote the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
2. Marianthi, T.; Tsalis, N.; Gritzalis, D. Smart Home Solutions: Privacy Issues. In *Handbook of Smart Homes, Health Care and Well-Being*; Springer International Publishing: Cham, Switzerland, 2017; pp. 67–81.
3. Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. Lightweight and secure session-key establishment scheme in smart home environments. *IEEE Sens. J.* **2016**, *16*, 254–264. [CrossRef]
4. Andreas, J.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733.
5. Choi, B.-M. A Study on Setting up the Concept of Smart City through Analysis on the Term 'Smart'. *J. Korea Contents Assoc.* **2011**, *11*, 943–949. [CrossRef]
6. Lee, M.; Park, J. Analysis and Study on Invasion Threat and Security Measures for Smart Home Services in IoT Environment. *J. Inst. Int. Broadcast. Commun.* **2016**, *16*, 27–32. [CrossRef]

7. Verhoef, P.C.; Kannan, P.K.; Luo, X.; Zhang, Y. Consumer Connectivity in a Complex, Technology-Enabled, and Mobile-Oriented World with Smart Products. Northeastern U. D'Amore-McKim School of Business Research Paper, No. 2912321. Available online: https://ssrn.com/abstract=2912321 (accessed on 23 June 2017).
8. Suryadevara, N.K. Wireless Sensor Sequence Data Model for Smart Home and IoT Data Analytics. In *Proceedings of the First International Conference on Computational Intelligence and Informatics*; Springer: Singapore, 2017.
9. Bandara, A.M.K.C. Secure Smart Home System. *Master of Science in Information Security*. 2016. Available online: documents.ucsc.lk/jspui/handle/123456789/3711 (accessed on 23 June 2017).
10. Tan, J.Y.; Ker, P.J.; Abdullah, A. Smart Home Design with XBee Wi-Fi and Android-Based Graphical User Interface. In Proceedings of the 2016 IEEE Student Conference on Research and Development (SCOReD), Kuala Lumpur, Malaysia, 13–14 December 2016.
11. Wang, G.; Song, D. Smart Home Services Using the Internet of Things. In *Internet of Things and Data Analytics Handbook*; Wiley: Hoboken, NJ, USA, 2017; pp. 613–630.
12. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. *J. Inf. Proc. Syst.* **2017**, *13*, 184–195. [CrossRef]
13. Lee, D.-H.; Lee, I.-Y. A Study on Enhanced 3PAKE Scheme against Password Guessing Attack in Smart Home Environment. *J. Korea Inst. Inf. Secur. Cryptol.* **2016**, *26*, 1471–1481. [CrossRef]
14. Fremantle, P. Privacy-enhancing Federated Middleware for the Internet of Things. In Proceedings of the Doctoral Symposium of the 17th International Middleware Conference, New York, NY, USA, 12–16 December 2016.
15. Prakash, N.S.; Venkatram, N. Establishing efficient security scheme in home IOT devices through biometric finger print technique. *Indian J. Sci. Technol.* **2016**, *9*. [CrossRef]
16. Fernandes, E.; Jung, J.; Prakash, A. Security Analysis of Emerging Smart Home Applications. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016.
17. Min, K.W.; Moon, S.Y.; Park, J.H. An enhanced security framework for home appliances in smart home. *Hum.-Centric Comput. Inf. Sci.* **2017**, *7*, 6.
18. Kim, M.-S.; Lee, J.-K.; Park, J.H.; Kang, J.-H. Security Challenges in Recent Internet Threats and Enhanced Security Service Model for Future IT Environments. *J. Int. Technol.* **2016**, *17*, 947–955.
19. Zhu, W.; Lee, C. A Security Protection Framework for Cloud Computing. *J. Inf. Proc. Syst.* **2016**, *12*, 538–547. [CrossRef]
20. Moazzami, M.-M.; Xing, G.; Mashima, D.; Chen, W.-P.; Herberg, U. SPOT: A Smartphone-Based Platform to Tackle Heterogeneity in Smart-Home IoT Systems. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016.
21. Jungho, K.; Park, G.; Park, J.H. Design of secure authentication scheme between devices based on zero-knowledge proofs in home automation service environments. *J. Supercomput.* **2016**, *72*, 4319–4336.
22. Kwon, T.; Lee, J.; Choi, H.; Yi, O.; Ju, S. Efficiency of LEA compared with AES. *J. Converg.* **2015**, *6*, 16–25.
23. Deschambault, O.; Gherbi, A.; Légaré, C. Efficient Implementation of the MQTT Protocol for Embedded Systems. *J. Inf. Proc. Syst.* **2017**, *13*, 26–39. [CrossRef]
24. Lee, S.-W.; Yu, J.-H.; Sim, K.-B. Real-time Streaming and Remote Control for the Smart Door-Lock System based on Internet of Things. *J. Korean Inst. Intell. Syst.* **2015**, *25*, 565–570. [CrossRef]
25. Wu, X.; Hu, X.; Moura, S.; Yin, X.; Pickert, V. Stochastic control of smart home energy management with plug-in electric vehicle battery energy storage and photovoltaic array. *J. Power Sources* **2016**, *333*, 203–212. [CrossRef]
26. Kang, J.; Kim, M.; Park, J.H. A reliable TTP-based infrastructure with low sensor resource consumption for the smart home multi-platform. *Sensors* **2016**, *16*, 1036. [CrossRef] [PubMed]
27. Jones, M.; Bradley, J.; Sakimura, N. JSON Web Token (JWT), RFC 7519, 2015. Available online: http://www.rfc-editor.org/info/rfc7519 (accessed on 23 June 2017).