International Journal of Internet, Broadcasting and Communication Vol.13 No.3 1-11 (2021)
http://dx.doi.org/10.7236/IJIBC.2021.13.3.1

IJIBC 21-3-1

Implementing Onetime Password based Access Control System for Secure Sharing Service

Namhi Kang

Professor, Department of Cybersecurity, Duksung Women's University, Korea
kang@duksung.ac.kr

Abstract

Development of ICT technologies leads exponential growth of various sharing economy over the last couple of years. The intuitive advantage of the sharing economy is efficient utilization of idle goods and services, but there are safety and security concerns. In this paper, we propose a onetime password based access control system to support secure accommodation sharing service and show the implementation results. To provide a secure service to both the provider and the user, the proposed system issues a onetime access password that is valid only during the sharing period reserved by the user, thereafter access returns to the accommodation owner. Especially, our system provides secure user access by merging the two elements of speaker recognition using voice and a one-time password to open and close the door lock. In this paper, we propose a secure system for accommodation sharing services as a use-case, but the proposed system can be applicable to various sharing services utilizing security-sensitive facilities.

Keywords: *Sharing Economy, Smart Home Security, Authentication, One Time Password, Speech Recognition*

1. Introduction

The sharing economy emerged in the late 2000s, and with the development of information & communications technology (ICT) technologies, various sharing services began to be widely applied to our daily lives. Sharing economy activities include sharing everyday items that we don't use and even expensive properties, such as cars and houses [1]. As the market for various sharing services expands, including leading companies such as Uber and Airbnb, it became easier for people to provide transportation or accommodation, even if they are not officially registered business operators. In particular, the development of various sharing platforms and the increase of social networking service users made it easy to connect consumers and suppliers and accelerated the growth of sharing economy businesses [2].

While the spread and development of the sharing economy have advantages in terms of efficiently using idle resources and creating additional benefits, there are also disadvantages such as safety and security issues including theft and personal data leakage [3]. In particular, accommodation sharing services such as renting a house or room to strangers can be directly related to safety and security issues for both visitors and providers [4]. In other words, the visitor has no way of trusting how the locks are managed and operated by the provider

Manuscript Received: May. 10, 2021 / Revised: May. 14, 2021 / Accepted: May. 16, 2021
Corresponding Author: kang@duksung.ac.kr
Tel: +82-2-901-8349, Fax: +82-2-901-8341
Professor, Department of Cybersecurity, Duksung Women's University, Korea

who wants to share the house. In addition, the provider cannot prevent previous visitors from sneaking in or trespassing unless the locking device is physically changed (such as changing the password or reinstalling the door lock).

The ICT technologies that boost the sharing economy also have security issues. In particular, the era of the Internet of Things (IoT) is on the rise as ordinary objects that have not been considered in the past are now connected to the Internet. Things or virtual objects are inter-connected to exchange information, and new application services are being created based on the connection. The range of services provided based on IoT technologies is expanding from smart homes to smart cars and smart cities. IoT technologies will have an impact on almost all aspects of our lives and change and enrich our life patterns. However, as IoT devices are closely related to daily life, the data transmitted also contain sensitive information and thus, the attack surface that exposes user information is also growing [5]. The increase in IoT devices will increase the exposure of data, which may lead to privacy violations and even problems directly related to peoples' lives. Therefore, security is one of the most significant issues in IoT environments [6].

This paper proposes and implements a service that provides secure access to door locks to prevent illegal entry or intrusion of accommodation sharing services or general households. In particular, this service allows only the user to use the accommodation during the sharing period and ensures that the door lock password is not shared with the provider before the period ends. It also enhances security by using voice recognition to verify the user's identity. The proposed technique is for accommodation sharing services, but it is also applicable to other sharing services by applying various technologies and can be safely applied to security-sensitive facilities.

This paper is structured as follows. Section 2 presents the background and motivation of the proposed technique and the open technologies applied for voice recognition. Section 3 describes the main functions and how the proposed system works. Section 4 describes the implementation results, performance, and security analysis of main functions, and the last section presents the conclusion.

2. Background and Motivation

2.1 Sharing Economy

In 2008, Lawrence Lessig, a professor at Harvard University, defined the sharing economy as "collaborative consumption made by activities of sharing, exchanging, and rental of resources without owning the goods." That is, it does not mean producing and owning new goods but sharing things that already exist. It is different from the production and consumption patterns in the past. The sharing economy made it possible to use underused assets or products that we do not use. It also helps the environment. In particular, smartphone penetration is a key driver that is accelerating the growth of the sharing economy because we can easily adopt and use it whenever and wherever necessary. The general public can now easily share goods and services even if they are not professional or registered agents or brokers. While the term sharing economy is the term most often used, it is also referred to as Gig Economy, Creative Commons, Access Economy, On Demand, and Open Source [1, 7].

Typical examples of sharing economy services include Airbnb, an accommodation sharing service, and Uber, a ride-sharing service. A representative company in Korea is Socar which supports a car-sharing platform. Furthermore, sharing economy platforms allow people to use not only large assets but also small assets. In the case of electronic kickboards, people can ride a kickboard for a short time, return the sharing board anywhere, and share their experiences. In addition to tangible assets, sharing economy platforms also apply and provide intangible assets such as labor and knowledge.

These services are receiving the spotlight because they provide various benefits and advantages. For example, they give people access to goods they cannot afford or do not use frequently. Many people use Airbnb not only because they need accommodation, but also because they want to experience the dwelling culture when they travel abroad. The sharing economy market is expected to grow further in the future [7, 8]. Figure 1 shows the growing number of sharing economy users (illustrated by the grey bar chart) and rate of the population (illustrated by the growing red line).

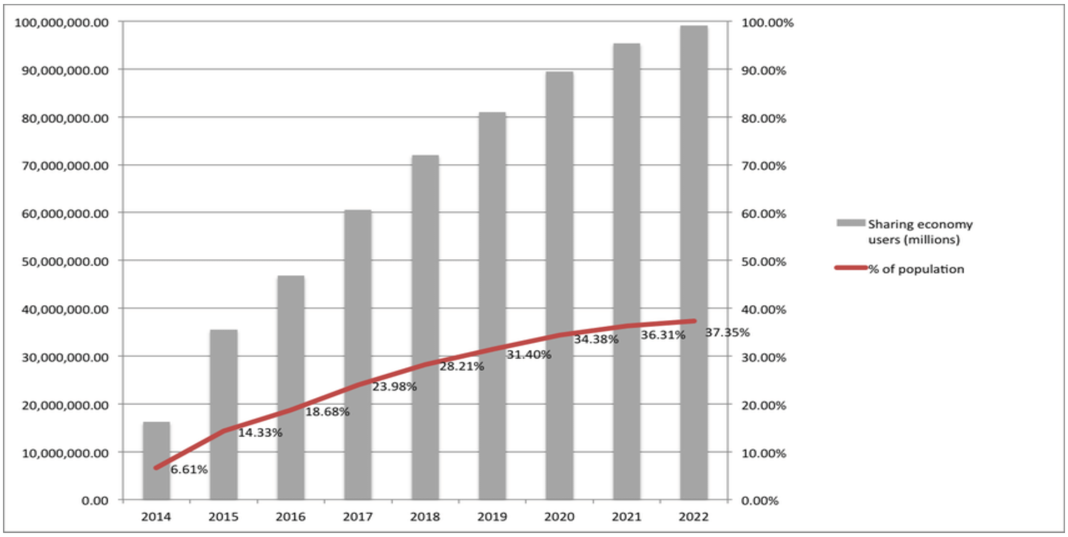


Figure 1. Size and growth of the sharing economy (source: eMarketer)

However, the sharing economy does not only have advantages. Major disadvantages include opposition from traditional business sectors, tax evasion, and violations of labor laws. There are also difficulties in management. In terms of car sharing, there are cases in which minors were involved in accidents due to poor vetting or identification procedures. In the case of accommodation sharing, even non-registered or unauthorized providers can share their homes, which raises security concerns. In addition, without proper laws, the regulations on Koreans and foreigners may differ [8].

2.2 Security Problem in Smart Space

The IoT means that things such as home appliances and electronic devices are connected through a network to exchange information with each other, collect and analyze data, and provide necessary services to users. IoT technologies are being used in our daily lives as they began to be applied to home appliances, health care, and meter reading. IoT technology is evolving into M2M/IoT, which connects various devices, and even virtual processes and resources to meet service requirements [9].

IoT security is a significant issue because the increasing number of IoT devices connected to Internet also increases the amount of data that can be exposed, such as sensitive personal information and medical information, which may lead to problems directly related to peoples' lives. However, most of the devices operating in IoT environments have limited resources and use batteries. They have limited computing power and storage capacity to perform complex functions for security. Moreover, it is challenging to develop security technologies suitable for all IoT devices because the wireless access technologies used to connect these devices use low power, resulting in small data transmission and loss and delay due to the characteristics of wireless media. Therefore, lightweight security technology is a key requirement in IoT [10].

IoT attacks target IoT devices (thermostat, webcam, light bulb, etc.) in a network, but these attacks evolved into using these devices as platforms for distributing malicious codes or executing distribute denial of service (DDoS) attacks. Dyn, a domain name system (DNS) provider in the US, was a victim of a massive DDoS attack in 2016. The attacks were reported to be executed through IoT devices infected with the Mirai malware. This malware turns vulnerable IoT devices using factory default passwords into zombie devices for DDoS attacks [5]. Recently, various types of attacks targeting companies and individuals have been developed through ransom distributed reflection DoS (DRDoS) attacks using IoT devices. DRDoS attacks use normal Internet protocols, so it is difficult to respond to these attacks. There are also difficulties in identifying or tracking the attacker, the actual sender of the request message, because these attacks induce a response by sending a request message by spoofing the IP address of the system to attack.

In IoT, responsibility for managing the services and devices is not clear. Especially, such an unclearness can issue various security problems due to the absence of continuous software updates. For example, IoT devices in smart home services are expected to be used for at least a few years after purchase and installation. However, most IoT devices do not have proper user interfaces, making it very difficult for users to update periodic security patches. Targeting the default passwords on routers are common attack scenarios in IoT. If the target is an IoT device, these attacks become greater threats because they can directly manipulate home appliances. In addition, if security vulnerabilities are disclosed, attackers can easily find vulnerable devices with device search engines such as Shodan [5].

2.3 Door Lock Access Control System

To support security and safety of an authorized user, physical access control system (ACS) is widely used in various fields such as offices, homes, and industrial fields. Especially, door lock systems are commonly used for entrance control and video surveillance systems using CCTV or IP camera are used to monitor private and/or public areas necessary to support security and safety. The both systems are generally integrated into a single access control system to avoid the access conflicts in personalized monitored areas [11, 12]. Therefore, the integrated ACS can prevent an unauthorized entry of outsiders and monitor the space in real time at the same time.

In case of door lock of ACS, a user submits a password or PIN code to ACS as proof of being a legitimate user, and then the ACS verifies the password to determine entry. Hence, the password is the most important factor in determining the strength of the ACS security. That must include secure methods to generate, manage, and discard the password for the ACS. In recent years, additional authentication technologies such as RF card reader, finger print reader, face recognition, voice recognition and visible light communication (VLC) technologies have been deployed to further enhance security [11].

2.4 Voice Recognition Technology

This paper used voice recognition technology to verify users. The door lock combinations are sent to the users whose voice has been verified so that they can use the accommodation safely only during the sharing period. To implement the proposed technique, we used the Speaker Recognition feature provided by Microsoft Azure. The open Speaker Recognition API is a cloud-based API that provides algorithms to verify and identify speakers, and this paper used speaker verification among the various features.

To use this service, audio samples are recorded during the initial voice registration process to register the voice to the API service. This step is called “Enrollment”. After completing registration, you can use several voice recordings or phrases to test the service. After registration, the "Identification" step provides the corresponding speaker ID information stored in the data base (DB) and the IDs of other speakers (candidates) in the recognition step.

It compares the voice input with all speakers to determine whose voice it is and returns the speaker ID if it matches any enrolled profile. The Request Parameter must have the identificationProfileIds (the IDs of candidates) and may be displayed with a shortAudio option for short speeches. The Request Body must have the user's voice file to be verified. The audio file format is WAV, encoding (PCM), rate (16k), sample format (16 bit), and mono channel.

In addition to Microsoft Azure, cloud computing service providers, such as Google and Amazon, also provide speech or voice recognition features. Google only offers Cloud Speech-to-Text API, an artificial intelligence-based speech recognition system, and Cloud Text-to-Speech API service, which naturally synthesizes text into speech. Amazon offers Amazon Transcribe API, an automatic speech recognition (ASR) service. The main function of this service is also converting speech to text. Amazon Transcribe also recognizes when the speaker changes and attributes the transcribed text appropriately. In Korea, Naver and Kakao are providing speech recognition services. Naver's Clova and Kakao's Newtone provide STT and TTS

3. Proposed System

The system proposed in this article targets accommodation sharing services. To provide a secure service to both the provider and the user, the system issues a "Door-Lock One Time Password (DLOTP)" that is valid only during the sharing period reserved by the user, and when the sharing period expires, the password is changed, and access returns to the accommodation provider. That is, as shown in Figure 2, only the registered user has access during the sharing period after access grant for the sharing. Also only the provider knows the door lock password when the sharing period is over.

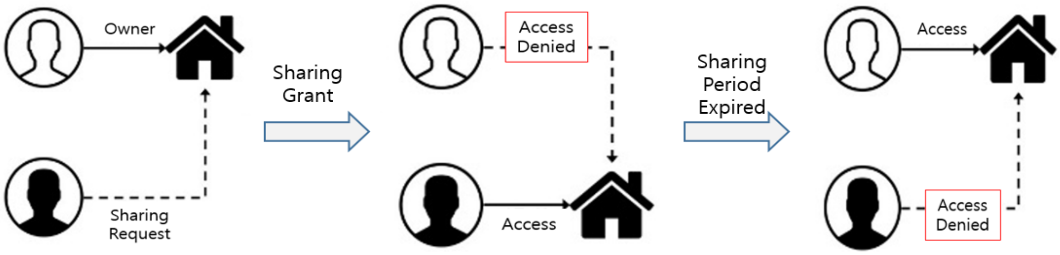


Figure 2. Conceptual model of the proposed scheme

The DLOTP used during the sharing period is issued based on the user voice verification and smart device-based mutual authentication. That is, the system provides enhanced security because the user needs to verify their voice and use a smart device for mutual authentication with the server to open the door look at the reserved accommodation. The length of the DLOTP can change depending on the application environment, and if it is a 4- to 6-digit number, the user can use the door lock keypad to enter the number. You can use a longer OTP for enhanced security and also QR codes for convenience.

3.1 Pre-Configuration and Speaker Registration

The proposed system uses speech verification for security purposes and to issue a temporary door lock password to use during the sharing period. The Speaker Recognition feature provided by Microsoft Azure was used to verify whether the user's voice is registered. The Speaker ID issued during the initial voice registration process is used as a value to identify the user during the sharing period. The speaker registration and verification process are as follows.

1) Register the user in the accommodation sharing service's member registration step and record the speaker's voice
2) Send and archive the recorded voice file via Microsoft Azure Speaker Recognition API
3) After registration, save the Speaker ID value issued by Microsoft Azure in the DB
4) The user records their voice through the Smart Phone Application for speaker verification
5) Send the recorded voice file via Microsoft Azure Speaker Recognition API
6) Microsoft Azure analyzes the voice file and returns the corresponding Speaker ID value
7) Compare the returned Speaker ID value with the Speaker ID value stored in the DB to determine if it is the same user
8) Issue and return a pre-shared key (PSK) that the system and the user's smart device can use through a separate channel (The separate channel uses SMS messages or e-mails to enhance security by using a different media than the communication channel used in the registration process).

3.2 User Verification and DLOTP Sharing

Various security services are required to cope with the security threats in accommodation sharing platforms. This paper focuses on a user authentication and access control scheme for the sharing resources. We developed the proposed authentication scheme based on the ISO/IEC 9798-1 standard [13]. The standard supports a mutual authentication scheme between devices based on symmetric keys, and is suitable for environments where lightweight devices such as smartphones and door locks are applied [13].

For mutual authentication to work safely in the proposed system, we need to set the user ID and obtain voice data. In the proposed system, the user ID can be either the Speaker ID generated during the speaker registration process or a smart device/user ID obtained during the membership registration process. The ID-based method must be able to counter reflection attacks, which should be considered in authentication and key agreement protocols (in other words, the IDs of user devices and door locks are registered, and mutual IDs are used in the authentication protocol to prevent unregistered devices from attempting reflective attacks). Figure 3 shows main procedures of the proposed authentication and access control system.

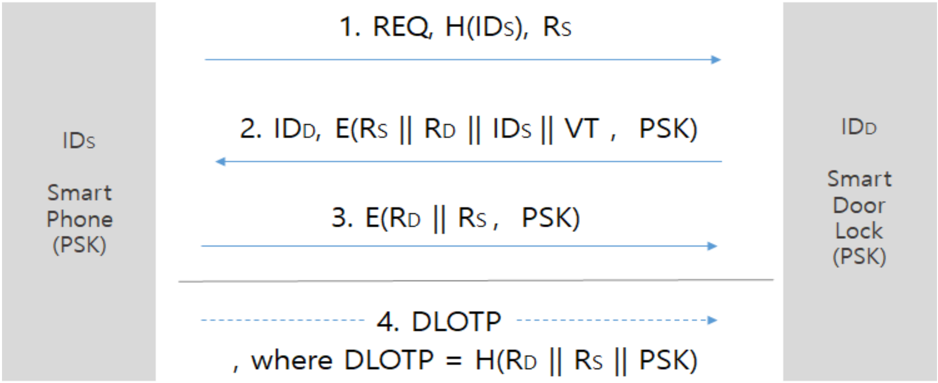


Figure 3. User authentication & DLOTP grant

(1) The smartphone of the user who is requesting authentication sends the hashed value of their ID and a

random number Rs as an authentication request initiation message to the smart door lock.

(2) The smart door lock encrypts its ID and message necessary for further transmission with the PSK and sends it. The additional message refers to the Rs sent by the smartphone, the random number RD generated by the smart door lock, User ID, and the valid time (VT) to use the DLOTP. The message format follows international standards.

(3) After receiving the message in step (2) above, the authentication requester uses the PSK to decrypt the password and authenticates the other party by confirming that the other party has a legitimate PSK by the random number sent from the received message and the random number and ID of the decrypted message. After that, to complete authentication, the random number generated by itself and the other party is concatenated and then encrypted with PSK and transmitted.

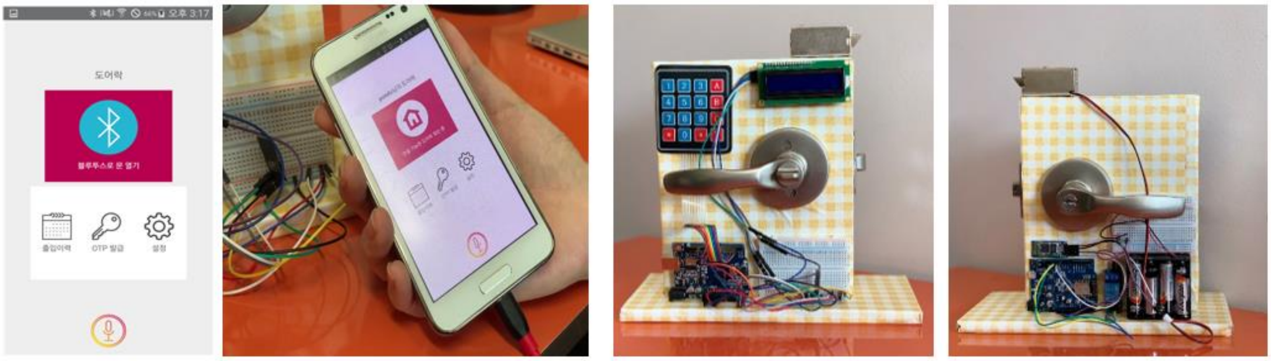
(4) Once step 3 is completed, the user can use the DLOTP safely during the VT period. The DLOTP is the result of hashing the concatenation of the two random numbers and PSK used above. For user convenience, you can use part of the hash value or the entire hash value by using a QR code.

(5) After the VT is over, the user's DLOTP is discarded, and the password is changed back to the combination set by the accommodation provider.

4. System Implementation and Analysis

4.1 Implementation and Testing

The smart door lock's authentication is implemented on the Raspberry Pi which is an open hardware development platform. And we utilize the Arduino to mechanically operate the door lock. Raspberry Pi and Arduino transmit messages using MQTT Protocol in consideration of their lightweight characteristics. The application implemented in the smartphone implements HTTP communication using Retrofit2.0 and sends and receives messages using the HTTP REST API implemented in Raspberry Pi. Figure 4 (a) shows the user interface implemented in the smartphone. And Figure 4 (b) shows the front side and rear side of the implemented smart door lock.

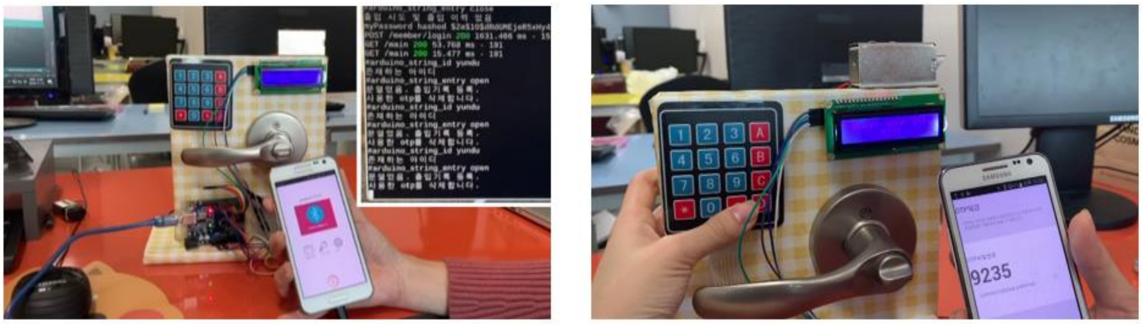


(a) User Interface for Smart Phone (b) Smart Door-Lock (Front) (c) Smart Door-Lock (Rear)

Figure 4. Implementation of the proposed scheme

Accommodation sharing users are issued DLOTPs to use during the sharing period, and even the owner cannot open the door lock installed in the space during this period. The proposed system verifies the user's voice before issuing DLOTPs for enhanced security. Figure 5 shows the test process for opening the smart door lock by showing the DLOTP issued to the user’s smartphone after the speaker verification process. For convenience, we have verified our test system using the first 4 numbers from the calculated hash result value.

The length of the DLOTP can be extended to increase security or camera features can also be used. The security elements of the proposed system are as follows.



```
#arduino_string_entry close
출입 시도 및 출입 이력 없음
myPassword hashed $2a$10$dRGGMEjeR5xHyd
POST /member/login 200 1631.466 ms - 15
GET /main 200 53.768 ms - 191
GET /main 200 15.477 ms - 191
#arduino_string_id yundu
존재하는 아이디
#arduino_string_entry open
문열었음. 출입기록 등록.
사용한 otp를 삭제합니다.
#arduino_string_id yundu
존재하는 아이디
#arduino_string_entry open
문열었음. 출입기록 등록.
사용한 otp를 삭제합니다.
#arduino_string_id yundu
존재하는 아이디
#arduino_string_entry open
문열었음. 출입기록 등록.
사용한 otp를 삭제합니다.
```

(a) Authentication & DLOTP Request (b) Opening the Door using DLOTP

Figure 5. Test result of the proposed scheme

- The main implementation technology is a two-factor authentication using two elements: speaker recognition and one-time password.
- Reduced risk of password loss and duplication by using speaker recognition technology to verify the user’s voice in addition to opening and closing conventional smart door locks by authenticating the set numeric combinations.
- Real-time visitor identification using camera features.
- Authenticated mobile devices can open the door lock via Bluetooth communication

4.2 Security Analysis

The proposed system allows both the provider and the user to use the accommodation space safely during the reserved period. The main threats in accommodation sharing take place because the provider knows the door lock password or if the user uses the password even after the sharing period. To solve these issues, the proposed system used a DLOTP that is only applicable during the sharing period and added user voice authentication so that the provider cannot open the door even if they know the password. That is, the system provides safe user access by merging the two elements of speaker recognition using voice and a one-time password to open and close the door lock.

The proposed system can respond to security attacks that may occur in mutual authentication of smartphones and door locks and DLOTP sharing technology in the following ways.

● Spoofing Attack

The proposed system uses wireless communication technologies such as Bluetooth or Wi-Fi to transmit messages between devices. In application environments that apply wireless communication, malicious attacks can be made by spoofing the messages sent between devices. If mutual authentication is not performed, malicious attacks can be launched by analyzing exposed radio frequencies. The proposed system prevents these attacks by mutual authentication and verifying the user’s voice. It means that the attacker must deceive the user voice authentication process and decrypt the encrypted random number to infer or acquire the DLOTP.

● Man-In-The-Middle Attack

Malicious attackers may exist between two devices in a wireless environment. The ID values of both devices can be exposed and intercepted by attackers, and then they can generate a random number and transmit it to the other device. In particular, replay attacks can happen after man-in-the-middle attacks if the message transmitted in authentication or key sharing technology is not changed. The proposed system encrypts transmitted data using a PSK and uses a random number that changes every time it operates in the encrypted messages to respond to man-in-the-middle attacks.

● Replay Attack

Attackers can eavesdrop on messages in a wireless network and resend them after a certain period. Even if an attacker makes replay attacks after a certain period, the authentication server in the proposed system can detect these attacks by checking the VT data. The proposed system also provides enhanced security by adding a user voice verification process before the authentication protocol. Furthermore, the devices initiating mutual authentication pass new random numbers to their counterparts every time to prevent replay attacks. The fresh time value can also be applied in the mutual device authentication and DLOTP generation process to enhance security.

4.3 Authentication Performance Analysis

This section analyzes the performance difference between the proposed system and previous authentication and secret key sharing technologies. Table 1 shows the performance differences, where we compared and analyzed the proposed scheme with two other authentication schemes for lightweight devices. As shown in the table 1, the proposed system uses only a symmetric key-based method and a hash function with small computational and memory requirements to authenticate and share DLOTPs on lightweight devices such as smart door locks. The ID-based approach tried to solve the computational overload associated with the certificate-based public-key method by using the IDs possessed by devices when there were multiple devices in the IoT environment. But the approach still requires a lot of computation to operate on lightweight devices. Smart home authentication can reduce the computational overload of lightweight devices using a symmetric key but is less efficient because it uses more communication and primitives than the proposed system due to authenticating devices using home gateways and intermediaries. The main abbreviations used in the table below are as follows.

- ENC: Encryption Function using Symmetric Key
- H: Crypto-Hash Function
- Voice REC: Voice recognition technology
- Setup: A function that takes security constants as input and outputs public parameters and master secret keys
- KeyGen: A function that calculates the inverse of the hash of the identification value ID using the master secret key and derives the signature key
- Prove: A public key-based function used by a prover with a private key
- Verify: A function that verifies the signature value in a public key-based approach

Table 1. Performance comparison

	Proposed System	ID-based approach [14]	Smart home authentication technology [15]
Key security primitives applied	Symmetric key-based encryption technology Hash technology (One-time speaker recognition technology)	ID-based signature using RSA	Symmetric key-based encryption technology
Communication between devices for authentication	3 way	3 way (based on canonical PI technique)	4 way + 2 way
Usage by password primitive type	2 ENC + 1H + Voice REC (Use DLOTP after 1 application)	Setup + KeyGen + Prove + Verify	4 ENC + 4 ENC

5. Conclusion

The accommodation sharing service market, such as Airbnb, has grown since 2008 with the spread of the sharing economy and the development of ICT technologies. At the same time, concerns about the safety and security of accommodation providers and users have also emerged as significant issues. Renting a house or room to someone whose identity is not guaranteed can be directly related to the safety of both the host and the guest. To address these issues, we proposed and implemented a system that allows both providers and users to safely provide and use sharing services by applying two authentication processes. Besides sharing services, our proposed system can also be applied to single-person households, dual-income households that need access security for children, and cases where the identity of visitors must be guaranteed (such as housekeepers or installation engineers). In addition to door lock passwords, the proposed system can enhance security by adding the registered user voice as an authentication factor and also provide extended features, such as applying longer passwords or using cameras for face recognition depending on stricter security policies.

Acknowledgement

This Research was supported by Duksung Women's University Research Grants 2020.

References

[1] Yun Seung Ko, “A Study on Sharing Economy of the ICT development,” The e-Business Studies, Vol. 15, No. 6, pp 77-100, DEC. 2014. DOI: http://dx.doi.org/10.15719/geba.15.6.201412.77

[2] Daniel Schlagwein, Detlef Schoder, and Kai Spindeldreher, “Consolidated, systemic conceptualization, and definition of the sharing economy,” Journal of the Association for Information Science and Technology, Vol. 71, No. 7, pp. 817-838, OCT. 2019. DOI: https://doi.org/10.1002/asi.24300

[3] Xiao Shuyang. "Research on the information security of sharing economy customers based on block chain technology," Information Systems and e-Business Management, Springer, Vol. 18, pp. 487-496, Dec. 2018.
DOI: https://doi.org/10.1007/s10257-018-0380-4

[4] Lim Eunjung, Shindo Mari, and Arita Shin, “A Korean-Japanese Comparison Research on Social Discussions about Accommodation Sharing Service: Using Network Text Analysis on Korean-Japanese Articles,” Journal of consumer policy studies, Vol. 51, No. 1, pp. 1-34, APR. 2020. DOI: http://dx.doi.org/10.15723/jcps.51.1.202004.1

[5] I-Deun Cho, Soo-Jin Park, and Namhi Kang, “Hacking Attacks and Countermeasures using Vulnerabilities of Lightweight IP Camera in Internet of Things,” Journal of Digital Contents Society, Vol. 20, No. 5, pp. 1069-1077, May 2019. DOI: http://dx.doi.org/10.9728/dcs.2019.20.5.1069

[6] Jeongin Kim and Namhi Kang, “Secure Configuration Scheme for Internet of Things using NFC as OOB Channel,” The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 16, No. 3, pp.13-19, May. 2016. DOI: https://doi.org/10.7236/JIIBC.2016.16.3.13

[7] Görög, Georgina, “The Definitions of Sharing Economy: A Systematic Literature Review,” Management (18544223), Vol. 13, No. 2, JUN. 2018. DOI: https://doi.org/10.26493/1854-4231.13.175-189

[8] Song Woon-Gang and Park Yongsook, “Study on the Regulations of Sharing Economy,” KANGWON LAW REVIEW, Vo. 55, pp. 353-401, OCT. 2018. DOI: https://doi.org/10.18215/kwlr.2018.55..353

[9] Ray Partha Pratim. "A survey on Internet of Things architectures." Journal of King Saud University-Computer and Information Sciences, Vol. 30. No. 3, pp. 291-319. 2018. DOI: https://doi.org/10.4108/eai.1-12-2016.151714

[10] J Park, H Kwon and N Kang, “IoT–cloud collaboration to establish a secure connection for lightweight devices,” Wireless Networks 23 (3), pp. 681-692, Springer, 2017.04. DOI: https://doi.org/10.1007/s11276-015-1182-y

[11] Yoon Sung Hoon, Lee Kil Soo, Mariappan Vinayagam, Young Ko Eun, and Woo Deok Gun and Kim Jeong Uk, “IoT Open-Source and AI based Automatic Door Lock Access Control Solution,” The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 12, No. 2, pp. 8-14 Apr 2020.
DOI: http://dx.doi.org/ 10.7236/IJIBC.2020.12.2.8

[12] Pradnya R. Nehete, J. Chaudhari and K. Rane, “Literature survey on door lock security systems,” International Journal of Computer Applications, Vol. 153, No. 2, pp. 13-18, 2016. DOI: http:/10.5120/ijca2016911971

[13] International Organization for Standardization, Gen`eve, Switzerland. “ISO/IEC 9798-1:2010, Information technology − Security techniques − Entity Authentication − Part 1: General,” Third edition, 2010.
DOI: https://doi.org/10.3403/00278828u

[14] Jieun Eom, Minhye Seo, Jong Hwan Park and Dong Hoon Lee, “Efficient ID-Based Authentication and Key Exchange Protocol,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 26 Iss. 6, pp. 1387-1399, Dec 2016. DOI: https://doi.org/10.13089/jkiisc.2016.26.6.1387

[15] So-Yeon Min and Jae-Seung Lee, “Device Mutual Authentication and Key Management Techniques in a Smart Home Environment,” Journal of Korea Academy Industrial Cooperation Society, Vol. 19, No. 10, pp. 661-667, OCT. 2018. DOI: https://doi.org/10.5762/KAIS.2018.19.10.661