

Home IoT device certification through Speaker Recognition

Dong-Gyu Shin*, Moon-Seog Jun*

*Department of Computer Science SoongSil University, Seoul, South Korea

nicesdg@naver.com, mjun@ssu.ac.kr

Abstract— IoT is a computing device, which identifies things in daily use and has the ability by mutual recognition of transferring data over a network. A home IoT device has a simple function to control things in the home environment. This has basic functions and a smaller interface than other IoT devices. For these reasons, security technology is often overlooked. If home appliances are operated by unauthorized voices, it is risky for home security. Therefore, introduction of security technology is urgent.

There are many security technologies in various fields that can be embedded into an IoT device. Among these technologies, biometric recognition technology is the best to be utilized. It can be expected to increase security and convenience by applying Speaker Recognition through this biometric recognition technology.

This paper illustrates voice recognition technology and the trend of security that also proposes a system to control functions of daily living in the home environment in which it is operated by an authorized user's voice key through the verification process of Speaker Recognition.

Keywords— Speaker Recognition, Home IoT, Biometric recognition

I. INTRODUCTION

According to Gartner's technology cycle curve, the interest level about Internet of things (IoT) technology reached its peak in 2014, and the placed second on the top 10 strategic technology trends that will lead 2015. In 2013 it is prospected that the Internet of things market will record about 3.8 trillion KRW, 22.9 trillion in 2022, and then the service related sales ratio will rise to 52.6% to lead the growth. Among these because home IoT (smart home) is ultimately 'a convergence of IOT in all daily necessities/devices necessary in private housing,' it is predicted that with the growth of IOT in 2015 it will see rapid growth.

Connecting and controlling in-home objects (Gas, light bulbs, boiler, refrigerator, TV, washing machine, etc.) is becoming the main issue with the rapid development of smart home technology, and while there is focus only on stable operation due to it being primary stages of development, there is no consideration at all in the security aspect. This and cause dangerous due to operations by users without permission. For example, if an IOT device that controls the gas valves are operated by a user without permission there can be dangers of gas leakage incidents. For this smart home devices need to be operated by authorized users not unspecified number of users.

The study suggests a security environment where only authorized users can control smart home devices by prior user registration and authentication applying voice recognition system.

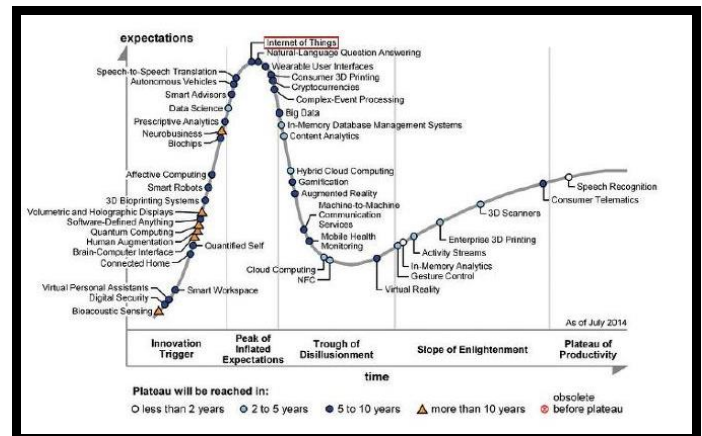


Figure 1. Gartner's technology cycle curve

II. RELATED STUDIES

A. Home IoT

Home IoT is where Internet of things is integrated into general devices necessary in private housing. It is an industrial field that has close relation with personal life and it can be said that it is a field that spans wide area that is related personal consumption. For Home IoT related industries there are such things as home network security, smart fusion devices / appliances, smart running, home health, green home building, home entertainment / home media, m2m intelligent communication, and for related sectors there are communications, appliances, security, education, medical health, energy, media, content, construction, and mobile and it is definitely a field that will have large influence on the overall growth of industry. Wired and wireless networks, smart devices, IoT communication standard, operating platform, control devices, and content which is called the six components of Home IoTs by default need to be organically combined for the appropriate use of Home IoT by the user. Among them, and the smart device sector there is active introduction of products in the manufacturing sectors and it is being approached with new ideas and various fields for the convenience of the users. Smart phone devices are essentially

based on communication and it can be classified into two forms one way communication and two-way communication.

Like in Table 1 one way communication generally consists of devices with the purpose of delivering and displaying information the device collected to the user, and two-way devices refer to devices that deliver information to the user by connecting with main devices in the home environment, where the user controls through device communication, where the user can control according to appropriate needs.

TABLE 1. ONE WAY AND TWO-WAY HOME IoT DEVICES CLASSIFICATION

Classification	Home IoT Devices
One Way	Gas meters, Electricity meters, smoke detector, Security Alarm
Two-Way	Room Temperature Control, Light Control, Gas Control, Security Control, Home Appliance Control

Input in two-way devices are done based on smart phones (smart devices) and makes the user recognize the transmitted information from the device by showing it on the display or LED. Among them the flow of basic control is composed of the structure where the control commands inputted into the smart phone through the Internet is delivered through the IP router to the IOT gateway system to operate the connected Home IoT devices.

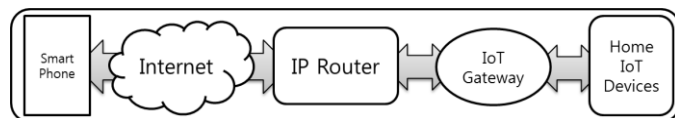


Figure 2. Existing Home IoT device control flowchart

In two-way smart devices there is the advantage that the user can monitor and control in real-time the information of the devices within the home whether they are outside or inside. In the future Home IoT system will be the term for two-way devices that enables control rather than the previous one way devices.

Home IoT devices are developing according to the user needs and it is being designed and developed so that various devices can be controlled in various environments. However the vulnerabilities and security following the increase in convenience is proportional. Especially because home environment devices have close relation with personal asset management in a society where individuals are becoming more important, the reality is that the security of Home IoT devices cannot be overlooked. As mentioned above Home IoT devices include products that have close relation with real-life such as lighting, gas, boilers, and waterworks. Malfunction or unauthorized user control of these devices causing dangers have close relation with personal assets and life.

The security measures to prevent these malfunctions and unauthorized operation are essential in Home IoT device control.

B. Home IoT security elements

There are various application methods to existing network and biometric security technology in Home IoT security elements, but because there is a limitation that it needs simple control and quick and accurate operation, it is in development to reduce procedures for users and maximize convenience.

TABLE 2. BIOMETRIC SECURITY TYPES AND CHARACTERISTICS

Classification	Features
Fingerprint Recognition	Fingerprint recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints.
Face Recognition	Face recognition uses the spatial geometry of distinguishing features of the face. It is a form of computer vision that uses the face to identify or to authenticate a person.
Speaker Recognition	Voice recognition or speaker recognition refers to the automated method of identifying or confirming the identity of an individual based on his voice.
Iris Recognition	Iris recognition refers to the automated method of identifying or confirming the identity of a subject by analyzing the random pattern of the iris.
Keystroke Dynamics	Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard.

Among various biometric security elements, voice recognition can be applied to disabling Home IoT device control for unauthorized users through authentication of the user through voice, and because it simply uses voice rather than complicated input method such as buttons or fingerprints, it is appropriate for Home IoT devices where convenience is important.

Voice recognition is a technology where the information about the speaker is extracted from the vocalized voice and generally it is divided into speaker identification and speaker verification

Like in Figure 3 speaker identification technology is a technology of finding the vocalizing speaker among the registered speakers through the input voice from any speakers. On the other hand like Figure 4 speaker verification technology is a technology that verifies if the speaking speaker is the speaker presented by determining if the voice is the voice of the presented speaker when particular speaker is presented.

Due to the limitation of the content of the voice inputted in these speaker identification and speaker verification methods, it is again divided into text-independent and text-dependent.

Text independent speaker recognition method is a method where there is no limitation in the form or type of text spoken for the verification or identification of the speakers. Thus the speaker recognition is done through input of voice composed of random form text. In text dependent speaker recognition method, speaker recognition is done only on vocalization of previously selected text.

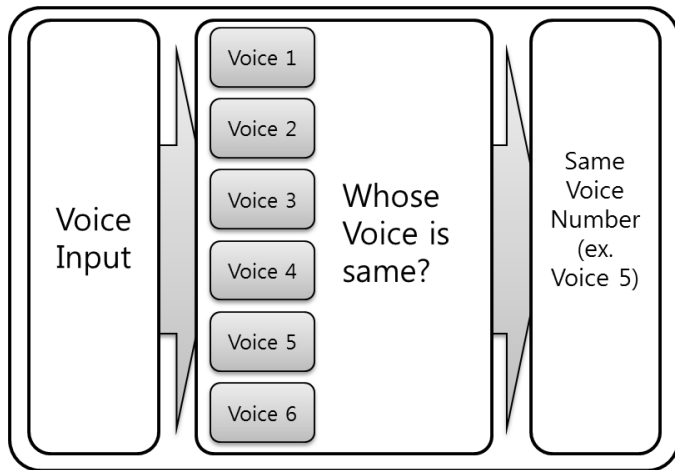


Figure 3. Speaker identification technology

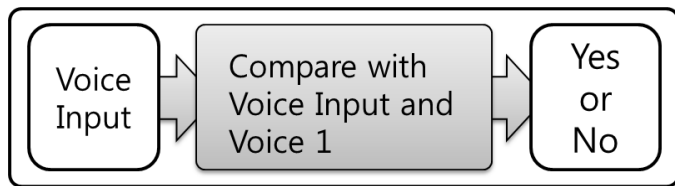


Figure 4. Speaker verification technology

III. HOME IoT DEVICE WHERE PROPOSED VOICE RECOGNITION IS APPLIED

The configuration can be largely divided into server part and device part.

The role of the server is as follows

- A. User preregistration
- B. User recognition
- C. Control command analysis

The role of the device is as follows

- A. Device command reception
- B. Device controlled then response

The overall structure of the Home IoT device control through user authentication applying to server and device that perform the above functions is divided into three steps. First in the user preregistration step, through device specific ID (DID) and personal identification number (PIN) implemented in production of the product, login is processed through smart phone application. When primary verification is done through login, the user goes through the process of registering his voice. It is inputted three times and through this the device stores voice information that matches the DID and PIN.

Second the user inputs his own voice commands into the smart phone. The inputted voice data is transmitted to the server and the server processes speaker verification. Voice of humans is a composite wave where various frequency components are combined in this sound wave is analyzed into various forms that can be seen by the eye through the sound spectrograph.

Through comparing this spectrograph, the three pre-inputted

voice data and the delivered voice data is compared to determine whether if it is a registered user. If it is not a user that is preregistered all of the voice data is committed and through the smart phone an error message is delivered. After verifying the registered user through the text dependent speaker recognition method, it is compared to the command set that exist on the database. For example for preregistered commands such as 'lights on' the user must know the command beforehand to vocalize it according to the content. Also it goes through the process where the result is delivered to the smart phone so that the user can confirm what they have inputted.

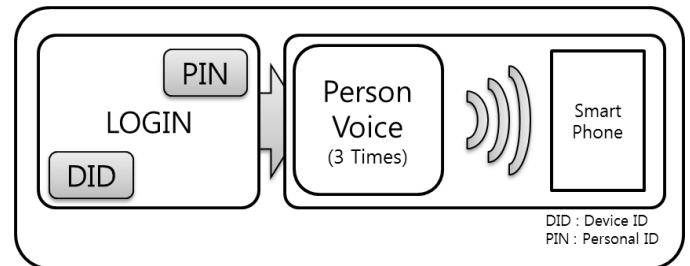


Figure 5. User preregistration

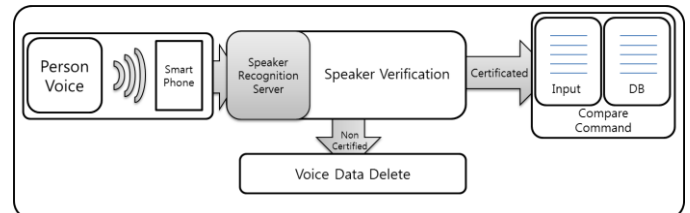


Figure 6. User recognition and command recognition through voice

Third is the step where the delivered command is received by the Home IoT gateway, where deep receive data is analyzed, then the corresponding device is operated.

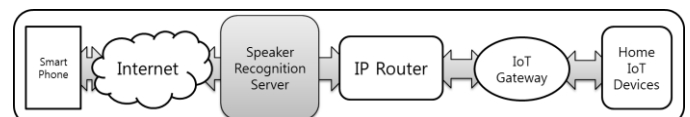


Figure 7. Home IoT device control through pre-certified commands

IV. CONCLUSIONS

To prevent control from unauthorized users of control devices in Home IoT, biometric security is being considered. Through voice recognition which is among one of them, the speaker can be recognized in advance and through analysis of corresponding commands only authorized users can control corresponding control devices at the same time with fast recognition rates high security can be expected.

ACKNOWLEDGMENT

This work was supported by the Soongsil University Research Fund.

REFERENCES

- [1] Gartner, Hype Cycles 2014 Research Report, Aug 2014
- [2] Carey, M. And Parris. E 'Speaker verification using connected words,' Proc. Institute of Acoustic
- [3] Smart Home(Home IoT) 6 Components, DigiEco Reports, 2014
- [4] Recently Speaker Recognition Technology Trends, The Magazine of the IEIE 2014
- [5] 'CT in-depth reports' Korea Creative Content Agency, Feb 2011
- [6] Voice Personal Identification Physics and high-tech April 2006
- [7] NIST Speaker Recognition Evaluation is available
<http://www.itl.nist.gov/iad/mig/test/sre/2008/>
- [8] <http://www.biometric-solutions.com/solutions/index.php>



Dong-Gyu Shin received his B.S. degree in Computer Science from Baekseok University, Cheonan-si, Korea in 2004, and his M.S. degree in Computer Science from Soongsil University, Seoul, Korea in 2006. He is a researching in Ph.D. Course of Soongsil University since 2006. His research interests Secure Communication and Information security and Smart Device Security and IoT Security.



Moon-Seog Jun received his B.S. degree in Computer Science from Soongsil University, Seoul, Korea in 1981, and his M.S. and Ph.D. degree in Computer Science from University of Maryland, Maryland, United States, in 1986 and 1989, respectively. He has been lecturing Computer Science in Soongsil University since 1991. His research interests information security and PKI and cryptography.