Pusat Pengajian Sains Kuantitatif
SCHOOL OF QUANTITATIVE SCIENCES (SQS)
Universiti Utara Malaysia

IACE' 2016
https://sites.google.com/site/sqsiace/

The 3rd Innovation and Analytics Conference & Exhibition (IACE) 2016
31 October-1 November 2016, Sintok, Kedah, Malaysia

Biometric Fingerprint Architecture for Home Security System

Apri Siswanto*[a,b], Norliza Katuk[a], Ku Ruhana Ku-Mahamud[a]

[a]*School of Computing, Universiti Utara Malaysia, Malaysia*
[b]*Teknik Informatika, Fakultas Teknik, Universitas Islam Riau, Indonesia*

Abstract

Home security system is an emerging technology that gained much attention recently by homeowners. The conventional hardwired system is easy to install in newly developed homes; however, the existing homes require complex configuration of such systems which involves substantial cost. Hence, a wireless home security system has been an alternative to the hardwired. This paper describes a simple home security system that is implemented using fingerprint biometrics technology. The system is known as BIOmetrics FIngerprint for Home Security (BIOFIHS). BIOFIHS is demonstrated using a prototype that consists of hardware and software components. The hardware includes fingerprint sensors, a microcontroller, a wireless network router, an application server, and a smartphone. For the software, a program is developed to record the fingerprint data and to verify the data on the remote server. All of the components are connected to the home network wirelessly that makes the system easier to implement with cheaper costs.

Keywords: Biometric techniques, fingerprint verification, smart home, home security, home network

1. INTRODUCTION

The development of information and communication technology (ICT) currently offers convenience to the users, and it improves various aspects of human life. The technology includes smart home which is also referred to as smart house or home automation. The smart home had emerged and developed since the 1960s when the first home automation processing device named Echo IV was designed. The machine, a private venture by a Westinghouse engineer, was designed to control home temperature and turn on the appliances at home (King, 2015). Meanwhile, Smart House term was first coined in 1984 by the American Association of house builders (Aldrich, 2003). Next, in 1994, BESTA Norway started the project, namely Smart Home technology for elderly housing (Faanes, 2014). However, until the year 2000, the concept of smart home has not been too popular in the community. The discussion of smart home becomes intense in late 2013 as the technology attracted attentions of many homeowners.

Current smart home technology allows homeowners to connect various electronic devices in the house to an integrated system that is accessible through a smartphone or other gadgets. The smart home also provides a system that authenticates homeowners to get access to the building for increasing the home security. It aims to

* Corresponding author. Tel.: +604-9285063; Fax: +604-9285067
E-mail: aprisiswanto@eng.uir.ac.id

improve the quality of life and safety of its occupants. According to Robles and Kim (2010) smart home is the term used for authenticating the residence using the control system that is integrated into a home automation system. The system allows electronic control for the homeowners with only a few buttons that are connected to the simple telecommunications system. Smart home includes communications, entertainment, security, and information systems.

Although smart home provides home automation features, many homeowners are not yet ready to go for it. It is due to the reason that designing and installing a hardwired smart home system is expensive and inconvenience especially in existing occupied homes. Hence, a simple and cheaper alternative is needed. Wireless smart home system is one of the solutions to overcome the issue. Unlike the hardwired system, the wireless smart home offers a simpler installation process and cheaper in costs. It is expected that the wireless system can provide homeowners with the similar functionalities and experience as the hardwired do. In line with this, the paper focuses on the home security as part of the overall smart home system.

The paper is organized in the following way. Section 2 of the paper discusses the related work from the literature. Then, Section 3 presents the architecture of the proposed system. Finally, Section 4 concludes the paper.

2. SMART SMART HOME AND SECURITY

A smart home system offers an automated mechanism for monitoring and controlling the home temperature, multimedia devices, windows, doors, alarms and others through a computer-based system (Bregman, 2010). The automated mechanism for monitoring and controlling the doors, windows and alarms is part of home security system that protects the residents from danger or threat of criminal acts or other unexpected events that disturb their privacy and safety. The system may use a numerical code such as a password, a personal identification number (PIN) and passphrases, security tokens like smart card, and biometric authentication methods for home authentication and access (Ishengoma, 2014).

Numerical codes and security tokens are considered as the common authentication method, and they have been used for this purpose for a quite a long time. Utilizing the unique features of human body parts, biometric technology is now an emerging trend for authentication. The technology can be defined as automated methods for recognizing human individually based upon one or more unique parts of their body or behaviours. It includes fingerprint recognition, retina, iris, face, and signature and keystrokes dynamics as shown in Figure 1.

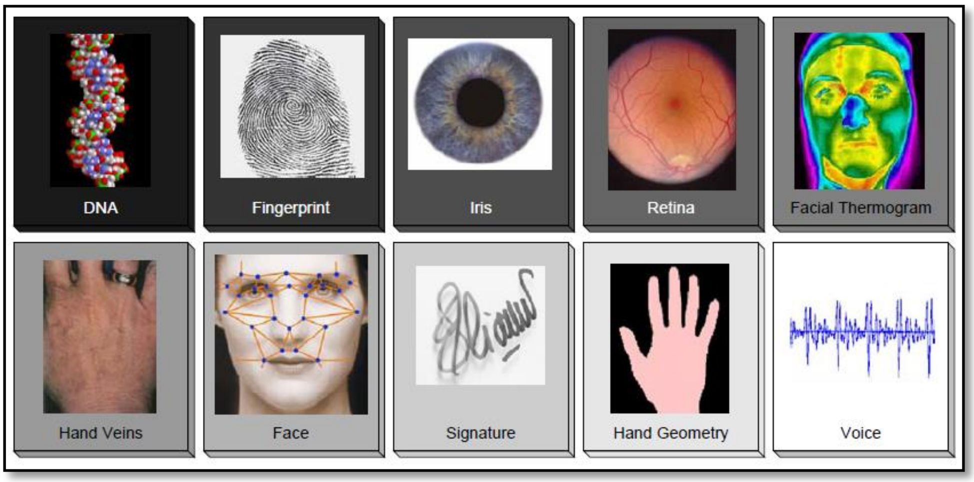

Figure 1. Different biometric attributes

Among the listed unique human body parts, the fingerprint is the most frequent part used for authentication. It is implemented through fingerprint recognition technology (FRT) that compares the pattern of human fingerprints to identify a person. In the context of home security system, the fingerprint can be used by the home residents for authorizing access to the house and unlocking the door or other main entrances. Since the fingerprint is unique, access to the house will only be permitted to the authorized residents only. This mechanism protects the residents and the house from being accessed by an unknown person.

To date, there are many studies have been conducted in the field of fingerprint and smart home. Zhou, Huang, and Zhao (2013) presented the architecture of smart home management system by developing an Android-based application that connects to a smart gateway, smart jacks, and smart interview terminal. The system had a reasonable structure, easy expanding, and satisfying the need of smart home management. The system supports common communication protocols, and as well as running on different devices. The results of their experiment suggested that the system is stable and easy to operate. Khiyal, Khan, and Shehzadi (2009) focused on controlling household appliances against tampering and providing security protection to the home when the occupants are away from the place. The occupants can control the household appliances through short message service (SMS) and they will also receive notification when intrusion or security breaches occur. Kaur (2010) designed a microcontroller-based home automation system which focusing on the home security. The home security comprised of a password based locking system, an automatic switching system, a temperature controlled cooling system, a lighting system, and fire and smoke sensors. Gangi and Gollapudi (2013) implemented a locker security system that used fingerprint, password and GSM technology for activating the locking system. The system authenticates and validates the user, then unlocks the door in real time for the locker secure access.

Afolabi and Alice (2014) Proposed a design door security system with a fingerprint sensor SN-FOR-UART and microcontroller PIC16F648A. Microcontroller is used to controls all of the door security system. An LCD status display is employed to show the operating status of the system. A door movement mechanism is used in the design to make the automated door system move in clockwise and anti-clockwise direction, then fingerprint input stage was implemented using the SN-FPR-UART. The development of system guarantees security for illegal intrusion into any entity to the room , the mechanism can be implemented in a broader sense of a door where there is restriction of access. But in this system there is no mechanism for home monitoring (shown fig 2a). Tobing (2014) made fingerprint security systems consisting of several components, the first component is input part in the form of multiple sensors, then the second is unit processors part (using ATMega8) as the main controller, and the third is output part , this section is controlled by the microcontroller. Output functions are for interacting with humans, while the last is part of the supply voltage and current to the system. The system will also be equipped with a buzzer that will sound in the event of certain defined conditions. besides this security system can also be controlled via the installed android smartphone application designed by the author (shown fig 2b). However previous proposed system no system is using wifi network technology, as discussed in this paper.

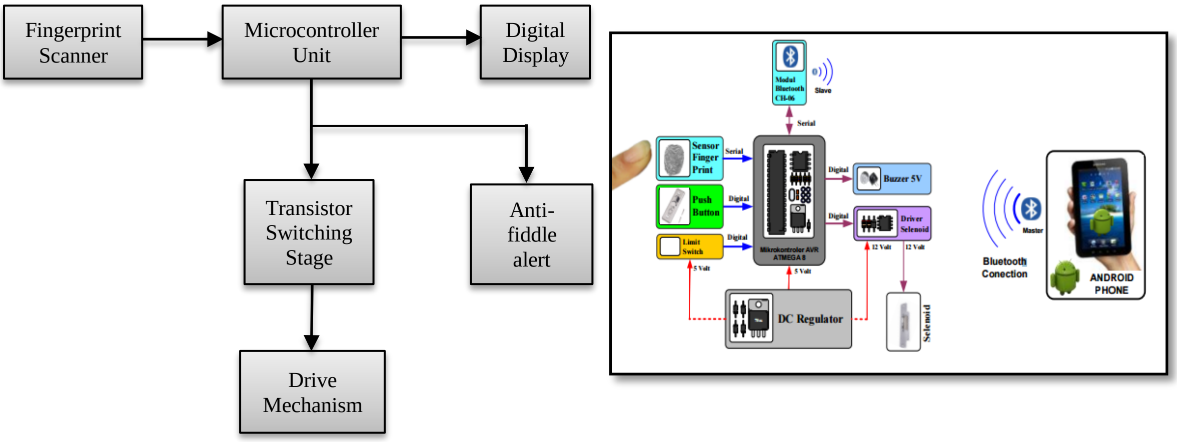

figure 2a

figure 2b

Figure 2. Past design architecture of Fingerprint for smart home door lock

3. THE PROPOSED ARCHITECTURE

This section explains the proposed architecture of biometrics fingerprint for home security (BIOFIHS). The components of the architecture are fingerprint sensors, a microcontroller board, wireless network router, an application server, connection to the Internet, and a smartphone. Figure 2 illustrates the architecture of BIOFIHS with its components.

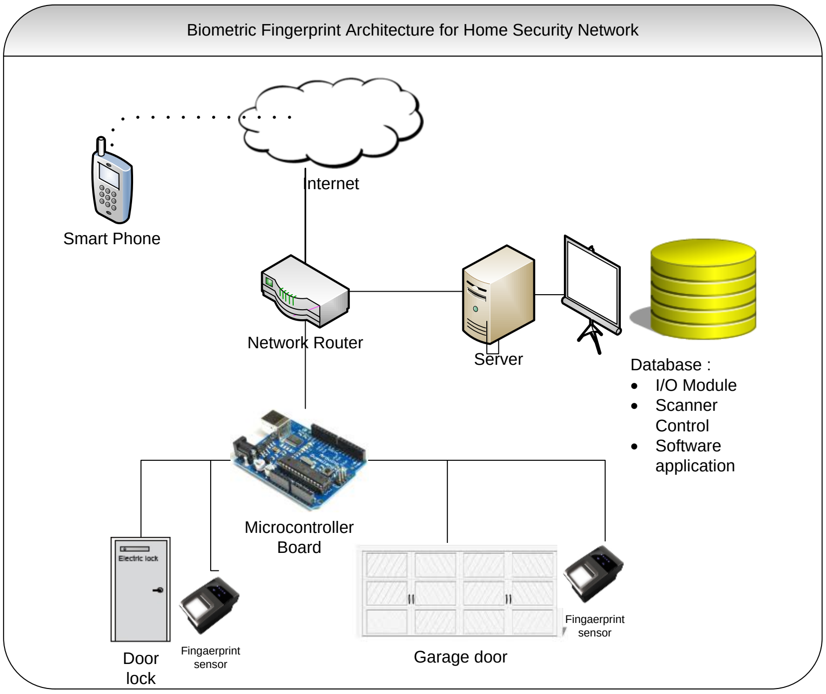

Figure 3. BIOFIHS Architecture

The function of each component is explained below:

(1) The fingerprint sensors serve as a sensor that receives images of fingerprints. The sensor produces digital data to create a biometric template and stores the data in the database for the first time and an input device for authenticating the fingerprints later.
(2) The microcontroller board serves as the hub of the systems and regulates all input and output activities. It retrieves data from the fingerprint sensors, and then processed, stored in the memory and communicates with the server through the network.
(3) The wireless network router forwards the data from the microcontroller board the server and vice-versa.
(4) The server processes the input and output data and runs the home security application.
(5) The smartphone is used for controlling and monitoring the house via a remote network.

The study intends to implement BIOFIHS at the main door of the house and the garage. When BIOFIHS is implemented at home, the authorized occupants are required to register their fingerprint data with the application stored on the server. The occupants scan their fingerprints using the fingerprint sensors. The result of the scanning is stored in a digital format at the server. After that, the fingerprint records are processed by producing a list of unique pattern features. The fingerprint pattern features are stored in the database. When the occupants scan their finger, the pattern produced from the fingerprint will be matched with the one stored in the database. If the both data match, then the server sends approval signal to the microcontroller for unlocking the door and grant access to the occupants. The flowchart in Figure 3 shows the flow of the process. An additional feature is also included where the system can be controlled remotely via smartphone. Notifications will also be sent to the occupants via the smartphones if intrusions of security breaches occur.

Biometric fingerprint system provides a good solution to home security. A novel architecture of technology cost-effective biometric fingerprint proposed in this paper. It gives a basic idea of how to integrate a door lock, fingerprint sensor, microcontroller, network routers, and smart phone based on wireless network. As a trend on the biometric security system, that arhitecture will require implementation in real systems so that these systems can provide better benefits. In the future will be created for the design of hardware and software to see the ability of this system to secure the house. The author predicts this architecture is very economical.

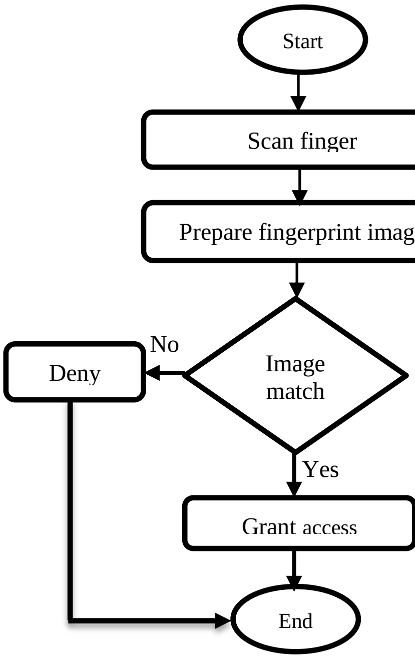

Figure 3. The process of BIOFIHS

4. CONCLUSION

The use of biometric fingerprint for home security system using wireless network can be one of alternative for home security that is reliable and convenient. In addition, the components of that are used relatively inexpensive and widely available on the market. It is expected that BIOFIHS using wireless network provides similar functions as the hardwired system.

5. ACKNOWLEDGEMENT

This work was supported by Ministry of Higher Education, Malaysia under the Trans-Disciplinary Research Grant Scheme (Ref: TRGS/2/2014/UUM/01/2/1, UUM S/O Code: 13164).

6. REFERENCES

Afolabi, Adeolu Olabode, & Alice, Oke. (2014). On Securing a Door with Finger Print Biometric Technique. *Transactions on Machine Learning and Artificial Intelligence, 2*(2), 86-96.

Aldrich FK. (2003). Smarthomes: past, present and future. In: Harper R (ed) Inside the smart home. Springer, London, pp 17–39

Bregman, D. (2010). Smart Home Intelligence - The eHome that Learns, International Journal of Smart Home 4(4), 35–46.

Faanes, E. K. (2014). Smart Cities - Smart Homes and Smart Home Technology, Master Thesis. Norwegian University of Science and Technology, Trondheim-Norwegia

Gangi, R. R., & Gollapudi, S. S. (2013). Locker Opening And Closing System Using Rfid , Fingerprint , Password And Gsm. International Journal of Emerging Trends & Technology in Computer Science, 2(2).

Ishengoma, F. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. Programmable Device Circuits and Systems. Retrieved from http://www.ciitresearch.org/dl/index.php/pdcs/article/view/PDCS072014002

Kaur, I., (2010). Microcontroller Based Home Automation System With Security, International Journal of Advanced computer Science and Applications 1(6), 60–65.

King, L. (2015, June 10) The evolution of the smart home. Retrieved from http://raconteur.net/technology/the-evolution-of-the-smart-home

Robles, R. J., & Kim, T. (2010). Applications , Systems and Methods in Smart Home Technology : A Review International Journal of Advanced Science and Technology , 15, 37–48.

Sikandar, M., Khiyal, H., Khan, A., & Shehzadi, E. (2009). SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security Preliminaries Home Appliance Control System (HACS), 6.

Tobing, Sandro Lumban. (2014). Rancang Bangun Pengaman Pintu Menggunakan Sidik Jari (Fingerprint) Dan Smartphone Android Berbasis Mikrokontroler Atmega8. *Jurnal Teknik Elektro Universitas Tanjungpura, 1*(1).

Zhou, C., Huang, W., & Zhao, X. (2013). Study on Architecture of Smart Home Management System and Key Devices. IEEE International Conference on Computer Science and Network Technology, 2–5. http://doi.org/10.1109/ICCSNT.2013.6967330