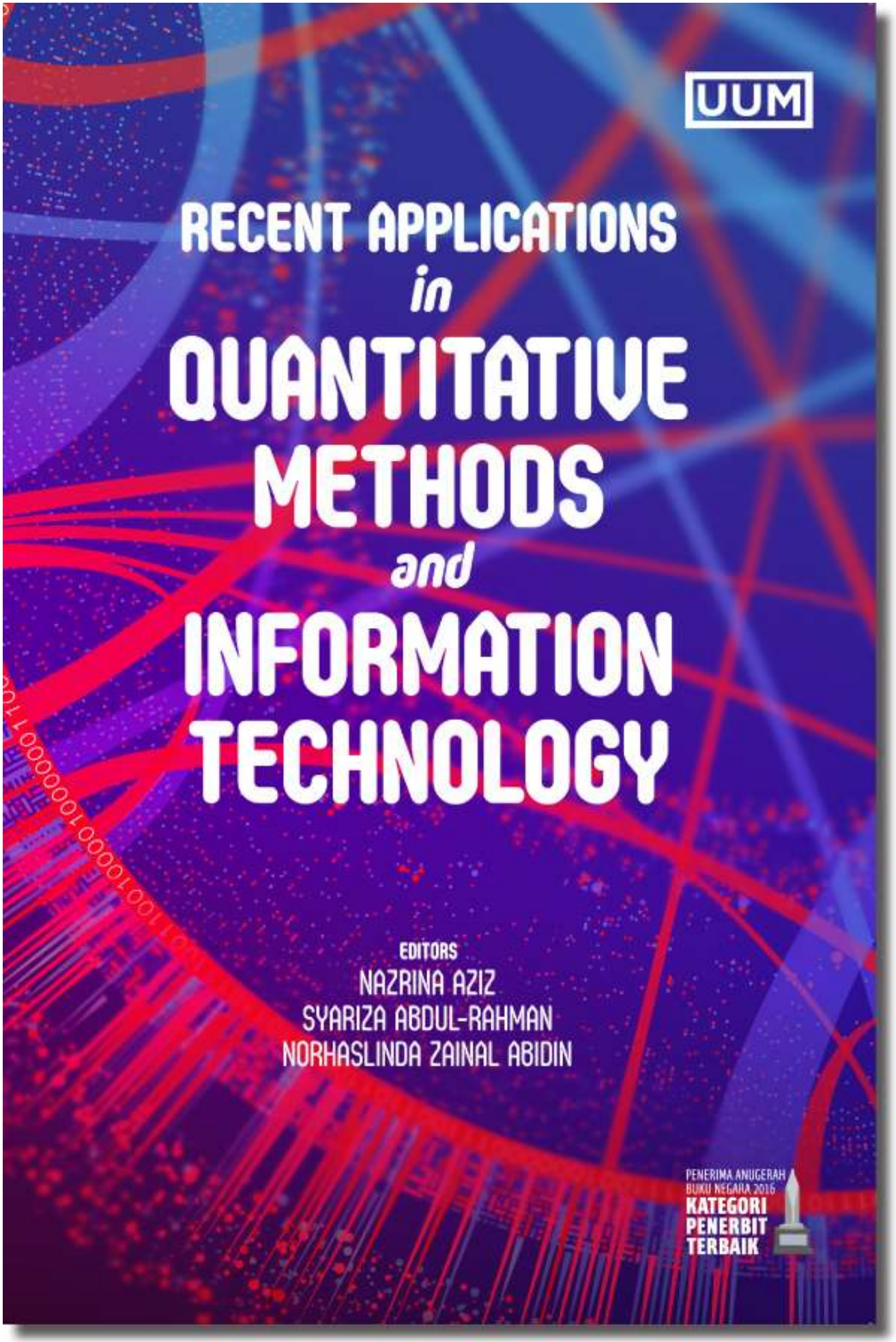

UUM
RECENT APPLICATIONS
in
QUANTITATIVE
METHODS
and
INFORMATION
TECHNOLOGY
EDITORS
NAZRINA AZIZ
SYARIZA ABDUL-RAHMAN
NORHASLINDA ZAINAL ABIDIN
PENERIMA ANUGERAH
BUKU NEGARA 2016
KATEGORI
PENERBIT
TERBAIK

1

An Architecture For Home Security System Using Biometric Fingerprint

Apri Siswanto, Norliza Katuk and Ku Ruhana Ku-Mahamud

1.1 INTRODUCTION

Security is one of the factors to consider in buying a new home. The smart home is an emerging technology that offers convenience to the users, and it improves various aspects of human life including the home security. It is 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.

The functionalities of Smart Homes are (Blanson Henkemans, Alpay, and Dumay, 2010):

1. Monitoring of measurements (for example meal intake, motion, and other activities of daily living, whereby critical situations are detected;

2. Security monitoring and assistance of domestic threats (intruders). Assistance includes notification of external relevant actors;

3. Safety monitoring and assistance of environmental hazards (for example, fire or gas leak). Assistance contains automatic turning on and off bathroom lights when getting out of bed and facilitating safety by reducing trips and falls;

4. Physiological monitoring of physiological measurements (for example temperature, pulse, respiration, and blood pressure, as well as blood sugar level);

5. Social interaction monitoring and assistance of social interactions (e.g., phone calls, visitors, and participation in activities). Assistance includes technologies that facilitate social interaction (e.g., video-based components that support video-mediated communication with friends and loved ones and virtual participation in group activities);

6. Cognitive and sensory assistance of automated or self-initiated reminders and other cognitive aids for users with identified memory deficits (e.g., medication reminder and management tools, lost key locators). Aids include task instruction technologies (e.g., verbal instructions in using an appliance) and aids for sensory deficits (e.g., sight, hearing, and touch).

Current smart home technology promotes security and green living. One term that is often used is sustainable smart home that ensures a minimum energy consumption from the electrical appliances in the house. The rapid development of mobile technology allows homeowners to connect various electronic appliances in the house to an integrated system that is accessible through a smartphone or other gadgets. The appliances

include lights, thermostat, coffee machines, refrigerators, washing machines, televisions, multimedia systems, and video surveillance (Hendricks, 2014). The high level of automation enables comfort, control and security of any part of the property.

Building smart homes needs integration of different computing technologies, such as ubiquitous computing, context-aware computing or home automation technology (Vilas et al., 2010). Unlike desktop computing, ubiquitous computing is carried out using any device, in any location, and in any format. It supports automatic interactions among residents, computer-equipped devices, and the home environment which lead to an intelligent home automation system.

Home automation systems have the following advantages (Puri & Nayyar, 2016; Vinay Sagar & Kusuma, 2015) :

1. User convenience: Electrical devices and appliances can be controlled without the need to physically close to them, all the instructions can be given via smartphones and users can sense relaxed and full comfort.
2. Security: Home automation system provides biometric security systems and surveillance via video CCTV or webcams which can be accessed from anywhere and everywhere through the Internet.
3. Flexible control: Electrical devices and appliances can be controlled remotely from anywhere.
4. Cost effectiveness: Smart sensor technology will turn off appliances or devices when it is no longer being used. It helps in energy-saving.

The smart home also provides a system that authenticates homeowners to get access to the building for increasing the home security. It aims to improve the quality of life and safety of its occupants. The system allows electronic control of the house for the homeowners with only a few buttons that are connected to the simple telecommunications system.

Although smart home provides home automation and security 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.

1.2 SMART HOME SECURITY SYSTEM

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. The utilization of the unique features of human body parts has made the biometric technology an emerging trend for authentication. Biometric systems use human features to allow access to authorized people only. Individuals that have entered their unique feature in the database for identification are allowed access only. 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.

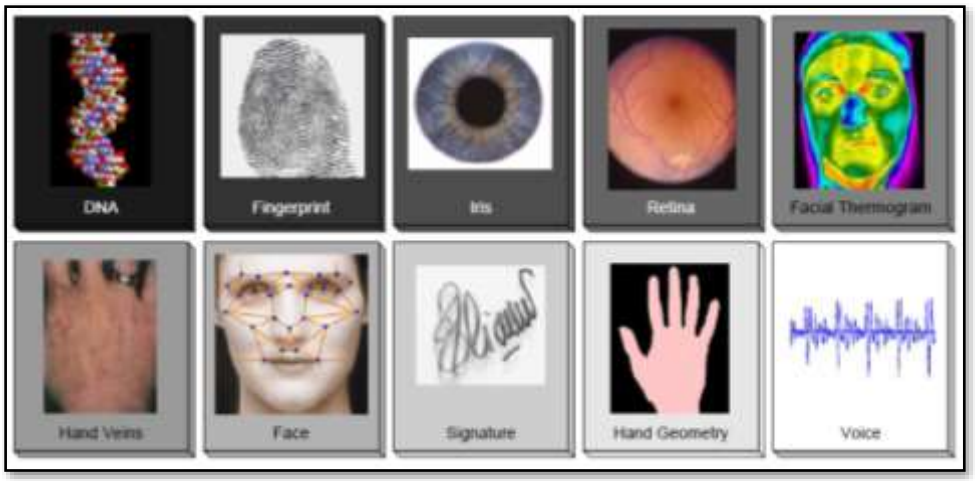


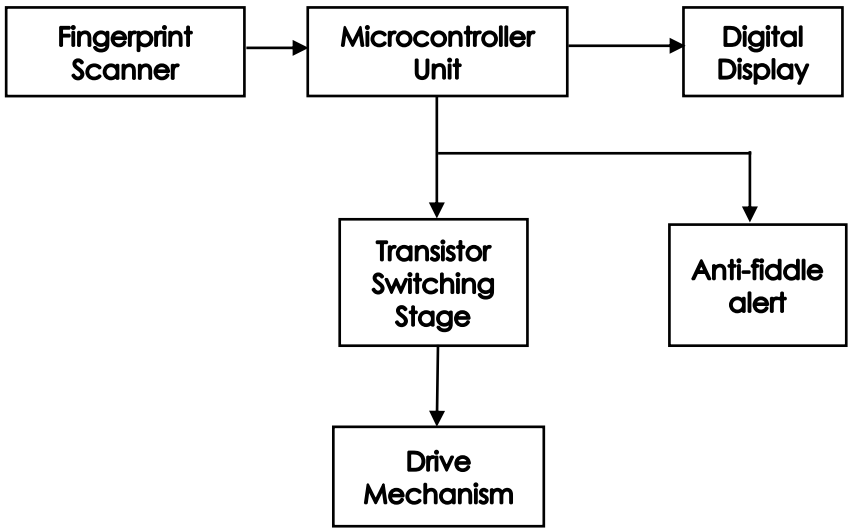
Figure 1. Different biometric attributes

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.

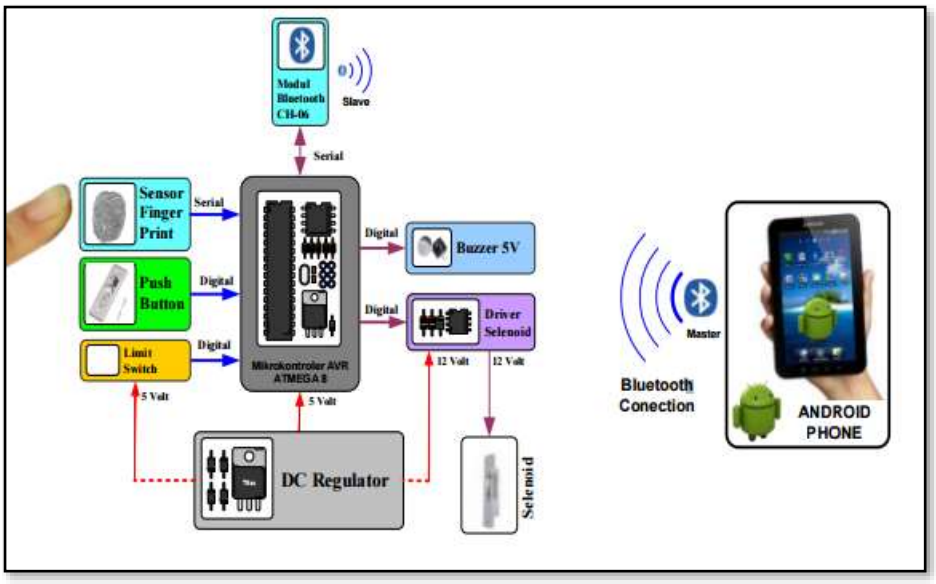
To date, there are many studies have been conducted in the field of fingerprint and smart home. Zhou, Huang, and Zhao (2013) presented the architecture of smart home management system by developing an Android-based application that connects to a smart gateway, jacks, and interview terminal. The system 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 disruption 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 temperature controlled cooling system, an automatic switching system, a password based locking 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 for a door security system with a fingerprint sensor and a microcontroller. The microcontroller is used to control 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 also used in the design to make the automated door system moves in clockwise and anti-clockwise directions. The fingerprint input stage was implemented using the fingerprint sensor. The development of the system guarantees the home security from illegal intrusion. However, the system has no mechanism for home monitoring. Figure 2(a) shows this architecture. Tobing (2014) designed a fingerprint security system consists of several components such as multiple sensors, a processor unit, an output unit for interacting with humans, and the supply voltage and current to the system. The system can also be controlled via a smartphone application. Figure 2(b) shows the architecture of Tobing's work.



(a) Afolabi and Alice (2014)



(a) Tobing (2014)

Figure 2. The architecture of the existing fingerprint security systems

1.3 The Proposed Architecture

This section explains the proposed architecture of biometrics fingerprint for home security known as 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 3 illustrates the architecture of BIOFIHS with its components.

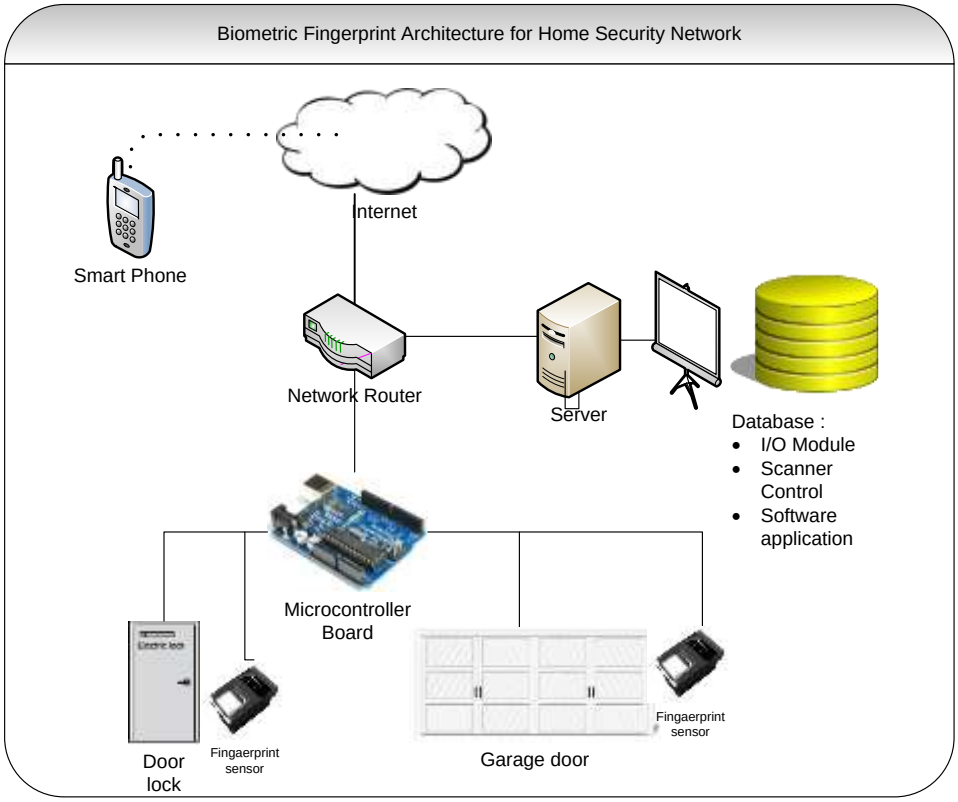


Figure 3. BIOFIHS Architecture

The definition and function of each component are explained below:

1. The fingerprint sensor is an electronic device for capturing a digital image of the fingerprint pattern. It produced an image called a live scan that is digitally processed to create a biometric template. When the first time users use the fingerprint sensor, it produces digital images data to create a biometric template and stores the data in the database. This is known as an enrollment process. Later, when the users scan their finger using the sensors, the fingerprint image will be compared with the one stored in the database. This process is known as verification. The combination of enrollment and verification represents the biometric authentication process. Both enrollment and verification processes are rendered in Figure 4.

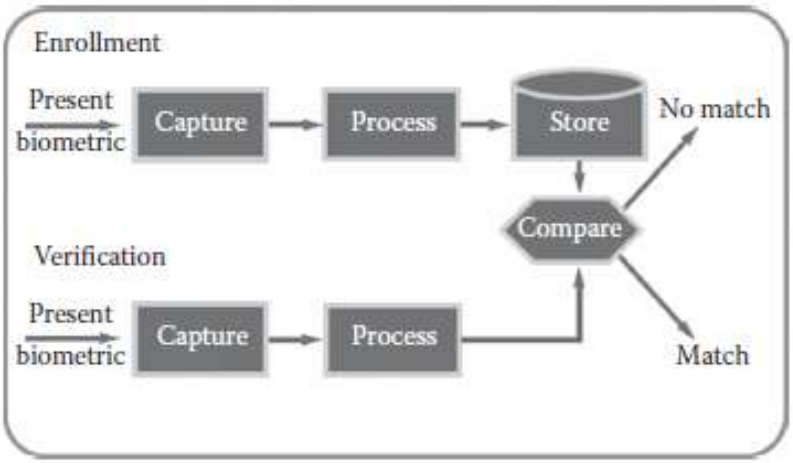


Figure 4. The process of biometric authentication

2. The microcontroller board is a small computer that can be used to make decisions, do things that are repetitive, and can interact with external devices such as sensors, LCD Display, and a motor for control purpose. It serves as the hub of the system and regulates all input and output activities. It retrieves data from the fingerprint sensor, processes and stores them in the memory. It also communicates with the server through the network.

3. The wireless network router forwards the data to the server from the microcontroller board and vice-versa.

4. The server processes the input and output data and runs the home security application.

5. The smartphone controls and monitors 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 5 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 or security breaches occur.

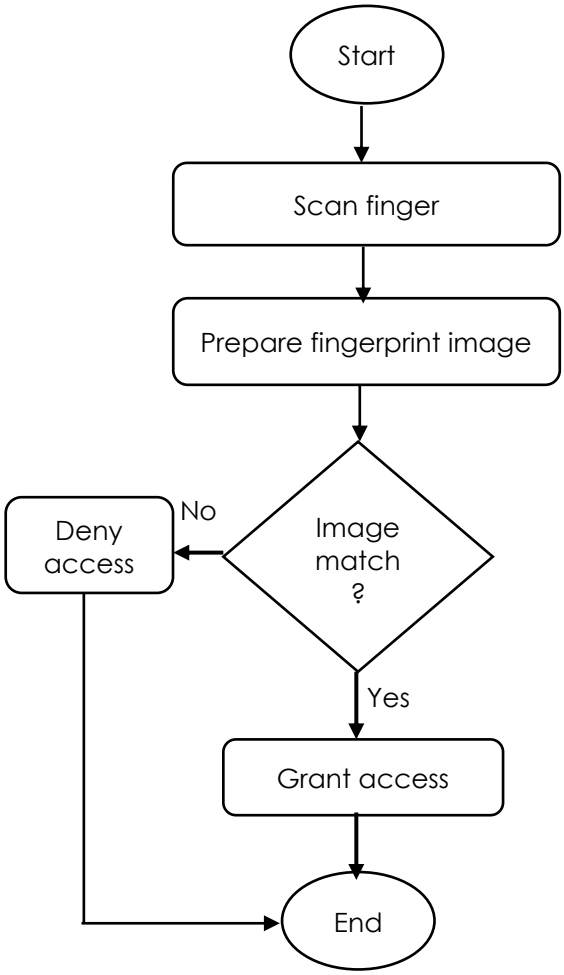


Figure 5. The process of BIOFIHS

A client-side and server-side algorithms have been developed to show the basic authentication process. The process is divided into the enrolment and verification.

The client-side algorithm for the enrolment process.

```
User scans finger using sensor;
Capture fingerprint image;
Extract fingerprint image;
Create fingerprint template;
Send fingerprint template to the server for enrolment;
```

The server-side algorithm for the enrolment process.

```
Receive fingerprint template from sensor;
Store fingerprint template in the database;
```

The client-side algorithm for the verification process.

```
User scans finger using Sensor;
Capture fingerprint image;
Extract fingerprint image;
Create fingerprint template;
Send fingerprint template to the Server for verification;
```

The server-side algorithm for the verification process.

```
Receive user fingerprint template from sensor;
Compare user fingerprint template with existing data in the
database;
if (user fingerprint templates match) {
     open door;
else
     display warning;
}
```

Biometric fingerprint system provides a good solution to home security. The architecture of a cost-effective biometric fingerprint system has been proposed in this chapter. It gives a basic idea of how to integrate a door lock, fingerprint sensor, microcontroller, network router, and smart phone based through a wireless network. The arhitecture requires real-world implementation so that these systems can provide better benefits.

1.4 CONCLUSION

Instead of a wired network, the wireless network can be used to create a home security system with biometric fingerprint for the existing homes. It provides home security that is more cost effective and convenient because the components are relatively inexpensive and widely available on the market. It is expected that BIOFIHS using wireless network provides similar functions as the hardwired system.

1.5 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).

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, Frances K. (2003). Smart homes: past, present and future *Inside the smart home* (pp. 17-39): Springer.

Blanson Henkemans, OA, Alpay, LL, & Dumay, ACM. (2010). Aging in place: self-care in smart home environments. *Smart home systems. Olajnica: In-Tech*, 105-120.

Bregman, David. (2010). Smart Home Intelligence–The eHome that Learns. *International journal of smart home, 4*(4), 35-46.

Faanes, Erlend Kydland. (2014). Smart Cities-Smart Homes and Smart Home Technology.

Gangi, Raghu Ram, & Gollapudi, Subhramanya Sarma. (2013). Locker opening and closing system using RFID, fingerprint, password and GSM. *International Journal of Emerging Trends & Technology in Computer Science, 2*(2).

Hendricks, D. (2014). The History of Smart Homes. *Retrieved from http://www.iotevolutionworld.com/m2m/articles/376816-history-smart homes.htm*

Ishengoma, Fredrick Romanus. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. *arXiv preprint arXiv:1410.0534*.

Kaur, Inderpreet. (2010). Microcontroller based home automation system with security. *International journal of advanced computer science and applications, 1*(6), 60-65.

Khiyal, Malik Sikandar Hayat, Khan, Aihab, & Shehzadi, Erum. (2009). SMS based wireless home appliance control system (HACS) for

automating appliances and security. *Issues in Informing Science and Information Technology, 6*, 887-894.

Puri, Vikram, & Nayyar, Anand. (2016). *Real time smart home automation based on PIC microcontroller, Bluetooth and Android technology*. Paper presented at the Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on.

Robles, Rosslin John, & Kim, Tai-hoon. (2010). Applications, Systems and Methods in Smart Home Technology: A. *A Review International Journal of Advanced Science and Technology, 15*.

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).

Vacca, John R. (2015). *Handbook of Sensor Networking: Advanced Technologies and Applications*: CRC Press.

Vilas, Ana Fernández, Solla, Alberto Gil, Duque, Jorge Garcia, Arias, Jose J Pazos, Cabrer, Manuel Ramos, & Redondo, Rebeca P Diaz. (2010). *An Aml-enabled OSGi platform based on socio-semantic technologies*: INTECH Open Access Publisher.

Vinay Sagar, KN, & Kusuma, SM (2015). Home Automation Using Internet of Things. *International Research Journal of Engineering and Technology (IRJET)*.

Zhou, Chunlai, Huang, Wenhui, & Zhao, Xiaoyun. (2013). *Study on architecture of smart home management system and key devices.* Paper presented at the Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on.

Index