Novel Hybrid Finger Print System for Bank Locking System

V.B. Kirubanand
Associate Professor,
Department of Computer Science,
Christ University, Bangalore

P J Bharani
Scholar, Anna University,
Chennai.

ABSTRACT

The Hybrid Fingerprint locking system can serve as a robust security mechanism and can avoid unauthorized access to a system at any circumstances. Fingerprints are the most widely used form of biometric identification overtime and the critical step in exploring its advantages is to adopt it for use as a form of security in already existing systems, such as bank lockers.

This paper work focuses on the use of fingerprints for bank locker system along with the conventional method of using keys. The supporting software enables fingerprints enrollment in a database.
Before anyone can open the locker, his/her fingerprint information is sent from the database system using ZigBee transmitter and is received by the ZigBee receiver in the locker. Then the fingerprint is matched against the database while users with no match in the database are prevented from opening the locker. By this system unauthorized access to the lockers or mishandlings can be avoided. The application of the Hybrid Fingerprint System is not restricted the Bank locker and it can be used in any system where the Fingerprint readers are used.

.

Keywords: *Zigbee, Fingerprint reader, Locking System, Pulse sensor*

1. INTRODUCTION

At present, number of locker systems is successfully utilizing fingerprint system for authentication. The authentication presented in this paper consists of two stages. In the first stage, the access is provided for the user in the database system and the fingerprint information is transmitted to the locker using ZigBee transmitter.

In the second stage, the information is received by the ZigBee receiver and is matched with the user. For further security purpose, the receiver retains the information for a certain time after which it gets erased and also, the fingerprint system requires two inputs.

This system serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based authentication systems along with ZigBee communication.

2. ZigBee

2.1 INTRODUCTION

ZigBee standard is developed by ZigBee Alliance, which has hundreds of member companies, from the semi-conductor industry and software developers to original equipment manufacturers and installers. The ZigBee alliance was formed in 2002 as a nonprofit organization open to everyone who wanted to join.

[1] ZigBee is a low-cost, low-power, wireless mesh networking standard. First, the low cost allows the technology to be widely deployed in wireless control and monitoring applications. Second, the low power-usage allows longer life with smaller batteries. Third, the mesh networking provides high reliability and more extensive range.

ZigBee is a standard that defines a set of communication protocols for low data rate short range wireless networking. ZigBee based wireless devices operate in 868MHz, 915MHz and 2.4GHz frequency bands. ZigBee is targeted mainly for battery power applications where low data rate, low cost and long battery life are main requirements.

ZigBee and IEEE 802.15.4: ZigBee wireless networking protocols shown in Figure 1. ZigBee protocol layers are based on the Open System Interconnect (OSI) basic reference model. The bottom two networking layers are defined by IEEE 802.15.4 standard. [2] This standard is developed by IEEE 802 standards committee and was initially released in 2003. IEEE 802.15.4 defines the specifications for PHY and MAC layers of wireless networking, but it does not specify any requirements for higher networking layers.

The ZigBee standard defines only the networking, applications and security layers of the protocol and adopts IEEE 802.15.4 PHY and MAC layers as a part of the ZigBee networking protocol. Therefore, ZigBee-compliant device conforms to IEEE 802.15.4 as well.

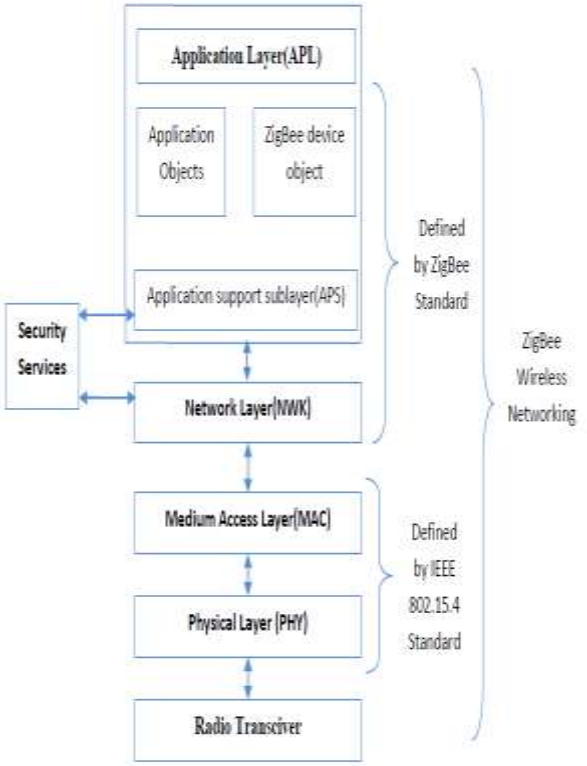

Figure 1 ZigBee wireless networking protocol Layers

2.2 INTEROPERABILITY

ZigBee has a wide range of applications; therefore, several manufacturers provide ZigBee - enabled solutions. It is important for these ZigBee based devices to be able to interact with each other regardless of the manufacturing origin.

In other words, the devices should be interoperable, which is one of the key advantages of the ZigBee protocol stack. ZigBee-based devices are interoperable even when the messages are encrypted for security reasons.

2.3 ZigBee TRANSMITTER

The ZigBee transmitter does major functions like, bit to symbol mapping, symbol to chip mapping, serial to parallel conversion, performing half sine pulse shaping and performing modulation. The receiver performs RF to baseband conversion, sampling and threshold, parallel to serial conversion and dispreading.

2.4 ZigBee RECEIVER

In the receiver configuration of ZigBee, we are using a MSK demodulator and a multiplier for dispreading. This multiplier output contains the baseband data and higher frequency harmonics. The multiplied signal is passed through a low pass filter for avoiding harmonics. This sampled data is passed through a decision device. Decision device is a simple comparator which contains a threshold value for making a decision. If the input to the comparator is greater than the threshold value, it decodes the bit as "1" otherwise it decodes as "0". Actually 2Mbps data coming from parallel to serial converter contains a small amount of offset delay. We must introduce this offset delay in the PN sequence data while multiplying with 2Mbps data, So that we will get original bit stream without any errors.

The following Figure 2 and Figure 3 show the block diagram for ZigBee transmitter and receiver.

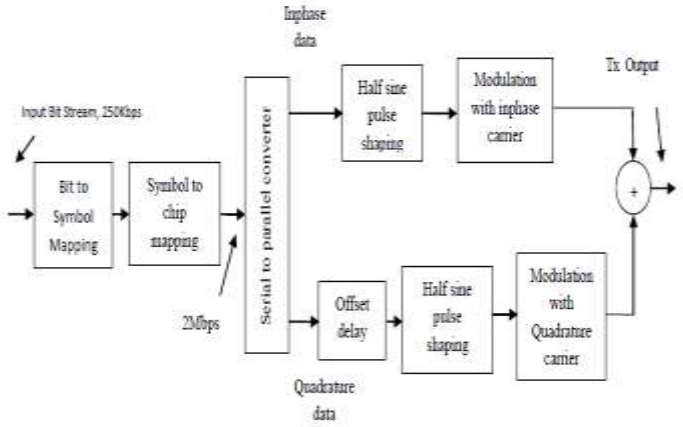

Figure 2 Block Diagram of ZigBee Transmitter

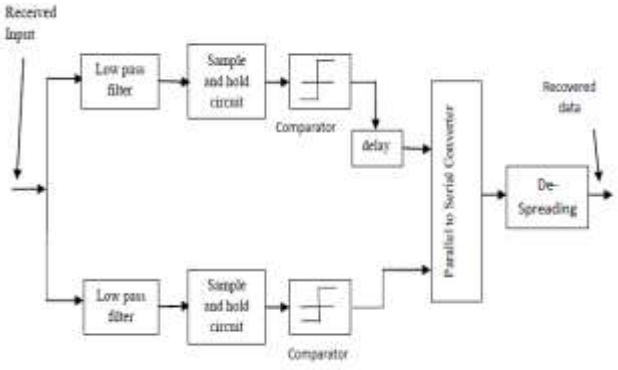

Figure 3 Block Diagram of ZigBee Receiver

3. BIOMETRIC IDENTIFICATION

3.1 FINGERPRINT READER

In traditional fingerprint access systems, an individual attempting to access a protected resource places their finger on a fingerprint sensor/reader at an access point such as a door or computer. The sensor reads the fingerprint and transmits the image, typically to a server, where it is compared against a database of stored fingerprints.

[3] If the live print matches a stored print, the individual is permitted access. Biometrics represents significant security advancements over proximity cards or passwords because they physically prove each user's identity.

In the Hybrid Fingerprint system, while enrolling, two fingerprints are captured and the order of the input is noted as well into the system. The sensor then reads the fingerprint and then the same and it is compared against the database similar to what we have in the traditional fingerprint access systems. What comes as additional security is that the user is alone aware of the input order and this has to be provided in s stipulated time.

3.2 ACCURACY AND RELIABILITY

With biometric finger scanning, remembering a password doesn't matter. [4] Since the technology uses your fingerprint to either allow or deny access, the only way forget your password would be to lose your finger, which likely won't happen.

[5] By choosing good model biometric equipment, we can have a security for as long as you need one. It is very secure and reliable since the fingerprints are unique and immutable.

3.3 PULSE SENSOR

The Pulse Sensor measures subtle changes in light from expansion of the capillary blood vessels to sense your heartbeat. Gently place the sensor on any area of skin (such as a finger or earlobe) and it will transmit pulse data for processing.

4. RELATED WORK

4.1 FINGERPRINT READER WITH PULSE SENSOR

Here a pulse sensor is embedded with the fingerprint reader circuit. This is mainly used for security purpose. If somebody did gain access to an authorized user's prints then the person could trick the scanner. In a worst-case scenario, a criminal could even cut off somebody's finger to get past a scanner security system. So the scanner is made with an additional feature of Pulse sensor to verify that the finger is alive, rather than a mold or dismembered digit.

The Fingerprint reader with pulse sensor is schematically illustrated in figure 4. The finger is placed in the reader first. The pulse sensor senses for the pulse. If pulse exists, then the finger pattern is captured and compared with the existing database and the result is produced.

[6] Most of fingerprint systems utilize optical or capacitive sensors for capturing fingerprints· These sensors detect difference between ridges and valleys of fingerprints. Optical sensors detect difference in reflection. Capacitive sensors, by contrast, detect difference in capacitance. Some systems utilize other types of sensors, such as thermal sensors, ultrasound sensors. In this paper we examine fingerprint systems which utilize optical or capacitive sensors.

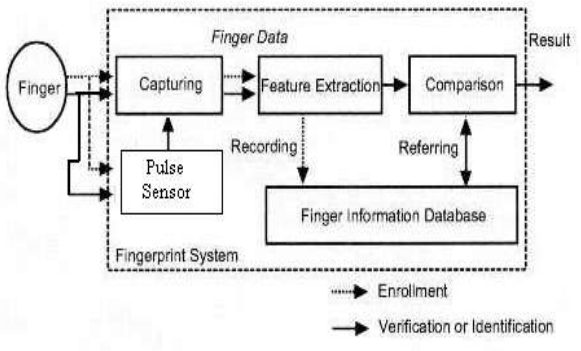

Figure 4: Schematic of Fingerprint Reader wit Pulse Sensor

[7] In the registration process, the system captures finger data from a user with sensing device which extracts the features, and then records them as template with personal information, e.g. a personal identification number or Bank Account number, of the enrollee into a database.

We are using the word "finger data" to mean not only features of the fingerprint but also other features of the finger, such as "live and well" features. In an identification or verification process, the system captures the fingerprint, extracts features, identifies the features by comparing with details in the database, and then outputs a result as "Accepted" only when the features correspond to one of the details in the database.

The Hybrid Fingerprint systems required two fingerprints as input serially (one by one) and the choice of fingers during enrollment is based on the user interest. But, the order of input during the registration is important. Failing to pass the order of input during execution may result unauthorized access to the locking system.

4.2 AUTHENTICATION PROCEDUR

The authentication consists of different stages in which first the users are registered in the database and their details and Fingerprints are stored. Secondly, when the user goes to the bank to access their locker, the user can furnish their Bank account Number and proceed further to access their locker. Then his/her information is transmitted to the respective locker by means of ZigBee from a base system in the bank.

The data at the received by the locker is stored only for a specific time after which it gets erased, so that the user can open their locker only when needed and mishandling can be avoided.

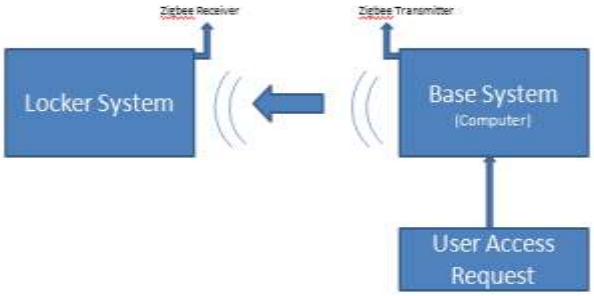

Figure 5: Fingerprint data Transmitted using ZigBee

While opening the locker, the user has to provide his/her fingerprint in the fingerprint reader installed in the locker. The order of fingerprints provided as an input should be the same as enrolled. The fingerprint reader with pulse sensor makes sure that pulse is present and only then the image is captured and sent for comparison with the database, so that any other form of fingerprints like plastic mould or transparent sheets can be avoided.

If the received fingerprints and the captured images matches, then the locker can be opened by using the physical key else the locker cannot be opened.

The database to store the user details are available only in the respective branch of the Bank where the locker is installed. The database management and base system access provision are done by the authorized person in the bank alone.

The data when transmitted is secure since we use ZigBee. In future, Encryption methods can be used during transmission, so that the data is secure in the air.

MERITS OF THE SYSTEM

1. Physical attributes are much harder to fake than identity cards
2. Unauthentic access to the lockers can be avoided.
3. Easy to track the access history.
4. Disarrays can be avoided.

7. CONCLUSION

Development of the locker system with Hybrid fingerprint once again shows that the security of any system must not rely solely upon the honesty of the clients or employees, but mainly on the availability of secure mechanisms and protocols for accidental errors or illicit and malicious collusion between different actors participating in the process.

In general the bank Id or the national identity document is used to identify the customer and the access to the respective locker is given to the consumer. In like manner, by employing the Locker System with Hybrid Fingerprint system which not only provides the right access to the lockers but can be developed further to integrate with the existing customer database for quick processing. As time progresses and this assurance becomes ever more robust and deserving of public trust, and use of this system can becomes a part of everyday life and we can achieve greater secure in the identification system and unauthorized can be avoided to a greater extent.

8. REFERENCE

1. Justo Carracedo Gallardo and Emilia P. Belleboni About Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees (Access date 02.02.2012)
2. Cranor, Lorrie F.; Cytron, Ronald K: Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA, 1996
3. INFSO-ICT-PSP-224993, secure identity across borders linked. http://www.eid-stork.eu/ (Access date 02.02.2012)
4. Drew Robb about How Biometrics Security Works Posted: 01-06-2006 at how stuff works.
5. Biometrics By John D. Woodward (Jr.), Nicholas M. Orlans, Peter T. Higgins
6. Guide to biometrics by Ruud Bolle
7. Smart Voter ID card with Biometric Fingerprint System – P.J. Bharani and B. Gopinath