I J C T A, 9(9), 2016, pp. 3923-3928

Key Management–New Fingerprint Security Technology in Wireless Communication Through ISM Band 2.4 GHz Bluetooth Technology

C. Bala Saravanan[1], P. Sarasu[2], R. Prabu[3] and P. Vijay Anand[4]

ABSTRACT

In this paper launch new Fingerprint security technique for wireless communication though 2.4GHz ISM Band. In Sky Tie Bluetooth wireless technology transfers the files up to 250 meters through 2.4GHz ISM Band. While Sky Tie connection has the advantages that they're automatic and wireless and have the disadvantages of their data being vulnerable to interception along with any other data sent on low power radio wave. In addition to the risk of other people being able to access your sensitive device. This is the major issues in wireless technology. So here we introduce new Fingerprint security techniques for wireless communication in 2.4GHz ISM Band. To develop portable Fingerprint Reader, specially designed to provide precision fingerprint capture, enhanced processing and secure transmission of the capture image to the connecting host using Sky Tie Bluetooth technology encryption.

1. INTRODUCTION

Sky Tie Bluetooth is a very nice technology, [1] but the security issue has to be taken into serious consideration. Risk is inherent to any wireless technology. Now us having different features can be developed into Sky Tie Bluetooth devices, with most having the ability to exchange data with only authorized device only without having to ask for permission. When an unknown device tries to connect to a user's device, the user is able to decide whether to allow or deny access. Some security measures that can be used are authorization and identification procedures. [2] Which require the user to consciously decide whether to open a file or accept data being accessible. Any security compromises must take a different form than trying to obtain or guess the decryption key. Exchange passkeys, also known as association or pairing getting a device to recognize your computer or another enable device. If everyone knows that passkey means can access and receive files from one device to another device [7].

2. IMPORTANT OF FINGERPRINT

The National Governments are creating a fingerprint database for law enforcement and security purpose to identify the authorized person entering and leaving databases. This fingerprint technology improves the Sky Tie Bluetooth secure transaction in wireless communication through ISM Band 2.4 GHZ.

3. PROPOSED WORK

The Fingerprint technique is a portable fingerprint scanner handled device that uses a silicon based capacities sensor to capture fingerprint. The capture figure image is specially processed to enhance the

[1] Research Scholar, Vel Tech Rangarajan Dr. Sakunthala R & D Institute of Science & Technology, Avadi, Chennai, Tamil Nadu (India), *Emails: c.saravanan@veltechmultitech.org, rprabhu@veltechmultitech.org, vijayanand@veltechmultitech.org*

[1,3,4] Assistant Professor of I.T Department at Vel Tech Multi Tech

[2] Director of R & D Department, Vel Tech Rangarajan, Dr.Sakunthala R & D Institute of Science & Technology, Avadi, Chennai, Tamil Nadu, (India), *Email: sarasu@veltechuniv.edu.in*

Figure 1: Fingerprint Format

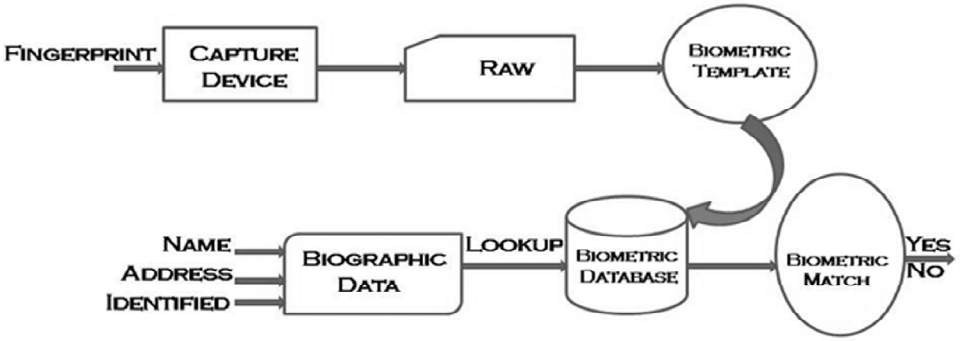

Figure 2: Fingerprint Storing Process

quality and encrypt for storage on the device. [7] It has a developed in wireless Sky Tie Bluetooth interface for host communication. The Fingerprint identification itself and provide the serial profile service (SPP) with the connecting host. In addition to the Passkey and authentication, it can establish another secure communication session for command and data transfer with the connecting host using Higher Encryption Standard (HES)[9].

3.1. Working Processing Method:

- To collect Fingerprint information from a valid person only.
- To capture Fingerprint data in raw form with high resolution image
- To transform raw Fingerprint data into the encoded fingerprint template
- To store all this information in the fingerprint database
- To Lookup the Fingerprint template for a particular individual
- To verify the stored template and the recently capture template match

3.2. Fingerprint Technology Features:

- Secure data transfer in additional to the standard Sky Tie Bluetooth protection
- High level Key management and encryption process with session key
- Ease of development based on Sky Tie Bluetooth serial port profile
- Transparency device operation without special user intervention
- Ease of application integration and development
- Optional Key management support
- User friendly operation with clear and visual notification

4. IMPLEMENTATION

This new fingerprint designed to [3] meets the new paradigms of wireless based solution for the provision of strong authentication to the corporate network. It provides a new dimension to use of technology for wired communication to mobility based platforms. [4] The new Fingerprint technology reader that can be used to support the current biometric solution through Sky Tie Bluetooth. [6] With a built in wireless Bluetooth interface for host communication.

5. CAPTURING FINGERPRINT TO ACTIVATE SKY TIE BLUETOOTH

Once the Fingerprint is powered on and the power on sequence is completed the activation and 1 Sec interval, indicating that the Fingerprint unit is ready to capture and transfer the valid image to activate. [5]

Figure 3: Workflow Setup Outline Techniques

The Fingerprint unit has built in Fingerprint transfer algorithm that will automatically sense a Finger on the sensor and initiate Fingerprint image capture. Then fingerprint will coordinate after it will start Bluetooth process and then generate a passkey to slave mode.

6. FINGERPRINT INTO SKY TIE BLUETOOTH

The Fingerprint unit is intended to be used in the orientation such that the tip of the Finger, [4] whose image is being captured to valid person. The ideal position of the Finger should be such that the midpoint between the tips of the finger to its first joint should be resting on the center of the fingerprint sensor. Rest the finger naturally on the fingerprint sensor with a light pressure on the sensor, ensuring the finger covers a sufficiently large area of the sensor. Once the finger is in position, hold the finger for a short while until the buzzer beeps indicating the fingerprint image is captured, and finger may be removed [6].

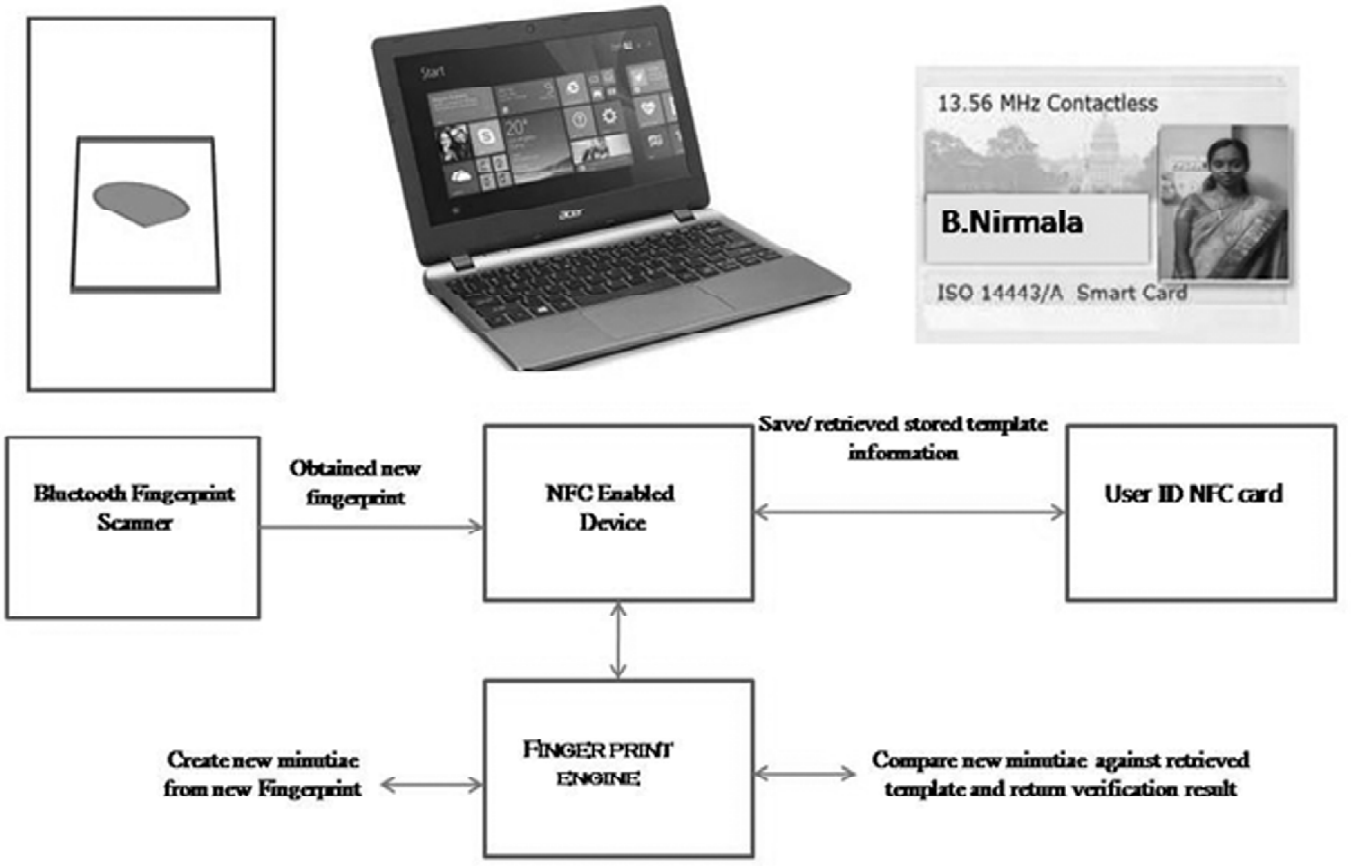

Figure 4: Fingerprint ID verification 1 to 1 Valid Person

6.1. Fingerprint Technical Specification

Table 1
Technical Specification of Fingerprint Machine

Fingerprint sensor	*Upek TCs 1 Touch chip Silicon Fingerprint*
Size	18.0mm × 12.8mm sensor surface, 256 × 360 square
Encryption	HES 256 Bit session Key
Operation Speed	Transfer cycle time < 6 sec good communication speed
Bluetooth Transceiver	Sky Tie Bluetooth
External Power	5V +/-regulated power 500mA

7. FINGERPRINT TRANSFER ALGORITHM:[FTA]

Algorithm: FTA

1. Function – Fingerprint set (Valid Person)
2. Input:
3. Fingerprint @ Valid Person
4. User ID @ Valid Person
5. Address @ Valid Person
6. Minimum – set (Target minutiae list)
7. Biometric Date Ω
8. Original data ()
9. goto next – Biometric template
10. else
11. goto next – failure template
12. else
13. goto next – target pair
14. return
15. Function – GENERATE PAIR (minutiae list)
16. return list of pair ≤ 8
17. Input:
18. Passkey ¥ GENERATE – Master α Slave
19. goto next – authentication verified @ valid person
20. goto next – file chooses
21. else
22. goto next – deactivate
23. return
24. minutiae – pair 1 ¥ send
25. if fingerprint matched @ sent
26. else
27. return
28. end

This algorithm generates to activate the fingerprint from Sky Tie Bluetooth. [2] The fingerprints are accessed only authorized person only to activate the device. Step 3-5 to store the valid person details to access the device. Step 6-13: pair the [3] valid person and give rights to access the device to transfer. If it doesn't match the device will be returned to deactivate. Step 15-20: fingerprints are matched and then Bluetooth device generate a passkey [5] to slave mode, otherwise the device process will be canceled and return to the main function. Step 23-28: fingerprint and passkey are matched and then the device will be sent file master to slave.

8. EXPERIMENTAL RESULT

In order to produce the performance of our proposed system delivered positive results. All security transactions between two or more parties are handled by the Fingerprint technology. Fig-5 It will show the result of security, communication in wireless technology through ISM Band 2.4 GHz. [7] from this result onwards Bluetooth will become a very strong communication to P2P. Before going to activate your Bluetooth you must be entered your fingerprint, then only activate your device. Authorized fingerprints are stored in Biometric database. If matched means allow you activate your device or else deactivate your device. Then generate a passkey to transmit from master to slave node.

9. CONCLUSION

Authorized fingerprints are stored in Biometric database. If matched means allow you activate your device or else deactivate your device. As technology makes progress, the new fingerprint security is being developed

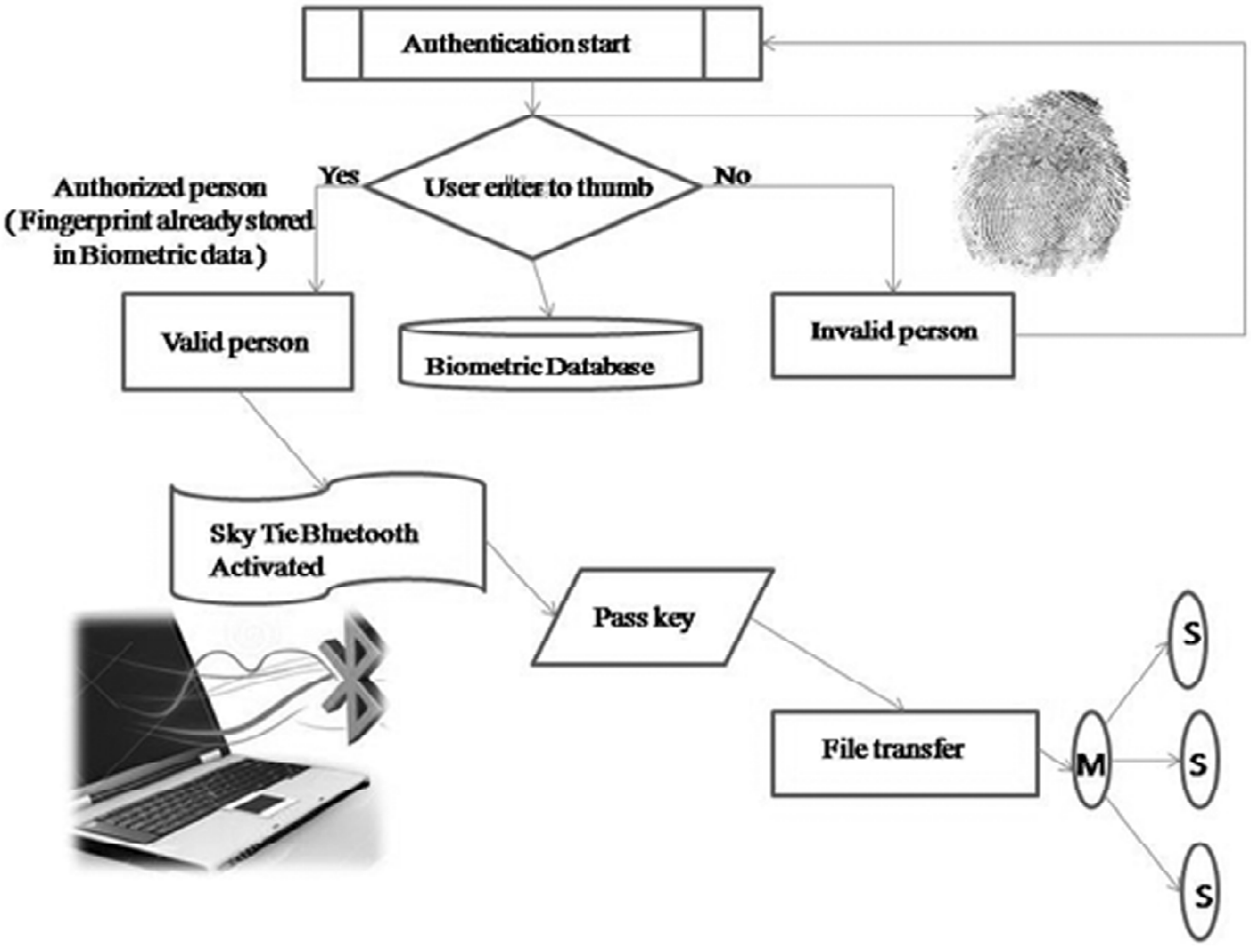

Figure 5: Fingerprint into Sky Tie Bluetooth Activate

by the Sky Tie Bluetooth authorized users. It is not possible to enter unauthorized person to, activate your device. So this result produced very strong and secure communication to P2P through ISM Band 2.4GHz.Fingerprint device all has Sky Tie Bluetooth as a mandatory feature and its potential security application are increasing. So we need fingerprint technology to carry on Bluetooth security to secure communication in wireless technology through ISM Band 2.4GHz.

REFERENCE

[1] Bluetooth security threats and Solutions: a survey Nateq Be-Nazir Ibn Minar and Mohammed Tarique. International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3, No. 1, January 2012.

[2] Improved Probability Algorithm Based on Low Energy Bluetooth Technology Lin Zhu. International Conference on Computer Science and Electronic Technology 2014.

[3] An Effective Algorithm for Fingerprint Matching1.Ying HAO, Tieniu TAN, Yunhong WANG. Funded in part by CAS and NSFC (Grant No. 69825105)

[4] Bluetooth Security. Juha T. Vainio. 2000-05-25

[5] Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances. Abinandhan Chandrasekaran, Dr.Bhavani Thuraisingham. Second International Conference on Availability, Reliability and Security (ARES'07) IEEE

[6] A Unique Wireless Device Fingerprinting Technique for Secured Data Communication in Wireless Network. Murali Kotha, Madhavi, International Journal of Computer Applications (0975–8887) Volume 43– No. 20, April 2012.

[7] Enhancing Bluetooth Authentication using Diffie HellmanAlgorithm.Rajveer Kaur, Rupinder Kaur Cheema. International Journal of Computer Applications (0975–8887) Volume 68–No. 18, April 2013.

[8] An Overview and Assessment of Wireless Technologies and Coexistence of ZigBee, Bluetooth and Wi-Fi Devices. Cihan H. Dagli, Available online at www.sciencedirect.com.

[9] Guide to Bluetooth Security. National Institute of Standard and Technology. Special Publication at Revision.