FINGERPRINT BASED SECURITY

Chander Singh[1], Dr. Devesh Katiyar[2]
[1] Student of MCA, [2]Asst. Professor
Department of Computer Science
DSMNR University
Lucknow, Uttar Pradesh, India

***Abstract*- Today in the digital world the most important thing is security of the crucial data from data corruption, data theft, data damage etc. Data confidentiality is a crucial topic to discuss. Nowadays at every stage security systems for the protection of valuable data is required. Fingerprint security is a trendy method used for authentication. It is being used almost in every field. But there are still some limitations and problems in this method. This paper represents one of those problems present in fingerprint based security systems in smart phones and methods to resolve it.**

***Keywords*- Security; Smart phones; Biometrics; Fingerprints; Authentication; Temperature based system; Steps count system; Fingerprint pattern**

I. INTRODUCTION

In this busy and fast moving world, the security of the data is primary concern. Today most of us buy expensive smart phones just by checking its some details like RAM, storage, processor, camera etc. Even we keep our confidential data in smart phones like bank details, photos, email id passwords and other passwords. But we just don't much care about its total security, and this is a bitter truth of today's "Smart World".

Yes, there are various methods for authentication. This is the field that has grown since its existence, and will also extend in future. There are various types of authentication techniques being used today. Among these techniques, some are:

A. *PIN:* In this method a four digit code is used for security. But the problem of this method is that the password can be retrieved by anyone by hit and trial method.

B. *Password:* To end up this problem password could be used as there is no limitation for number of characters or digits. The password can be created using multiple characters and digits. But this system also had some drawbacks, as the password could be theft or hacked. Sometimes the user might forget the password.

C. *Pattern:* The pattern security consists of 9 dots that are to be joined in a sequence so that a required pattern is formed. This method also had similar problem as that were in password security.

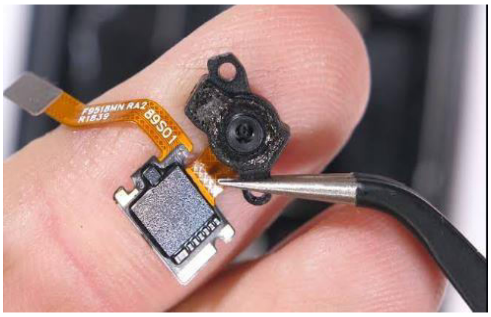
D. *Voice Recognition*: Voice Recognition has also been used for security purpose. For voice recognition, MATLAB software is used for coding. In this, the authentication of owner can be confirmed by the characteristics of voice. But sometimes in winter of during cough and cold, the voice changes, due to which the voice might not be recognized. Even there are various voice artists so, voice can also be copied.

E. *Fingerprint Security:* Fingerprint security is a biometric type security system. This is also a fine method used today. Fingerprinting method with the aim of authentication was being used for more than 2 centuries. Babylonians used to press tip of their fingers on clay for recording the business transactions. Even Chinese applied ink to print their fingerprints for business. Fingerprint system was also used for identifying the criminals. This was among the best and secure methods of authentication as the fingerprints of each person are somehow different from one other. Yet the fingerprints of every finger of the person vary from one another. It was being used in various sectors where there was need of authentication and security. During 2010s fingerprint security system was added in smart phones.

1. *Types:* There are various techniques used for fingerprints.

1.1. *Optical reflexive:* This is very common method. In this, the finger is put on the glass plane that is lighted up by a light emitter diode. When finger is put on the glass, the ridge part of finger absorbs the light and the crest part reflects back the light. This result in light and dark areas recorded.

Optical reflexive fingerprint scanner



Optical reflexive fingerprint scanning device

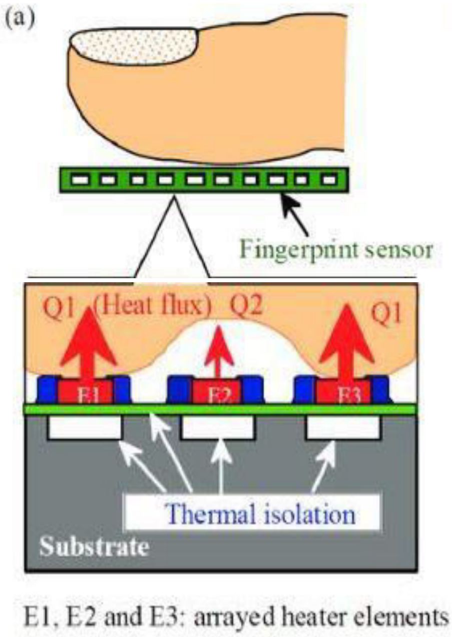
1.2. *Capacitive:* The sensor panel contains multiple transducer elements (pixels). These elements contain two adjacent electrodes. Capacitance around electrodes is decreased when finger is touched on panel. It is reduced more at raised portions and reduced less on spaces between them. This is not operative with skin with scars, moisture or dust.

Crossmatch EikonTouch 710 Capacitive fingerprint scanner

1.3. *Mechanical:* The surface contains thousands of pressure transducers. The finger ridge puts more pressure on pressure transducers that forms unique pattern.

Mechanical fingerprint scanner

1.4. *Thermal:* In this system the heat produced by finger is used for authentication. There is variation between the heat produced on ridges and the heat produced at valley. As the heat produced on the ridge is more as compared to valley, so a unique pattern will be formed. It is even used for finger with dirt and moisture.



Sensing principle of a thermal fingerprint sensor

2. *Drawbacks:* This is among the most secure methods of authentication. But everything has some drawbacks. The key drawback I observed in present system is fingerprint theft. Yes, when a person falls asleep or unconscious, anyone (unauthorized user) who wants to get access the mobile phone could just make victim’s finger touch on the sensor and the phone will be accessible. This is a major threat to the data.

II. THE PROPOSAL SYSTEM

To trounce the above discussed drawback some proposed systems are as follows:

(1) *Temperature Based System:* In this system thermal fingerprint sensor will be helpful. As per some researches during sleep the temperature of the human body slightly decreases. If we make a temperature as standard say 38^{0} C, then it would be helpful to make the data more secure. The mobile phone would not be accessible till the temperature detected is above 38^{0}C. As body temperature will definitely be less than 38^{0} C during sleep, the phone would not open. But if a person is not sleeping then the temperature of the fingers can be increased just by rubbing hands, so this system will work even during winters.

(2) *Step Count System:* As we know that when a person is asleep, there is almost no movement of the body. We can take the advantage of this for security purpose. A feature can be added to the smart phones in which the smart phones will open only when the person is moving along with putting his finger on the sensor. For this a device called “accelerometer” can be used. Accelerometer is a small device which is used to calculate proper acceleration i.e. the number of steps. Nowadays, this device is used in fit bands and even in smart phones to count steps moved by the person.

For security purpose, the minimum number of steps can be fixed on the device to get access. For accessibility, the person has to put his finger on the sensor and have to move at least the minimum fixed steps. As during sleep, one can make the victim’s finger touch but can’t displace him.

(3) *Fingerprint pattern:* In this method, multiple fingerprints could be used for security. Let us understand it briefly. Multiple fingerprints will be stored as authentication security in a specific pattern. If the pattern stored contains the scanned pattern in the sequence ‘thumb left hand 2 times and then middle finger of right hand single time’, then during unlocking user has to scan the fingers in the same sequence i.e. thumb of left hand 2 times and then middle finger of right hand single time. Otherwise the device would not be accessible. It will be more complex or impractical to guess the pattern in which the fingerprints are entered.

III. CONCLUSION

In this modern and fast growing world, the security problems can never end. But we can reduce the security risks to a minimum level. Any of the discussed proposed systems can be added in smart phones to handle the present day existing drawbacks.

IV. REFERENCES

[1] International Journal Engineering And CS Issuing Date: 03-03-2015, Page No. 10810 to 10814

[2] “Guide To Biometric Home Security Devices” by Vincent Dail

[3] https://simple.m.wikipedia.org/wiki/Fingerprint_scanner

[4] https://identamaster.pro

[5] https://Androidauthority.com/how-fingerprint-scanners-work-670934

[6] https://www.researchgate.net/profile/Chander_Kant4/publication/41890634_Reducing_Process-Time_for_Fingerprint_Identification_System/links/56a8f6fc08aeaeb4cef920d5.pdf