Dynamic Fingerprint Pattern Lock Mobile Application Using Android

K. Ramesh , M.Anto Bennet, S.Prasanth, M A .Anand , V.Sujith Kumar, R.Ragavendran M.Thirumana sambantham

***Abstract*: In this paper we are examining about information security in mobile. Numerous cell phone creators currently fuse biometric security highlights into their products. Furthermore, some gadget makers presently enable application designers to utilize these highlights through their product advancement packs (SDKs). In this investigation, we use fingerprint recognition with a pattern, to build up a security for mobile application. Before, application had the single time finger press. Here we have utilized various time check and long-term hold confirmation techniques. Inside a constrained time, outline, the unique fingerprint image can be utilized to open the app which has classified information identified with government, banking, training, and so on which must be verified. As the generation of cell phones with fingerprint recognition keeps on expanding, this type of authentication system, the one we present in this paper, will turn into a great safety measure.**

Index Terms: Marketing, Segmentation, Technology and Buying Behaviour.

I. INTRODUCTION

This project Finger Print Pattern Lock enables access to mobile for those whose fingerprints that are pre-put away in the memory. Put away fingerprints are held even in case of complete power disappointment or battery drain. It must be opened when an approved client is available since it has keys or blends, that must be entered by the approved client's fingerprints. The fingerprint-based lock along these lines gives a magnificent answer for conventionally encountered inconveniences. This report centers around the utilization of fingerprints to open mobiles, instead of the built-up strategy for utilizing simply an example or stick. Biometric frameworks have additional time filled in as hearty security instruments in different areas. Fingerprints are the most established and most broadly utilized type of biometric distinguishing proof. The utilization of finger impression for distinguishing proof has been utilized in law authorization for about a century. A lot more extensive utilization of fingerprint is for individual verification, for example, to get to a PC, a system, an ATM machine, a vehicle or a home. Electronic lock utilizing unique finger impression acknowledgment framework is a procedure of confirming the unique finger impression image to open the electronic lock. This undertaking features the advancement of unique finger impression check with an example. Verification is completed by comparing the data of authorized fingerprint image with incoming fingerprint image entered in a pattern a few times. At that point, the data of approaching fingerprint image will experience the examination procedure to contrast and approved unique mark picture. In this project, digital image processing algorithm is employed in a pattern to identify whether the incoming fingerprint images are genuine or not.

II. BIOMETRIC SECURITY SYSTEMS

Biometrics is utilized for perceiving clients dependent on their concoction, physical, and conduct highlights. Biometric advances are depicted as the mechanized validation of an individual dependent on their physiological and conduct trademark. Biometric acknowledgment frameworks are iris, retina, face, unique mark, vein, palm, voice, mark and keystroke. A unique mark comprises of the edges on an individual's finger and a unique mark recognizes an individual from others by the exceptional example of those edges. 35 percent of shoppers utilize the unique finger impression coordinating technique. Considering the portable security highlights like SIM card security with the PIN code, drawing designs on the screen for secure access to an advanced cell, email and secret phrase confirmation for getting to applications, each of those referenced have few weaknesses.[1] A biometric validation strategy can decide the personality of the client and can't be imparted to other people; however, a secret key or token-based verification can't demonstrate the client. Considering every one of the upsides of biometric acknowledgment, cell phone makers have begun to convey diverse biometric sensors on cell phones. Goode Intelligence anticipated that 3.4 billion clients will utilize biometric frameworks on their cell phones by 2018[2]. Presently unique mark sensors are accessible on the most recent savvy cell phones. 40 % cell phones will be furnished with biometric sensors. Versatile biometric acknowledgment, particularly unique finger impression acknowledgment, can be utilized for safe portable instalment exchanges, to open the screen lock of a gadget, portable banking and designers can utilize unique mark security highlights for their versatile applications. The cell phone pioneers, Apple and Samsung, have taken measures to secure client unique finger impression information. The unique finger impression information remains inside the secured equipment conditions. This demonstrates unique mark

Revised Manuscript Received on December 22, 2018.

K. Ramesh, CSE Department, Hindustan Institute of Technology and Science, Chennai, India**.**
M.Anto Bennet, ECE Department, VEL TECH, Chennai, India
S.Prasanth, ECE Department, VEL TECH, Chennai, India
M A .Anand, ECE Department, VEL TECH, Chennai, India
V.Sujith Kumar, ECE Department, VEL TECH, Chennai, India
R.Ragavendran, ECE Department, VEL TECH, Chennai, India
M.Thirumana sambantham, ECE Department, VEL TECH, Chennai, India

information are secure in cell phones. The FIDO (Fast Identity Online) Alliance is a non-benefit association to take care of the issues of recollecting numerous usernames and passwords. It stores all accreditations incorporating biometric ID in the cloud. The FIDO framework will give another course to client acknowledgment frameworks with the help of biometric ID. Also, passwords might be swapped by biometric confirmation for cell phones. [3-12]

III. FINGER PRINT PATTERN LOCK AUTHENTICATION APPLICATION FOR SMARTPHONES USING ANDROID

Fingerprint recognition is the most utilized biometric acknowledgment arrangement of all. Fingerprint recognition is turned out to be both more secure and helpful than passwords, making finger impression detecting an inexorably normal and highlight in cell phones, tablets, and PCs.For perfect fingerprint recognition the following steps are done:

1) Fingerprint image capture

The purpose is to acquire advanced unique digital fingerprint image. An advanced digital fingerprint image is acquired through picture getting card to manage the 2D prints got by squeezing the unique finger impression. Such a technique is so tedious. Nonetheless, present-day frameworks receive programmed input strategy like ongoing internet catching to get advanced unique digital fingerprint image, which is one of the key systems.

2) Pre-processing image

The procedure of image pre-processing incorporates portioning, upgrading, parallel coding and diminishing. The intention is to improve the unique mark picture quality. Minutiae extractor is utilized for this. The accuracy of unique finger impression recognizable proof depends for the most part on the noticeability to the ridgeline structure and minutia point data, and finger impression picture will be influenced by a wide range of clamours brought about by finger itself and procurement conditions. In this way, it's important to improve the portioned unique mark pictures to make unique mark highlights be progressively dependable. In a fingerprint identification system, the digital fingerprint image is a hazy dark picture which will be changed over into paired picture with just high contrast through binary coding.

3) Minutia Feature extracting and matching

A feature extracting is the procedure to extract minutia features from the diminished edge mapping structure. On the off chance that the nature of the picture input is extremely great, it's anything but difficult to distinguish the edge build. Be that as it may, the fingerprint image input doesn't generally have great edge develop which will diminish the exactness of the picture separating. In this way, by and large, pre-preparing is important to decrease the commotions and improve the removing exactness. Fingerprint feature matching has two patters: one to one and one to many. For the primary, constant gained unique mark information is specifically contrasted and relative format in finger impression database to pass judgment on whether both are from a similar finger. While, for the other, request and correlation of database are required on the grounds that client highlight layouts haven't been recognized. One great coordinating algorithm ought to be furnished with the following characters: autonomous on contributing edge and position, unaffected by outside weight and certain blunders allowed.Even though fingerprint recognition is most used and secure it has few disadvantages and that is what we are noticing and proposing the new features in this paper. It is discussed and explained in detail and it follows:

Securing confidential data

Many smartphone users have important data to store and secure in their phones. But those who want to secure confidential or very important data with fingerprint lock and who fear their fingerprint lock can easily be unlocked by thieves and robbers want more secure and multi-level security system. They don’t care about how many touches or seconds it takes to unlock their mobile. There are many security concerns in the normal fingerprint recognition system.

Security Concerns in fingerprint recogniton system

Fingerprint authentication also raises security concerns like anyone can use our fingers to unlock the device when we are unconscious or asleep. And many uses pattern swipe lock along with fingerprint lock, which is not very secure because pattern lock can easily be cracked even by those who don’t knowing hacking. i.e. when kept in bright light the pattern can be seen on the screen as the user would have swiped the screen many times. And that is why we are proposing a feature called fingerprint pattern lock.

Fingerprint pattern lock feature

These security concerns can be addressed with finger print lock in a pattern. Using this application, we provide a multilayer security to the user. The Proposed system is a fingerprint pattern lock app which allows to secure the user’s data in an app in next level. Multiple fingers are placed on the sensor multiple times and press and hold for few seconds, which is a pattern. We develop a system that is well structured and computerized. And the goal of our project is to avoid the problems faced in the existing system of fingerprint recognition system and develop as a fully efficient one.

IV. PROPOSED SYSTEM:

This app is to secure confidential documents. We access the fingerprint sensor and the fingerprint image stored in the default fingerprint application. The user must set a pattern in our app. Whenever they need to access the documents stored, they must give this fingerprint pattern as input. If they use the wrong finger, or if someone else tries to access this app, the user will receive an alert SMS. To give the swipe pattern that is now available in phones we need to look at it. But this fingerprint pattern can be entered even without looking and with our phone in our pocket. This way now on can see and find the pattern.

The data flow diagram of this paper is shown in fig 1.

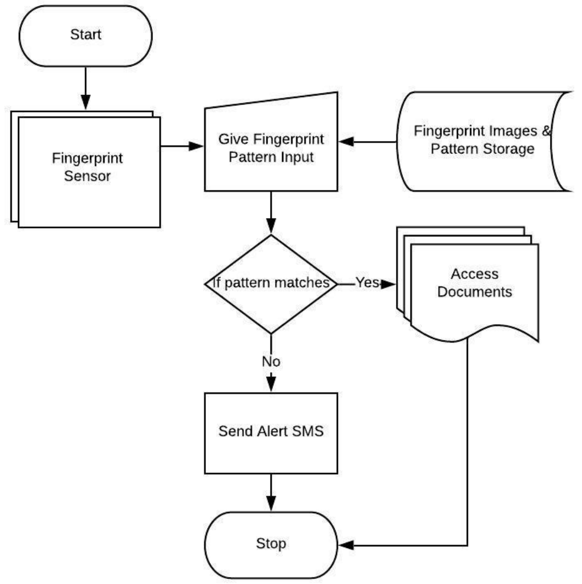

Fig 1 Data flow diagram of this project

V. COMPONENTS USED IN THIS PROJECT AND THEIR DESCRIPTION

The Block Diagram, components and its descriptions are given in fig 2.

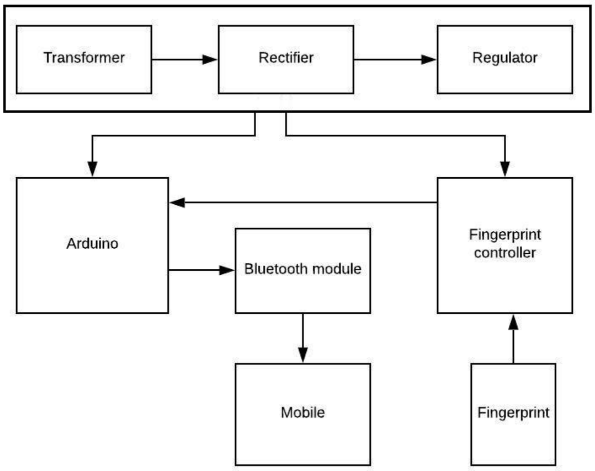

Fig 2 Block Diagram of Static Fingerprint-In-A-Pattern Lock

Components used are Stepdown Transformer, Rectifier, Filter and Regulator, LCD Display, Arduino UNO, HC-05 Bluetooth Module and R-307 Optical fingerprint reader sensor module

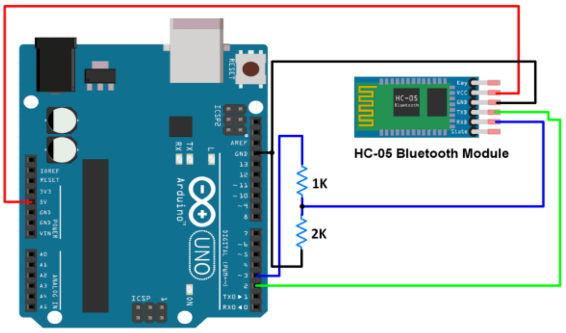

Fig 3 **Interfacing HC-05 Bluetooth Module with Arduino**

UNO

HC-05 is a Bluetooth device used for wireless communication with Bluetooth enabled devices (like smartphone). It communicates with microcontrollers using serial communication. It is used to connect the kit with mobile through Bluetooth. If it sends signal and mobile receives it then app can be accessed. Or an alert SMS saying, “someone is using the app” will be sent to a ten-digit number that is set by default shown in fig 3.

Figure 4: R-307 Optical Fingerprint Reader Sensor Module

A Fingerprint controller is used to give fingerprint input and store it in the board. It is connected to the power supply unit and Arduino. Low power consumption, low cost, small size, excellent performance, Professional optical technology, precise module manufacturing technics. Good image processing capabilities can successfully capture an image up to resolution 500 dpi Finger detection function. It is the main part of the paper and this is where we give the input shown in fig 4.

VI. CONCLUSION

This is a simple and basic mobile lock android app which takes the security to another level which works based on finger print in a pattern access, thus giving at most security to important or confidential data in devices. The future enhancement that can be developed from the paper is to make sure it is easy and compatible to make every user have this feature. We don’t have the technology or idea to make it a one-step access which many users would want, so this is not in the proposed system, and foreign fingerprint access email alert can be in the future enhancement. Processing speed also should be taken under consideration for enhancement. This application will be a new and next level attempt in data security.

REFERENCES

1. I. Akyldiz, W.Su, Y. Sankarasubramanian and E. Cayirci, “A survey on sensor networks,” IEEE Communication Mag., vol. 40, no. 8, Aug. 2002, pp. 102-14.
2. C. Shen, C. Srisathapornphat, and C. Jaikaeo, “Sensor information networking architecture and applications,” IEEE Personnel Communications, Aug. 2001, pp.52-59.
3. Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas "Routing Protocols in Wireless Sensor Networks" Sensors

2009,9,8399-8421;doi:10.3390/s91108399.

4. S. Tilak, N. Abhu-Gazhaleh, W. R. Heinzelman, “A taxanomy of wireless micro-sensor network models,” ACM SIGMOBILE Mobile Comp. Commun. Rev., vol. 6, no. 2, Apr. 2002, pp. 28- 36.
5. P.N.Renjith, E. Baburaj, “Analysis on Ad Hoc routing protocols in wireless sensor networks” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.6, December 2012.
6. Dr. AntoBennet, M, Sankar Babu G, Natarajan S, “Reverse Room Techniques for Irreversible Data Hiding”, Journal of Chemical and Pharmaceutical Sciences 08(03): 469-475, September 2015.
7. Dr. AntoBennet, M , Sankaranarayanan S, Sankar Babu G, “ Performance & Analysis of Effective Iris Recognition System Using Independent Component Analysis”, Journal of Chemical and Pharmaceutical Sciences 08(03): 571-576, August 2015.
8. Dr. AntoBennet, M, Suresh R, Mohamed Sulaiman S, “Performance &analysis of automated removal of head movement artifacts in EEG using brain computer interface”, Journal of Chemical and Pharmaceutical Research 07(08): 291-299, August 2015.
9. .Dr. AntoBennet, M “A Novel Effective Refined Histogram For Supervised Texure Classification”, International Journal of Computer & Modern Technology , Issue 01 ,Volume02 ,pp 67-73, June 2015.
10. Dr. AntoBennet, M, Srinath R,Raisha Banu A,“Development of Deblocking Architectures for block artifact reduction in videos”, International Journal of Applied Engineering Research,Volume 10, Number 09 (2015) pp. 6985-6991, April 2015.
11. AntoBennet, M & JacobRaglend, “Performance Analysis Of Filtering Schedule Using Deblocking Filter For The Reduction Of Block Artifacts From MPEQ Compressed Document Images”, Journal of Computer Science, vol. 8, no. 9, pp. 1447-1454, 2012.
12. AntoBennet, M & JacobRaglend, “Performance Analysis of Block Artifact Reduction Scheme Using Pseudo Random Noise Mask Filtering”, European Journal of Scientific Research, vol. 66 no.1, pp.120-129, 2011.