FINGERPRINT AUTHENTICATED SECURE ANDROID NOTES

Manish Agrawal, Saloni Shah, Anubha Sah, Subrata Sahana
E-Mail Id: manish.agrawal00050@gmail.com, saloni.shah150@gmail.com, sahanubha12@gmail.com, subrata.sahana@gmail.com
School of Engineering, Sharda University, Sharda University, Greater Noida, India

Abstract- This Venture permits the clients to store individual notes in android portable utilizing unique mark verification. Android notes are the notes wherein one can store individual data. Individual data isn't making sure about to store in android telephones. Be that as it may, it will be smarter to store the notes with some sort of validation gave to it. The use of biometric as a distinguishing proof and acknowledgment measure fills a significant need in light of the fact that the headway of data innovation has coupled the requirement for high security or passwords. This is done to keep away from the danger to discover or still. Unique mark scanners can be utilized to recognize one scanner from another because of the exceptional examples. The surface example creates the hand math for made sure about and confirmed admittance control and it is the genuine substitute for passwords and identifiers in correlation with the current strategy biometric attributes for example unique mark accomplish real close to home ID.

Fingerprint authentication is a secured biometric feature through which we can secure any data.so our Note application will be secured with Fingerprint authentication which makes this secured and private app. Users can use this note app for their private use keeping their fingerprint as security to access the app. Only the owner of the phone who has access to their phone can access this app which will make this app highly secured.

Keywords: Fingerprint Authentication, Android Notes, Security, Biometric Application.

1. INTRODUCTION

New technologies on the phone have made the user do different tasks on the phone. The task includes playing games, surfing as well as storing data. To perform all these reliable mechanisms must be used to verify the identity. An old method such as password, the pin has many security issues such as guessing, brute force attacks, etc. [7]. so, it is very crucial to secure the fingerprint authentication from the possible threats. The Fingerprint is both used for unlocking the phone as well as accessing other applications [8]. Currently maximum phones as using fingerprint authentication.

This application is a straightforward and savvy application used to make sure about android notes.it utilizes unique mark validation to make sure about .it needn't bother with any secret word to enter like the customary strategy. Just the proprietor of the telephone access through these notes. Clients can include, alter, and erase notes.

1.1 Fingerprint

It is an impression or imprint made on a surface by an individual's fingertip. It can recognize people by an uncommon example of a unique mark.

Fig. 1.1 Fingerprint

1.2 Authentication

It is the demonstration of offering admittance to a PC System. It was set up to confirm the client.

1.3 Password

It is the most common form among all the authentication. It is a code or string. The password should be strong enough so that it cannot be guessed easily.

1.4 Android Notes

It is a note making the application. This note is simple and very easy to use.
Modules in Android Notes:
- ➤ Fingerprint Authentication: The owner has to scan a finger to get access to the notes
- ➤ Add Notes: The user can add new notes.
- ➤ Edit Notes: The user can edit old notes
- ➤ Delete Notes: The user can delete notes

1.5 Advantages

- ➤ This app can be used as personal notes or a private diary.
- ➤ The authentication used in this app gives the highest level of security.
- ➤ Only the owner can access the notes.
- ➤ We can add an unlimited number of notes there is no certain limit.
- ➤ To run this app no internet is required
- ➤ To access through this app no registration is needed

1.6 Disadvantages

- ➤ The app does not work if there is no biometric feature on the phone.
- ➤ This app can be used in the phones which have an android version less than marshmallow.

1.7 Application

The following applications where finger print authentication gives more security as: [9-10]
- ➤ Financial Sector: PIN codes and passwords are a story of the past. They give helpless assurance to a bank's clients as they are simpler to fake and consequently lead to burglary. They likewise have helpless ease of use as they are frequently hard to recall making them awkward for security. The financial area has now stepped up its security by utilizing biometric advances to monitor its customers. Security to one's record has been fixed by advances, for example, unique mark scanners, facial acknowledgment, and so forth. Banks use biometrics for cutting edge verification to ensure the information of clients. It is a drawn out market move that has been progressively assuming control over the customary methods for making sure about one's money related information. Also, with regards to making sure about our funds, biometrics are a lot more secure when contrasted with passwords and pins since it requires your valid approval. The financial business is likewise searching for additional arrangements in the utilization of biometric innovations to secure the monetary information of its purchasers.
- ➤ Hospitality Sector: The cordiality area is tied in with giving solace, extravagance, and security to its customers. The associations that are staying aware of the movement of this adjustment in innovation are cutting down their adversaries effectively in this profoundly serious industry. Envision never remaining in lines for looking into an inn during their bustling season or yielding for security checks. This is the thing that biometrics is bringing to the friendliness area. Biometric gadgets are utilized in the majority of the high-class lodgings because of its safe and client amicable highlights. To approach selective rooms and places, the visitors can just give biometric information needed by the inn. Registration and registration with fingerprints or facial acknowledgment can make it simpler and advantageous for the visitors and make their stay agreeable and safe.
- ➤ Healthcare Sector: Facial acknowledgment tech, iris scanner, and finger scanner are the absolute most utilized biometric innovations in emergency clinics to gain admittance to or control information. It is a more solid methods for access when contrasted with key cards which can be handily lost or lost. It likewise gives the medical services simpler and snappier admittance to the information they have to give care to the patients. Emergency clinics are getting more worried about giving better security insurance and wellbeing measures to their customers, henceforth the expanded utilization of biometric advances for documentation and observing purposes. The profitability of specialists and medical caretakers can likewise be effortlessly observed using biometrics.
- ➤ Commercial Industry: In a journey to forestall robbery, numerous retailers are depending on the biometric innovation that gives facial acknowledgment of its clients. It is utilized against an information base of realized shoplifters to screen any possible criminals by contrasting the checked facial information. Facial acknowledgment can likewise empower retailers to elevate relatable things to the clients as per their perspectives and interests in a specific item. The business is upset by biometric advancements fundamentally in light of the fact that the retailers are propelled to chop down robbery by clients and even workers.

1.8 Ease of Use

- ➤ This app can be used as personal notes or a private diary
- ➤ The authentication used in this app gives the highest level of security.
- ➤ Only the owner can access the notes
- ➤ We can add unlimited number of notes
- ➤ To run this app no iternet is required

> To access through this app no registration is needed

2. LITERATURE SURVEY

Anil K. Jain zeroed in on the security of biometric models. This is a serious deal since compound biometric models can't be denied and reissued, in contrast to passwords and tokens. Ensuring models is a troublesome errand because of the inconstancy between clients in the biometric attributes obtained. He introduced a diagram of different biometric model insurance conspires and talked about their focal points and weaknesses as far as security, revocability and group exactness [1].

Brindha, V.E. presented on the protection of the fingerprint model from the creation of physical representation and its replacement with the imposter model to obtain unauthorized access to applications that use biometric encryption systems. In this proposed system, a more secure and authenticated fuzzy deposit was generated to improve the security of the archived models [2].

Dacheng Xu and Bailiang Li proposed and introduced a key pseudo-arbitrary unique mark grouping calculation dependent on a fluffy vault. It is commonly hard to change the model and produce an erasable unique mark model, however in this technique it is conceivable to change the little and exact design. This conquers weaknesses [3].

Kumar D talked about the issue that an individual needs to recollect their passwords or mystery codes and is hard to ensure. The So a biometric unique mark installment framework is utilized for different sorts of installment frameworks, as it is substantially more secure and simple to utilize and even without utilizing any passwords or mystery codes to recollect. It is solid and costly and has a larger number of points of interest than others [4].

Khan, M.K. show that their plans perform one-sided validation and that there is no common confirmation between the client and far off frameworks. To take care of the issue, they propose a proficient and secure far off common validation plot utilizing single direction hash capacities. The computational expense and productivity of the proposed plot are superior to other related distributed plans [5].

Nand Kumar K. also, AK Jain introduced a completely programmed usage of the fluffy vault plot dependent on unique mark minutes by removing the high shape focuses got from the unique mark direction field and utilizing them to adjust the model and cross examine the particulars. They applied a subtlety of details when disentangling. Vault execution is actualized in two distinctive unique mark information bases [6].

3. PROPOSED WORK

3.1 For Fingerprint Authentication

Step 1: System (Android phone) will check the following criteria-
> At least one fingerprint is registered
> The Lock screen is secured with at least one type of lock
> Android version should be greater than or equal to marshmallow
> The Device has fingerprint Scanner
> Have permission to use fingerprint scanner in the app

Step 2) if the system satisfies all these conditions, then the app will run otherwise the app will not run.

Step 3) at homepage app will ask to place your fingerprint scanner.

Step 4) after placing the fingerprint on the scanner if the fingerprint is valid then you can access the app otherwise it will throw an error of Authentication failed.
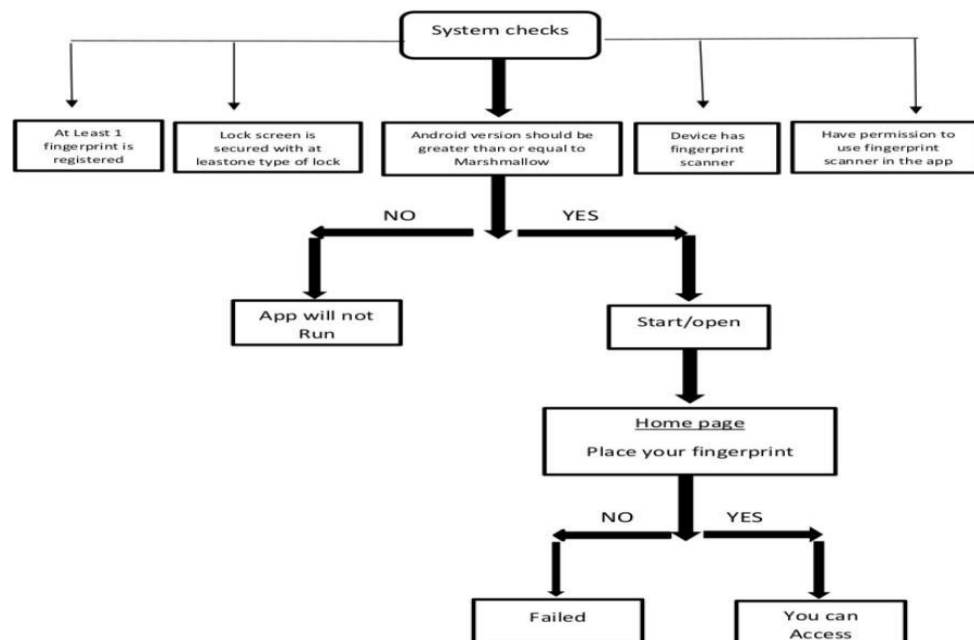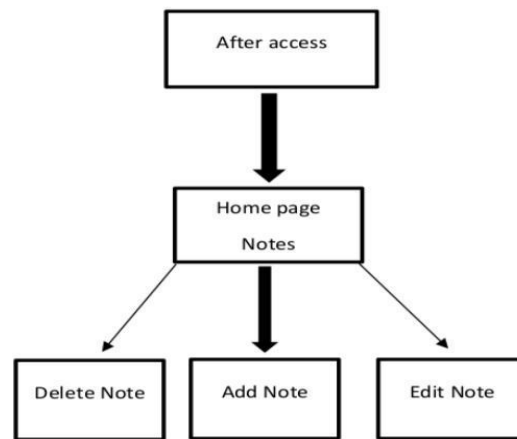

Fig. 3.1 Flowchart for Fingerprint Authentication

3.2 For Notes

Fig. 3.2 Flowchart for Notes

Step1) after access, the note will open where at home page you can see one menu option in which you can Add notes

Step2) saved notes will be visible in the homepage

Step3) you can edit the notes and delete the notes too.

4. RESULTS

Fig. 4.1 Homepage

Fig. 4.1 shows the home page of the app when the app runs. This app will ask to place the fingerprint to access.

Fig. 4.2 Verified

Fig. 4.2 shows after placing the finger on the sensor if the required fingerprint matched then you can access the app.

International Journal of Technical Research & Science

Fig. 4.3 Failed

Fig. 4.3 shows if the fingerprint does not match the required fingerprint, then it shows the error.
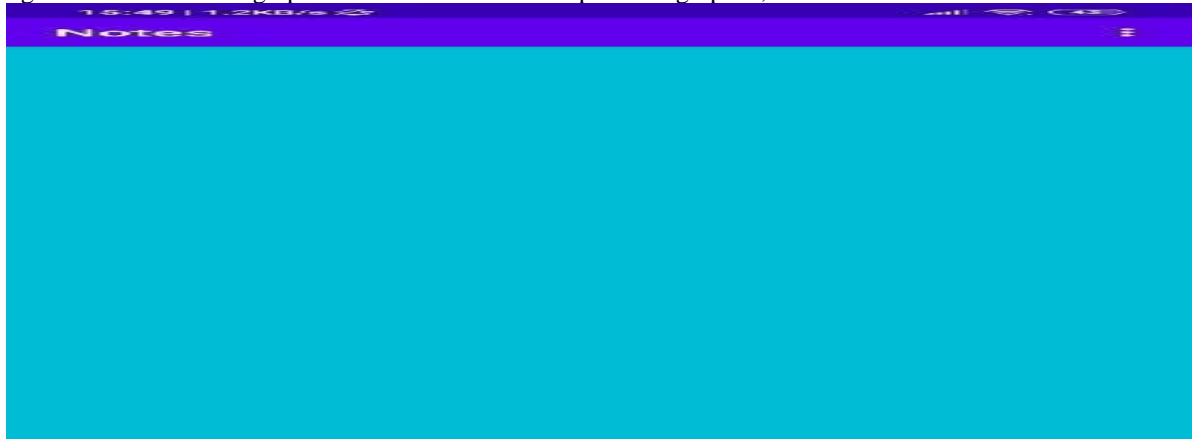

Fig. 4.4 Notes Home

Fig. 4.4 shows after successfully matching the fingerprint the app gets access to the notes and the home page of the notes.
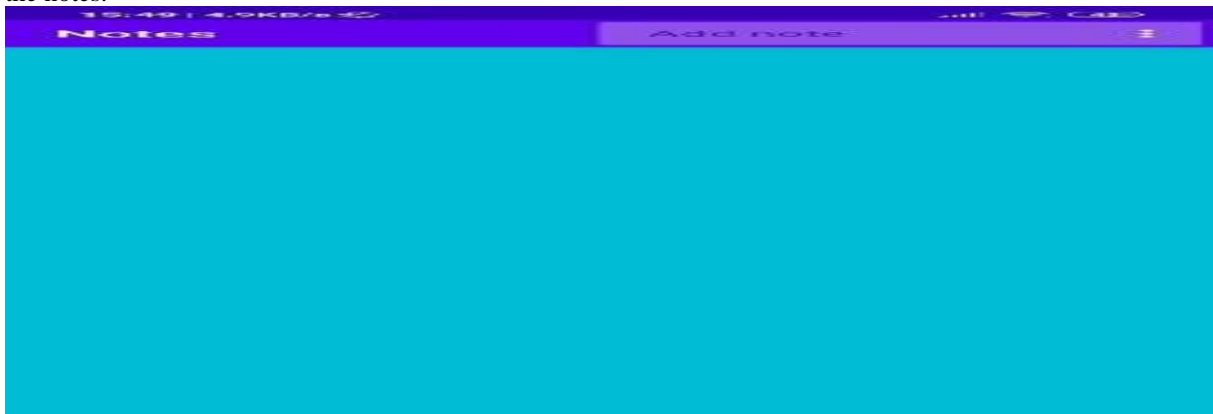

Fig. 4.5 Option Menu

Fig. 4.5 shows on the home page there is one option menu at the right top from which we can add notes.

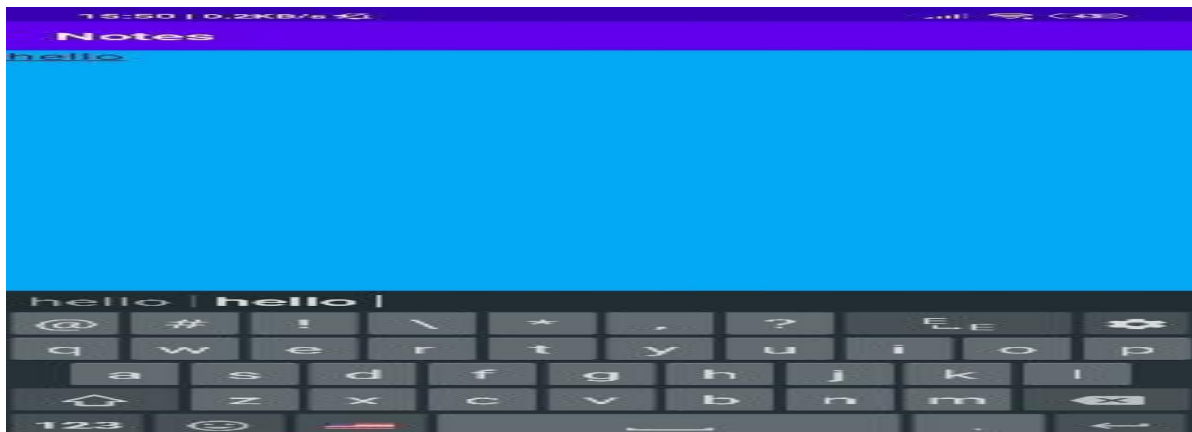**Fig. 4.6 Writing Page**

Fig. 4.6 shows an example of writing any note. To save the required note user have to press back button, then it gets saved.
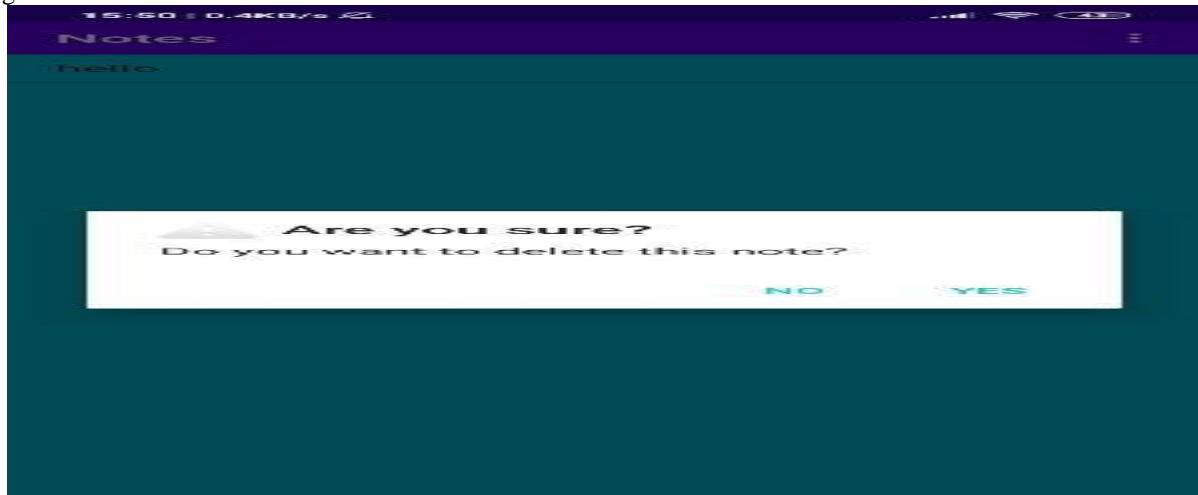

Fig. 4.7 Deletion

Fig. 4.7 shows the saved notes will be visible on the home page of the notes and to delete the notes user has to long-press the noted then the dialogue box appears as shown in the figure and from there we can delete by selecting yes.

CONCLUSION

Cell phones fluctuate from easy to brilliant just as modest to costly. The utilization of cell phones isn't just to convey yet additionally to make sure about information, and data like passwords, bank subtleties, and so on this information can be abused when cell phones are lost or taken. So, security assumes a significant job. On the off chance that there is appropriate security gives to the telephones to get to, at that point this abuse of information is impossible. Unique mark validation innovation is presently days adjusted my numerous versatile enterprises in view of its higher security gave. Unique mark Validation implies confirming an individual dependent on natural attributes, for example, unique mark, face, voice, and retina. The upside of unique mark verification over biometric validation is better and higher security. All the individuals on the planet have their various fingerprints even the twins have various fingerprints.

REFERENCES

[1] Varsha J. Rathod, Nalini C. Iyer, Meena S M, A Survey on Fingerprint Biometric Recognition System, 2015 ICGCIoT.
[2] Guoqiang Li, Christoph Busch, and Bian Yang, A tale approach utilized for estimating unique mark direction of curve finger impression, Norwegian Data Security Research center of Gjovik College School.
[3] Vladimir I. Ivanov and John S. Baras, Authentication of Fingerprint Scanners, Institute for systems research, University of Maryland, USA.
[4] Neha Kudu and Dr. Sunil Karamchandani, Biometric Identification System using Fingerprint and Knuckle as Multimodality Features, EXTC Department DJSCOE, Villeparle (W) Mumbai.
[5] PavanShrivastava, Sushil Kumar and Vijay Choudhary, Delta Compression Effect on Smart Card Fingerprint Verification System, IIT Bhopal, India.
[6] Qinghai Gao, Effectiveness of authenticating users with randomly constructed fingerprint templates, Department of Criminal Justice & Security Measures, Farmingdale State College, Farmingdale.
[7] Nancy Singla, Manvjeet Kaur, Sanjeev Sofat, Secure Fingerprint Fuzzy Vault Including Novel Chaff Point Generation Method, Department of CSE, PEC University of Technology, Chandigarh, India.
[8] Mohamed Labby, Yassine Ismaili, AbdelbakiAttioui and AbderrahimSekkaki, Performance Analysis of minutiae-based fingerprint matching algorithms, Casablanca, Morocco.
[9] S. O. Ojo, T. Zuva and S. M. Ngwira, Survey of Biometric Authentication for E-assessment, CSE, Tshwane University of Technology, Tshwane, South Africa.
[10] Subba Reddy Borra, G. Jagadeeswar Reddy, E. Sreenivasa Reddy, A broad Survey on Fingerprint Recognition Systems, IEEE WiSPNET 2016 Conference.