Mobile Banking Transaction Using Fingerprint Authentication

Lokesh Sharma
M. tech Scholar
Dept. of Computer Science
MACERC, Jaipur
lokesh.maiet@gmail.com

Manish Mathuria
Associate professor
Dept. of Computer Science
MACERC, Jaipur
manishmathuria@outlook.com

Abstract:Mobile banking services have become one of the most important applications on the Internet, being provided by most of the banks all over the world. The end-user can manage the accounts or make some payments without being forced to go to the physical bank office. That's why security concerns regarding authentication have to be taken into the account and the bank should provide various and combined methods for login and payment, in order to increase the confidence in their services for mobile banking. This research paper will introduce some concepts about these two fields: Mobile banking and fingerprint authentication process. During our researches, we developed a Java based Mobile application to simulate access to Mobile Banking for login and payment options. We also perform sample test for this application and as a result, we found it is very secure and 100% successful and user-friendly.

Keywords: ***Mobile banking , Fingerprint authentication, Two Way Authentication***

I. INTRODUCTION

The smart phone revolution in India has paved way for an unprecedented growth of Mobile Commerce and Mobile Banking in India. The Mobile banking services are playing a significant role in the interactions between consumers and financial service providers. The unique feature of Mobile banking is that it enables Anywhere Anytime Banking and is the most convenient and easy way to stay connected to the bank. Banks are permitted to offer Mobile banking services (through SMS, USSD or Mobile banking application) after obtaining necessary permission from the Department of Payment & Settlement Systems, Reserve Bank of India. Mobile banking services are made available to bank customers irrespective of the mobile network. It virtually allows consumers to do all their banking activities such as obtaining financial account information, conducting financial transactions with their financial institution and allowing consumers' to transfer money and make credit card payments anywhere[6]. These services have recently broadened with array of options like banking transaction details, viewing of account balance, mini statement, third party transfer of funds, utility bill payments features etc. has led to a surge in Mobile banking transactions. With the advent of Mobile banking, banks have also embraced Mobile Applications popularly called as Apps.

II. LITERATURE SURVEY

Lupu, CătălinandVasile-Gheorghiţă Găitan have proposed a technique for security enhancement for online banking authentication process. First thing, this process was not affordable for the Mobile Banking and another thing it require another special biometrics device for fingerprint authentication. [1]

The similar research work is discussed by Venugopal, Hridya, and N. Viswanathand they have proposeda good method in online banking with a robust and secure authentication mechanism. The main issue was with this method that based on the feature set from multiple data files. So that was very slow and it will consume more time for the authentication and was not fit for mobile banking. [2]

Yıldırım, Nilay, and AsafVarol have implement a two-way authentication scheme for the mobile banking login but they didn't implement any security or authentication feature at payment time and that was main issue of this implementation. Another problem with this implementation was that only work for a particular device. [3]

As reviewed, the research paper on"One-time biometrics for online banking and electronic payment authentication." by Plateaux and Aude provides a concept for security as a one-time biometrics. This context requires that authentication is realized by the bank and not only by the user(or by the personal device) contrary to standard banking systems.[5]A paper "Usable security of authentication process: New approach and practical assessment." By Althobaiti, Maha M., and Pam Mayhew describes and analysis different different security mechanism for authentication processes and at end of paper they conclude and told that Fingerprint biometrics is more effective , usable and good approach as compare to other biometrics technique. [4]

III. THE PROBLEMS WITH PASSWORD-BASED AUTHENTICATION

Password-based authentication is one of the most popular approaches to authenticate a user in various Mobile applications. But there are many problems associated with the password based authentication systems and the risks associated with using passwords as an authentication mechanism for enterprise applications is not completely secure. One of the main problem with password-based authentication is that most users either don't know, how much password should be strong. Extra rules that increase complexity are seen to drive call volumes for password-related issues to help desks proportionately. This problem can result in IT and management letting password standards slip and as a result passwords of shorter length and complexity tend to happen, such as simple seven character words. These passwords can be cracked in a matter of a few short minutes making them almost as ineffective as no password at all or a password that is discovered from a sticky note, either in use or carelessly discarded. While those avenues need to be guarded against, passwords also need to be less predictable to machines. There are so many method to crack the password through Guessing, Brute Force Cracking, Dictionary Attacks or other common methods.[9]

Downside:

Security vs. Ease-of-Use for Passwords

Single high-value target

Does not provide strong identity

Weak and susceptible to numerous attacks.

Shoulder Surfing Attack

IV. SYSTEM ANALYSIS AND DESIGN

- **Biometric Modality:**The most common biometric modality is fingerprint. The other types of modalities include gait, vascular, retina and facial thermography. There are two types of biometrics such as behavioral biometrics and physical biometrics. Behavioral biometrics are related to the behavior of a person and it can be used for verification. Physical biometrics are related to the shape of the body and it can be used for either identification or verification. Biometric system components consists of sensor, signal processing algorithms, data storage, matching algorithm and decision process. At first sensor collects data and converts the information to a digital format. Algorithm(s) perform quality control activities and create the biometric sample/template. Then the data storage keeps information that new biometric sample/template to one or more templates in data storage. Finally decision process uses the results from the matching component to make a system level decision.[8]
- **Fingerprint Recognition:** Human(s) used fingerprints for personal identification for many years and the matching accuracy using fingerprints have shown to be very high as compare to other biometrics technology. Fingerprint recognition is one of the best known and most widely used biometric technologies. An image of the fingerprint is captured by mobile device's scanner, enhanced and converted into a template.Biometrics which refers to automatic identification of a person based on his or her personal physiological or behavioral characteristics is inherently more reliable and more capable in differentiating between a reliable person and a fraudulent imposter than traditional methods such as PIN and passwords. Automaticfingerprint identification is one of the most reliable biometric technology among the different major biometric technologies which are either currently available or under investigation. [7]
- **Proposed secured fingerprint authentication:** This project is to suggest Biometric Authentication possibilities in Mobile Banking. The Banks are now successfully securing the mobile banking with User Ids and Passwords. But still there are various security aspects and threats for mobile banking. So enhancing the existing security is a must. This technology evolution is inevitable. Now there are mobileshave biometric

verification inbuilt, for Login with Finger Print Sensing. This same verification method can be integrated to Mobile Banking applications as well. During our study in this paper, we were able to develop a Java bases android application that can: (i) acquire the fingerprint of the user; (ii) do the enrollment and store the template in a database; (iii) do the verification of the user and then perform the transaction/payment.

We implement **two factor authentication** for login that mean just after open the application, user will enter username and password and after that next step will be fingerprint authentication. After the correct authentication process, user will be on the Home screen of the Mobile banking application.

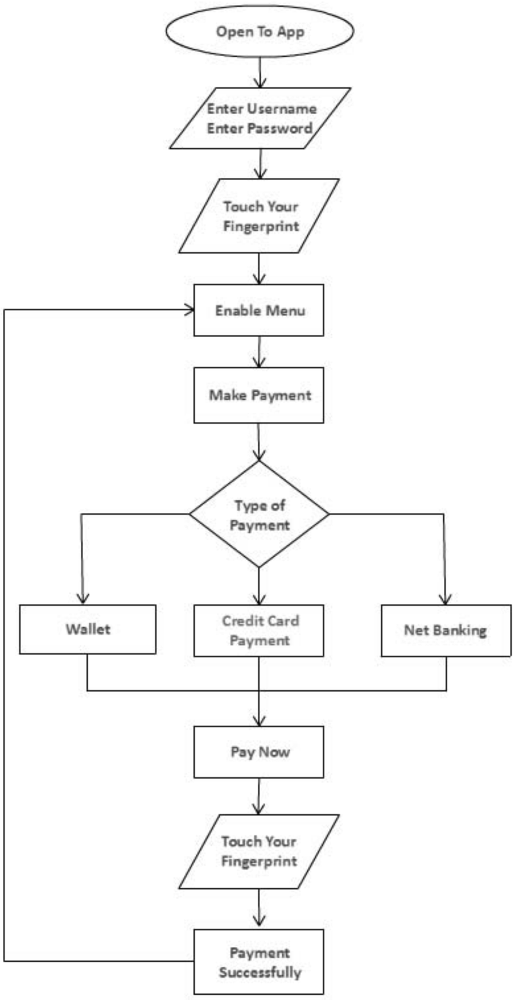
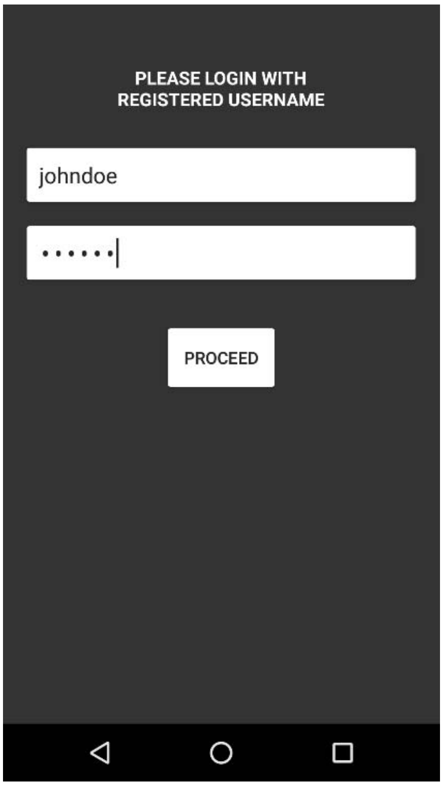


Fig 1. App Flow Chart

Development of a Mobile Banking application: This phase has been split to sub modules like

A. *Login Module: (Two Factor Authentication)*

Step 1-Login verification with the user name and password. After successful validation of the credentials it passes to Fingerprint authentication screen.

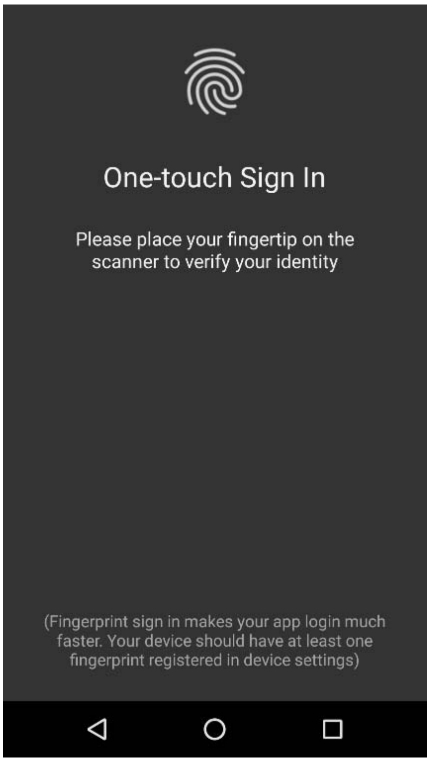

PLEASE LOGIN WITH
REGISTERED USERNAME

johndoe

••••••

Fig 2. Login verification with user name & password

Step 2- After successful Fingerprint authentication, it passes to the Home Screen otherwise none can be reach at Home Screen.


One-touch Sign In

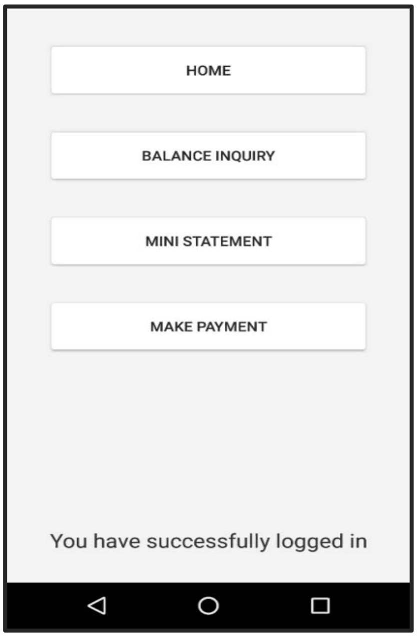
Please place your fingertip on the scanner to verify your identity

(Fingerprint sign in makes your app login much faster. Your device should have at least one fingerprint registered in device settings)

Fig3. Fingerprint authentication

B. Menu Display Module:

After successful two way authentication, Menu Screen will appear that contain four main basic feature: Home, Balance Inquiry, Mini Statement and Make Payment.



You have successfully logged in

Fig 4. App Menu

C. Payment Module:

If user select Make Payment option, at the next screen three category will show and every screen have Pay Button. Just after click on the **Pay** button again user need to authenticate him/herself by using fingerprint authentication. After successful Fingerprint authentication amount will transfer to the respective category like: Net Banking, Credit Card Payment, and Wallet.

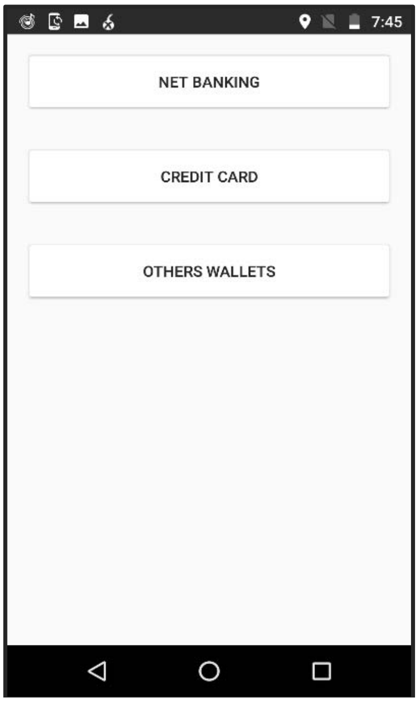
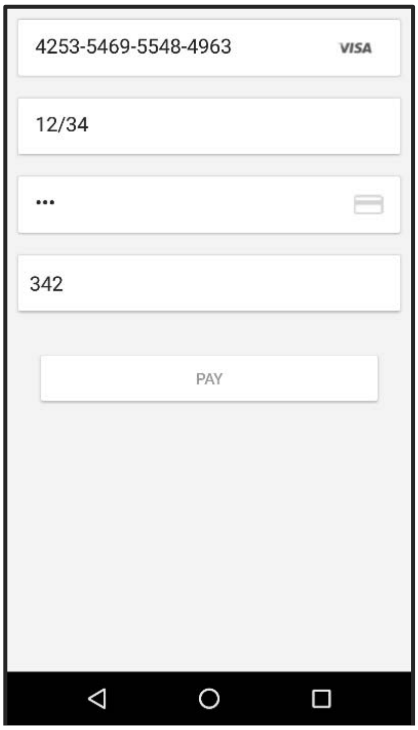


Fig 5. Types of payment method

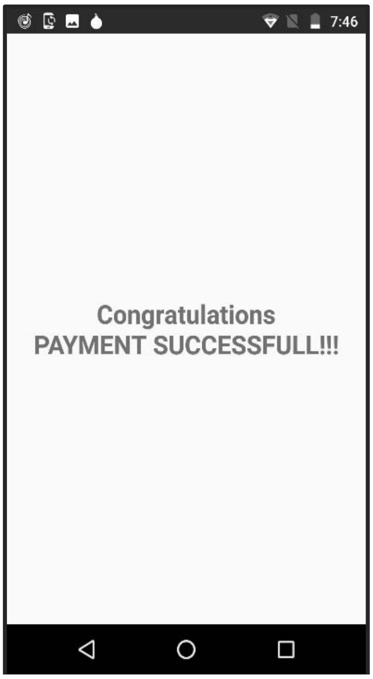

4253-5469-5548-4963 VISA

12/34

•••

342

Fig 6. Credit card details screen


7:46

Congratulations
PAYMENT SUCCESSFULL!!!

Fig 7. Payment successful screen

D. *API/GUI Development:*

Developing API/GUI that is Application Program Interface or Graphical User Interface for the Finger Print Sensor to be used.

- Fingerprint Scanner and API Source Code Collection
- Modifying the API to compatible GUI

E. *API Integration:*

Integrating the API/GUI to the Mobile Banking application such that the API is used to authenticate the Login and Payment process by Fingerprint authentication.

- Integrating the API/GUI to respective modules of the Banking Application

F. *Application testing:*

- We test this mobile application in different phases like Unit Testing, Integration testing and System Testing.
- We run this application more than thirty types of different android devices at different conditions to test the performance of the application (Samsung Galaxy S8, One Plus 3T, Lenovo K3 Note, Moto Google Nexus 6 and many more…).

V. CONCLUSION

Mobile-Banking industry in today's technology is facing several major challenges and issues. First and perhaps most important is the security concern. Customers are certainly concerned of giving their bank account information online or paying an invoice through internet. Another challenge facing mobile-banking industry and theE-business in general is the quality of delivery serviceincluding both delivery speed i.e., short advance time required in ordering and delivery reliability which meansdelivery of items or services on time. Mobile-banking application at present is using the username and password security mechanism which can easily reached by mere guess workand password can be hacked. To reduce the potential vulnerabilities regarding to the security, a combination of userid & password and fingerprint recognition system seem to be one of the most reliable means of authentication in a, mobile banking application environment. In order for mobile banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of mobilebanking can be very prosperous. The future of mobile banking will be a system where users are able to interact with theirbanks "worry-free" and banks are operated under one common standard.

REFERENCES

[1]. Lupu, Cătălin, Vasile-GheorghiţăGăitan, and ValeriuLupu. "Fingerprints used for security enhancement of online banking authentication process." Electronics,Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on. IEEE, 2015.

[2] Venugopal, Hridya, and N. Viswanath. "A robust and secure authentication mechanism in onlinebanking." Green Engineering and Technologies (IC-GET), 2016 Online International Conference on. IEEE, 2016.

[3] Yıldırım, Nilay, and AsafVarol. "Android based mobile application development for web login authentication using fingerprint recognition feature." Signal Processing and Communications Applications Conference (SIU), 2015 23th. IEEE, 2015.

[4] Althobaiti, Maha M., and Pam Mayhew. "Usable security of authentication process: New approach and practical assessment." Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, 2015.

[5] Plateaux, Aude, et al. "One-time biometrics for online banking and electronic payment authentication." InternationalConference on Availability, Reliability, and Security. Springer International Publishing, 2014.

[6] Dr.GomathyThyagarajan “MOBILE BANKING – A REVIEW”International Journal of Management and Social Science Research Review, Vol.1, Issue.14, Aug - 2015. Page 175

[7]Ali, Mouad MH, et al. "Overview of fingerprint recognition system." *Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on*. IEEE, 2016.

[8] Rabie, Ahmad, and Uwe Handmann. "Biometric for home environment challenges, modalities and applications." *Information Technology and Computer Applications Congress (WCITCA), 2015 World Congress on*. IEEE, 2015.

[9] Kirushnaamoni, R. "Defenses to curb online password guessing attacks." *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*. IEEE, 2013.