ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 1, January 2017

Survey on Biometric Authentication in Mobile Banking

Gaurav Ogale[1], Pranita Hatte[2], Anand Sutar[3], Pratik Chaudhari[4], Prof.A.M. Wade[5]

B. E Students, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India

Asst. Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India

ABSTRACT: Cell phones are evolving very rapidly making manufacturers introduce various features in small devices. Features like fingerprint sensor, high resolution camera provides developers various tools to integrate them into one application. Mobile banking is very popular these days due to large development in smartphone industry. Digital era helps us to use various means of banking methods. To make secure payments through mobile phones new secure authentication methods must be used. Biometricsare considered as one of the most effective authentication for everyone. A person can be uniquely identified using biometric system. We intend to give brief survey about various biometric parameters and also fingerprint authentication is proposed in this paper.

I. INTRODUCTION

Biometric is the technology used for identifying individuals uniquely by using their physical, chemical and other characteristics. Biometric systems assume that every individual has different physical traits like fingerprints. These traits can be used for authentication purposes, In this case in our proposed architecture we are using fingerprint sensor for authentication [1].

Today, mobile devices have become an important part of human life. Users access their e-mails, social networks, bank accounts, and various other websites via mobile devices. This paper gives a brief survey about why we should prefer biometric system compared to the traditional ones used in mobile phones and also propose architecture of a system based on fingerprint authentication. Biometric systems are more reliable and convenient than the traditional systems in comparison to security provided to mobile phones. Different biometric technologies discussed here are face, fingerprint, iris, retina, hand veins, key strokes [1]. Variant parameters decide whether the given biometric technology is suitable for that application or not. Parameters discussed here are universality, uniqueness, permanence, collectability, performance, acceptability, circumvention.

However,these various biometric methods also have various limitations like in face recognition aging of the user, bad light quality affects recognition rate. Voice recognition can be affected by illness, coughetc. Fingerprintauthentication also gets affected due to some injury on finger or dirt on it [2]. Traditional systems use one step or two step authentication like PIN, location of device etc. But these authentication methods depend upon lot of other supporting tools, hence biometric form of authentication is good way.

Elements of biometric system consists of [1]

- A sensor unit which is connected with system.
- A processing unit, which takes input from sensor and performs actions on that.
- A database unit, where all the data about respective user is stored and this data is retrieved for authentication purpose.
- A matching unit that compares latest template with the one stored in database.

.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 1, January 2017

II. LITERATURE SURVEY

Mobile banking which is today's generation need, also is, scalable, efficient and reliable privacy preserving method. Mobile banking is also at theft. So, to prevent these Biometric securities for cell phones [1] uses biometric parameters for the security system. They also compared different biometric means for authentication on various parameters. The comparison table based on their selected parameters like universality, uniqueness etc. is shown in the Table:1

To work for the implementation of Fingerprint authentication, Robust Privacy Preserving Fingerprint Authentication [3] uses widely adopted minutiae based fingerprint authentication system. This paper also includes the modification for BosworthMatcher. The description of Bosworth Matcher can be given as this algorithm consists of 3 steps.

1. Constructing intra-fingerprint minutia-pair tables.
2. Constructing inter-fingerprint pair-pair (compatibility)table by comparing the two intrafingerprint minutiae pair tables, where sufficiently similar minutia pairs are considered to be compatible.
3. Traversing the inter-fingerprint compatibility table to build a web and accumulate a match score

While performing mobile banking we also need to authenticate the original account holder, Biometric Authentication System Based on Delaunay Indexing Method [4], introduces a new triangular method to do so. This is known as Delaunay Triangulation Indexing (DTI). DTI stores non invertible biometric index values in the server side rather than storing template in the database

Attendance System on Android Smartphone [5] provides the architecture for the fingerprint authentication system we are interested in. They used fingerprint for means for authentication in their android platform. Authentic Mobile-Biometric Signature Verification system [6] presents an authentic mobile verification system and comparative analysis of this system for different datasets. This paper also removes the drawback of physical biometrics. Their proposed architecture depends upon signature generated by the user. The generated signature is matched with the one user stored during the registration phase of the system

Personal Authentication Using Fingerprint Biometric System [7] introduces a fingerprint enhancement algorithm in the minutiae extraction module. It also put forth a high speed fingerprint authentication algorithm which improves the ridge and valley structure of input fingerprint image. A Note on Fingerprint Recognition System [2] presents an overview of different fingerprint recognition systems. It compares all the existing recognition methods. Fasskey [8] presents an identity authentication system which is cryptographically strong and is able to run on mobile devices and can be extensively used for banking. Android Based Mobile Application Development for Web Login Authentication Using Fingerprint Recognition Feature [9], [10] introduces fingerprint authentication for development of secured web login authentication mobile app. A new way of authenticating an online purchase by using asymmetric key obtained from android keystore.

Biometrics	Universality	Uniqueness	Permanence	Performance
Face	High	Low	Medium	Low
Fingerprint	Medium	High	High	High
Keystroke	Low	Low	Low	Low
Iris	High	High	High	High
Voice	Medium	Low	Low	Low

Table 1: Comparison of various biometric technologies

III. PROPOSED ARCHITECTURE

The systems we are proposing assume that there is some mean of biometric sensor associated with the device like in this case we are using fingerprint sensor associated with smartphone. There are three main sections of architecture user, sensor and database. Figure 1 shows the proposed architecture. Flow of execution

1. Application is initialized on the mobile.
2. once application is initialized it will ask user to touch his finger on fingerprint sensor

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

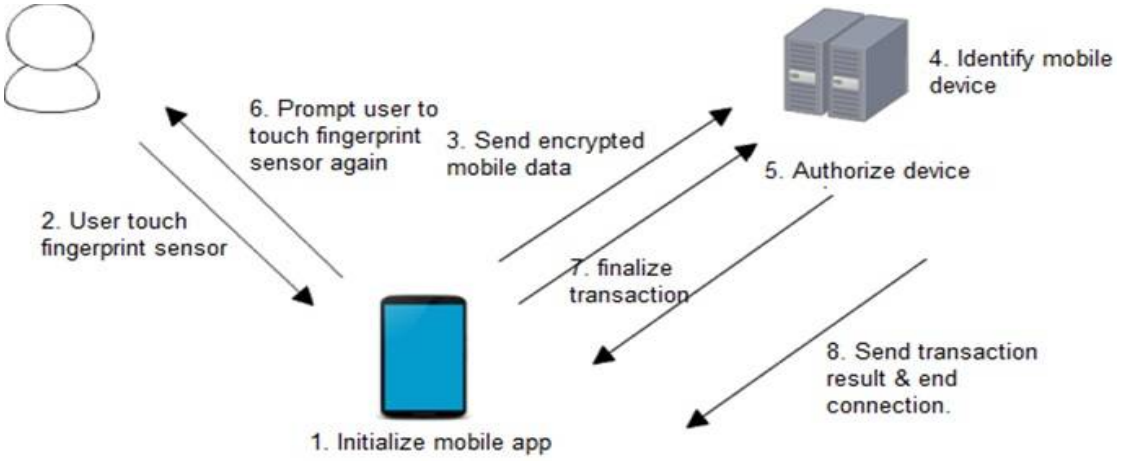

Figure 1: Proposed Architecture

3. Biometric template is generated once user touched sensor. This biometric template is used for further authentication purpose. This template is encrypted using advance encryption standard and sent to the server/database.
4. A matching unit/server identifies the user by comparing generated template with the stored template.
5. The device and user is authorized by the server.
6. Now user will able to see all his saved payment cards on the application screen.He will select one of the saved card and the application again prompt user yo touch fingerprint sensor again to complete transaction.
7. Again new template is generated which is used for matching .After authentication the transaction user intended for is complete.
8. All the transaction history is prompt on the screen.

IV. CONCLUSION

Using biometric authentication method in mobile banking reduces various fraudulent activities which in turn increases security and provides the user with safe and reliable transaction. This system also increases the trustability of the user. Various biometric authentication methods and an architecture consisting of fingerprint authentication proposed in this paper will have high uniqueness, performance and permanence.

REFERENCES

1. Adrian pocovnicus. *Biometric Security forCell Phones. Informatica Economic vol. 13, no.1/*, 2009.
2. R. Rajesh B. ShanmugaPriya. *A Note on Fingerprint Recognition Systems. IEEE*, 2011.
3. Ye Zhang and FarinazKoushanfar. *Robustprivacy-Preserving Fingerprint Authentication- IEEE International Symposium on HardwareOriented Security and Trust (HOST)"*,3
4. Prof S.Maria Celestin VigilawberkinAlbert Antony. *BiometrieEneryptionsystembasedon Delaunay Indexing Method. International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]*, 2013.
5. Echo SimanjuntakFergyanto E. GunawanenfanoSoewito, Ford LumbanGaol. *AttendanceSystem on Android Smartphone. 2015 International Conference on Control, Electronics,Renewable Energy and Communications (ICCEREC)*, 2015.
6. SuraiyaJabinFarhanaJavedZareen. *Authenticmobile-biometric signature verification system.The Institution of Engineering and Technology2016*, 2016.
7. Mrs. V. Evelyn Brindha V Prasathkumar. *Personal Authentication using Fingerprint Biometric System. International Journal of InnovativeResearch in Computer and Communication Engineering*, 2014.
8. Heejo Lee John Milburn. *FASSKEY: A Secureand Convenient Authentication System*. 2015.
9. AsafVarolNilayYlldmm. *Android Based MobileApplication Development for Web Login Authentication Using Fingerprint Recognition Feature*.2015.
10. Http://android-developers.blogspot.in/2015/10/newin-android-samples authenticating.htm.