ISSN 2349-6193
Impact Factor: 2.805

IJESMR

International Journal OF Engineering Sciences & Management Research

SECURITY IN MOBILE BANKING: A BIOMETRIC APPROACH

Simranjeet Kaur*
*Assistant Professor(Computer Science), Panjab University Constituent College, Nihal Singh Wala,Punjab,India

Keywords: *biometric, quantitative analysis, authentication, mobile banking*

ABSTRACT

In present day world, mobile banking has emerged as a winner among various banking services. The major concern for mobile banking is its security. Since present authentication methods such as passwords, OTPs do not offer high level of security, there is always a risk of fraudulent attacks. To avoid this risk, reliable authentication procedures must be used. Biometric serves the purpose of reliable authentication mechanism. The paper gives the overview and quantitative comparative analysis of various physiological and behavioral biometric techniques that can be used in mobile banking. Various criteria that have been used for analysis are uniqueness, universality, permanence, circumvention, performance, and collectability and acceptability.

INTRODUCTION

Mobile banking is the most popular and prevalent norm of financial transactions among millions of users. Reason behind the rapid spread of mobile banking is its convenience and cost effective delivery channel of various banking services[1].According to RBI report, from 2010 to 2012, the number of users of mobile banking services has grown from 5.96 million to 22.51 million and the value of transactions has grown from Rs. 6.14 billion to Rs. 59.90 billion. These figures clearly indicate that mobile banking in the country is growing at a very high rate. According to latest RBI report, there is a rapid growth in total value of transactions of mobile banking. From 2012 to 2014, value of mobile banking transactions has reached 4017.8 billion [2].

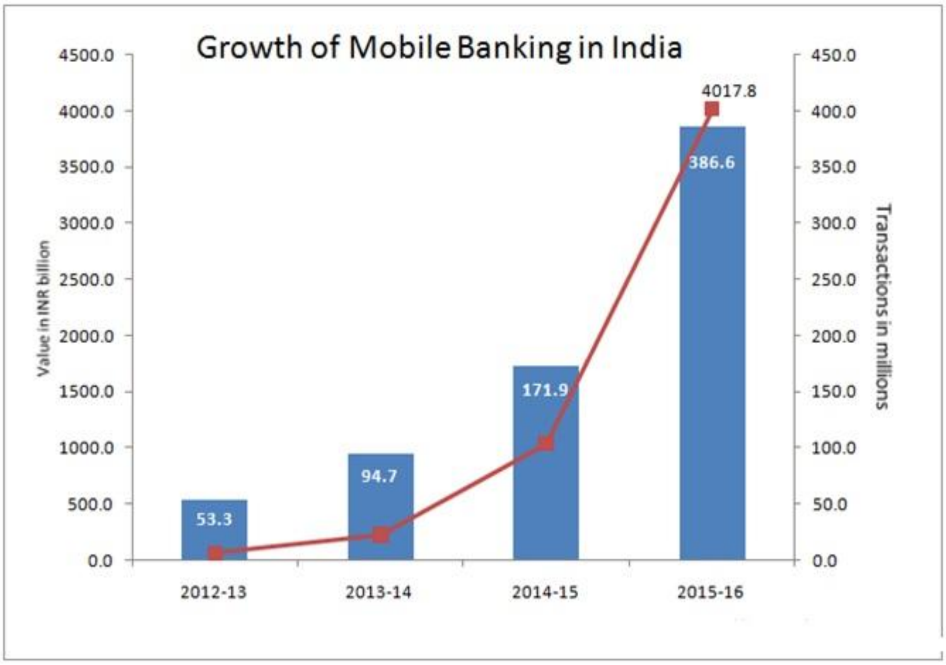

Fig 1 - Growth of mobile banking in India. Data Source: Reserve Bank of India

There is no doubt that mobile banking has proven to be most convenient way of using banking services. But, along with various benefits, mobile banking exposes itself to various types of security risks. Major concern for mobile banking is to prevent unauthorized access. Considering the increasing number of financial frauds, a reliable authentication system must be incorporated. Biometric systems are known to be most reliable authentication systems, because they have the potential to solve many security problems [3]. "Biometrics" is defined as "the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioral traits" [4]. Biometrics is widely used across various fields like forensics, ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. But apart from its wide usage it is still not implemented in mobile banking. Fig 2 shows proportion of using biometrics in different operations.

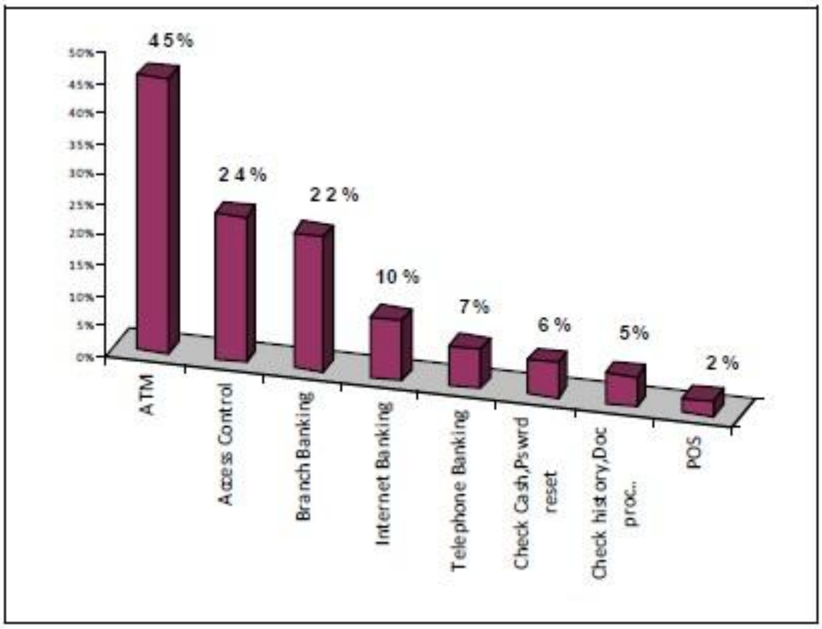

Fig 2- Proportion of using biometrics in different operations [15]

AUTHENTICATION SCHEMES IN MOBILE BANKING

In mobile banking, there are mainly two types of authentication schemes used i.e. single factor authentication and multi factor authentication [5].

Single Factor Authentication

Single factor authentication refers to the use of authentication credentials i.e. user name and password. Disadvantage of this scheme is that the passwords can easily be guessed and stolen by using different algorithms [5].

Multi Factor Authentication

Multi factor authentication makes the use of mainly two different factors i.e. something you have and something you know. It involves combination of two factors i.e. static passwords and one time passwords generated by small devices. Although this scheme provides higher level of security than single factor authentication, but it is not reliable. There is always a risk of unauthorized access to mobile devices so the OTPs can be easily stolen [6].

Considering the shortcomings of single factor and multi factor authentication schemes, it is concluded that more reliable authentication mechanism must be incorporated in mobile banking. In this context an analysis of various biometric techniques is required so that best of them can be used for the authentication system.

AN OVERVIEW OF BIOMETRIC TECHNIQUES

Biometric techniques have been categorized based on two features i.e. physiologic features and behavioral features. Physiological features include finger print recognition, Iris recognition, DNA recognition, Hand vein recognition and behavioral features include signature verification, voice recognition etc. [7]

Finger Print Recognition

Finger print recognition is one of the oldest and most widely used biometric techniques. In this, finger prints of an individual are used for authentication purpose. Finger prints are graphical ridges present on a finger that are saved as a template that can be matched later. The reason for popularity of this method is its distinctiveness and stability. However some environmental factors like sweating and grease on fingers can make the recognition difficult [8, 9]

Iris Recognition

High resolution images of iris of an individual’s eye are used for pattern matching in Iris recognition. As compared to finger print recognition, images of an iris can be used for lifetime because iris is an internal organ and it will not change over a longer period of time. However, some medical and surgical procedures can affect the color and shape of Iris [8].

Hand Vein Recognition

Veins are carrier of blood to heart. Every individual possess a unique structure of veins. So veins can be used for authentication purposes. Vein recognition is getting popularity because of its higher level of accuracy and relatively low cost of installation [8].

Face Recognition

This is the most commonly used biometric technique. Recognition is based on the facial features of a person. Images of various facial features are stored based on the location and shape of features. The measurements are stored and comparison is made when a person stands in front of the camera. Major disadvantage of this method is that it may be ineffective when facial expressions of a person change [10].

Signature Verification

Signature verification is based on the calculations of the movements of the pen while signing. This is not an image comparison method. Special devices are used to identify movements in all the three directions. Major disadvantage of this method is that the signatures can easily be falsified [10].

Voice Recognition

In this method, voice signals are converted into electrical signals and then compared with database. These systems operate with user’s knowledge. However, wrong voices cannot always be avoided. Biggest drawback of this scheme is that the system may be hacked with prerecorded voice messages [11].

GENERAL SCHEME OF A BIOMETRIC SYSTEM

There are three main functionalities of a biometric authentication process which are given below [12]:

Enrollment

process of acquiring, accessing and storing data in the form of template for later use is called enrollment.

Verification

verification is the process of matching between stored template and biometric. Matching score is provided between 0 and 100%.Although no system ever reach to 100%.

Identification

process of identifying an individual from a number of database values is called identification. Access may be granted to user or the user can also be rejected.

IJESMR
International Journal OF Engineering Sciences & Management Research

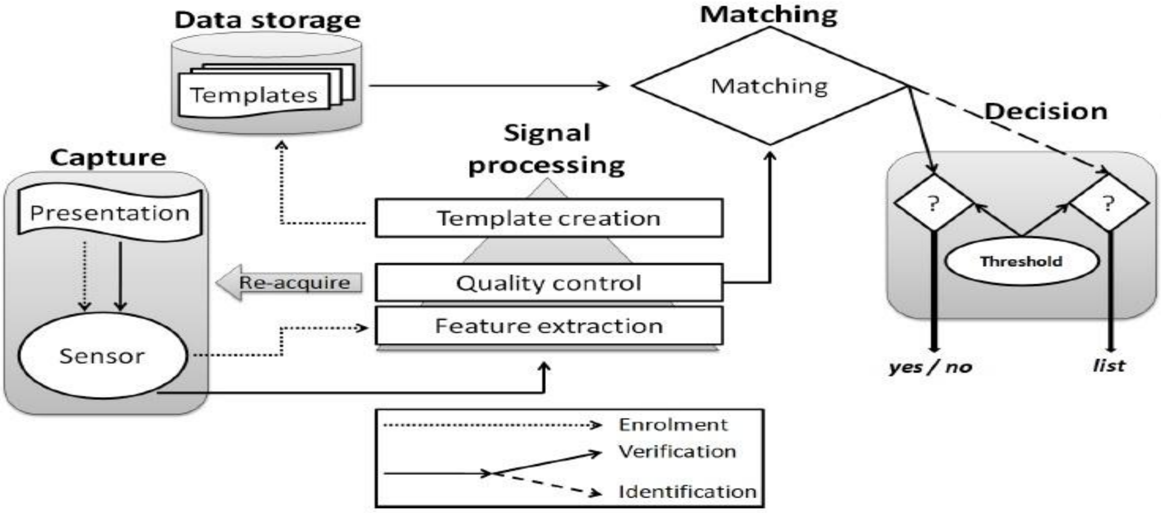

Fig. 3- General scheme of biometric system[13]

COMPARISON OF BIOMETRIC TECHNIQUES BASED ON THEIR PROPERTIES

Biometric techniques are mostly characterized by seven properties [13, 14]. These properties have been used as criteria for comparison.

- **Universality:** Every individual must have this property.
- **Uniqueness:** It should be distinct for two different individuals.
- **Permanency:** it should be preserved for lifetime of an individual.
- **Collectability:** it should be easily measured.
- **Acceptability:** it measures the use of a particular biometric system by users.
- **Performance**: it indicates the achievable accuracy, speed and robustness of the biometric property
- **Circumvention:** it relates to ease with which a biometric system can be circumvented or bypassed.

Table 1: Comparison of various biometric techniques based on seven criteria

Biometric technique	Universality	Uniqueness	Performance	Collectability	Acceptability	Resistance to Circumvention	Permanence	Total	reference
Fingerprint	2	3	3	2	2	3	2	17	[13]
Face	3	1	2	2	3	1	2	14	[13]
Iris	3	3	3	2	1	1	3	16	[13]
Signature	1	1	1	3	3	3	1	13	[13]
Voice	2	1	1	2	3	3	1	13	[14]
Hand Vein	2	2	2	2	2	1	2	13	[14]

DISCUSSION

Table 1 refers to the comparison between six biometric techniques i.e. Fingerprint recognition, Face recognition, Iris Recognition, Signature recognition and hand vein recognition. Comparison is based on seven criteria which are characterized by three levels i.e. Low, Medium and High [13, 15]. In order to do quantitative analysis, numerical values have been assigned to these three levels i.e. 1 refers to low level, 2 to medium level and 3 to high level.

Table 2: Ranking of Biometric techniques

Sr. No	Biometric	Total value
1.	Fingerprint	17
2.	Iris	16
3.	Face	14
4.	Signature	13
5.	Voice	13
6.	Hand Vein	13

In this study, six biometric techniques which are more applicable to mobile banking have been chosen for analysis. Table 2 refers to ranking of biometric techniques. Based on total values of seven indicators, Fingerprint recognition is the highest ranking biometric feature, Iris recognition is second and Face recognition is placed on third rank which is followed by Signature, Voice and Hand vein recognition. Biometric systems require hardware implementation for proper functioning of the system. Fingerprint, Iris and face recognition require scanners for recognition. Since most mobile phones are equipped with these scanners nowadays days so it will be easier for banks to include biometric features in financial transactions. In order to achieve higher level of security, biometric systems can be combined with passwords.

CONCLUSION

Since traditional authentication methods used in mobile banking such as passwords, tokens etc. do not assure high level of security, it is clear that use of biometric system is imperative for security in mobile banking. This paper presents overall quantitative analysis of various biometric techniques so that appropriate technique can be incorporated in mobile banking. From above analysis, it has been inferred that Fingerprint recognition is best among six biometric techniques used for comparison. Future work will focus on studying and analyzing more important features other than above mentioned. Another scope for future work is to analyze various problems and security risks involved with Biometric systems

REFERENCES

1. *https://www.rbi.org.in/SCRIPTs/PublicationReportDetails.aspx?UrlPage=&ID=243 accessed on 10-03-2017*
2. *http://www.itnext.in/article/2016/05/16/mobile-banking-growth-continues-4-fold-increase-2015-16 accessed on 10-03-2017*
3. *W. Khalifa, M. I. Roushdy, and A.-Babeeh M. Salem "A Rough Set Approach for User Identification Based on EEG Signals", Egyptian Computer Science Journal (ECS), Vol.38, No. 3, ISSN 1110-2586, September 2014, pp. 43-50*
4. *D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar," Handbook of Fingerprint Recognition. Springer-Verlag", 2003*
5. *Silvia Parusheva, "A comparative study on the application of biometric technologies for authentication in online banking ", Egyptian Computer Science Journal, 2015*
6. *Sameer Hayikader et al.," Issues and Security Measures of Mobile Banking Apps", International Journal of Scientific and Research Publications, Volume 6, Issue 1, January 2016*
7. *Harpreet Saini1, Kanwal Garg2,"Comparative Analysis of Various Biometric Techniques for Database Security", International Journal of Science and Research (IJSR)), Volume 2 Issue 4, April 2013*

8. *Kalyani Mali1 , Samayita Bhattacharya2,"Comparative Study of Different Biometric Features ", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013*
9. *Ms. C.B. Tatepamulwar1, Dr. V. P. Pawar2," Comparison of Biometric Trends Based on Different Criteria", Asian Journal of Management Sciences, 2014.*
10. *K P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface ", International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011*
11. *Renu Bhatia ,"Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013*
12. *Mohamad El-Abed, Christophe Charrier, "Evaluation of Biometric Systems", New Trends and Developments in Biometrics, pp. 149 - 169, 2012*
13. *P. Stavroulakis, M. Stamp,"Handbook of Information and Communication Security", Springer Science&Business Media, 2010, p. 139*
14. *K. Sharma, A. J. Singh"Biometric Security in the E-world", in: "Cyber Crime: Concepts, Methodologies, Tools and Applications: Concepts, Methodologies, Tools and Applications", IGI Global, 2011, pp. 507-514*
15. *Seyyede Samine Hosseini, Dr. Shahriar Mohammadi," Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System" ,Journal of Basic and Applied Scientific Research,2012*