ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

SECURE MONEY TRANSACTIONS USING BIOMETRICS

[1]S.K.Vimaladevi , [2]S.Sharmila,[3]Dr.G.Vijaya M.E.,Ph.D
[12]IV – B.E (CSE),[3]HOD/CSE,
[123]Kalasalingam Institute Of Technology
[1]vimalakasthuri6@gmail.com,[2]sharmila.cse22@gmail.com,[3]viji.pooshan@gmail.com

Abstract:

Most authentication schemes are vulnerable to observer attacks because user has to explicitly input a secret , for instance a password , that positively identifies her . By observing user input , an imposture can capture the secret(password) and later to use it. A survey shows that there is no proper security in transaction cash. There are no proper authentication methods applied for security during transactions. In this paper, security approaches of ATM or mobile devices has been focused on and has been improved using biometric and password based authentication technique i.e.fingerprint recognition.Here the proposed system provides more security then existing system with finger print recognition because of finger print is unique.

Keywords-*Secure Banking Internet, Fingerprint-Based Authentication, Password Verification.*

Introduction

Nowadays Online banking Transactions is increasing everywhere in the world.Users are using their ATM cards, Credit cards,Debit cards,etc.for making Online payment for various types of purchase.biometrics in bankingThe rapid digitization of banking services combined with the continued need to adopt stricter customer and employee identification protocols to prevent identity theft and fraud has set the table for biometric identification technology to become an integral and strategic part of financial service security platforms. Acting as a strong authentication tool to help secure ATM, brick and mortar, and online transactions, biometrics in banking also helps to increase customer trust and improve brand reputation. The necessity for a stronger authentication solution became inevitable in banking services because of the growing pace of sophisticated transactional technology adoption along with the unfortunate rise in fraud and security breaches due to reliance on traditional security systems such as passwords.

Many mobile device makers now corporate biometric security features into their products. And, some device manufacturers now allow application developers to use these features via their software development kits (SDKs). In this study, we utilize fingerprint scanning and recognition technology, a popular biometric security feature, to develop a login authentication mobile app. With a frame, the secure passwords can be used to sign in/log in to online user accounts related to government, banking, education, etc. As the production of mobile devices with fingerprint recognition continues to increase, finger print user authentication apps, like the one we introduce in this study, will become a prevalent security measure.

ComputersystemsconnectedtotheInternethaveg rownmoreprobabletoincreasinglySophisticated

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

attacksbyabusingoftheirremote access ports . Byeavesdropping or "sniffing" on network connections ,attackers can obtain login ids and passwords of legitimate users.

Currentlyexisttocombatthissituation.Theproblemswiththesecurrentimplementationsare:

- Thehardwareunitstorestheuser'ssecretpassword.Iftheunitisstolen,thethiefcangenerate.
- Theuser'sOTPforaccesstothecomputersystem,regardlessiftheattackerknowstheuser'sSecretpassword.
- Theuserchoicesaweakpasswordtoremembrwhichcouldleadtoattacksbasedonspecifics.
- **Biometrics**

The word “biometrics” comes from the Greek language and is derivedfrom the words bio (life) and metric (to measure). This paper will refer tobiometrics as the technologies used to measure and analyze personalcharacteristics, both physiological and behavioral. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional security methods by providing twomajor improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes. Since biometrics can better solve the problems of access control, fraud and theft, more and more organizations are considering biometrics a solution to their security problems. However, biometrics is not a panacea and has some hurdles to overcome before gaining widespread use. This paper will discuss the recent history of biometrics, benefits of biometrics over traditional authentication methods, some of the most widely used biometric technologies and the issues surrounding biometrics to include issues standing in the way of widespread biometric implementation.

Objective

The motivation for this project was lack of security while doing the online transaction using previousauthentication techniques. As anyone can hack username and password and make money transfer or any othermalicious activity. So it is necessary to provide strong security for online banking. So we are providing securityusing different biometric factor of a user as they cannot be stolen easily.

Literature Review

Security Experts says that Automatic Teller Machine (ATM) in future will have biometric authentication techniques to verify identities of customer during transaction. In South America, there are companies that have introduced fingerprint technology as a embedded part of ATM systems, where citizens have already started using fingerprint in place of PIN or Password for general identification with their ID cards. Gregg Rowley said- “Banks will move to smart cards and biometric will be next step after that “[10]. Bank has already been moved to smart cards and now is the time to implement biometric authentication approach in ATM systems. Nowadays, there are devices to perform biometric identification and authentication of following: fingerprint, hand, retina, iris, face, and voice. Rowley says, ”Most insecure is a magnetic stripe with a PIN, more secure is a smart card with a PIN, and even more secure is a smart card with biometrics” [10]. India is still lacking in implementing biometric with smart card as a safety approach. Various ideas

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

are given by researchers for biometric authentication including- fingerprint, iris and retina, voice, etc. Fingerprint approach for identification given by Oko S. and Oruh J. (2012) not proved efficient as when citizen will move to ATM system, fingers may become dirty from natural environment and will not be able to access his account with ATM system, since fingerprints will not match from the one that was traced during identification. Secondly, a iris and retina approach proposed by Bhosale S. and Sawant B.(2012) as a identification method, but citizens might not want a laser beamed into their eyes for retina scan at every time he wants to access account through ATM. Thus, iris and retina as identification authentication proved inefficient. Vibration detector sensor were also proposed as a security system for ATM machines by Ajaykumar M. And Bharath Kumar N.(2013). Voice was also proposed for security in ATM systems as a biometric with smart card. The cons were there at the same time as two citizens can have same voice and one can easily hack and can fraud with another's account. Thus, this paper came with an idea of finger recognition technique with 3 different angles as a biometric authentication that cannot be lost, stolen, harmful, dirty, copied, forgotten and is always available.

Existing System

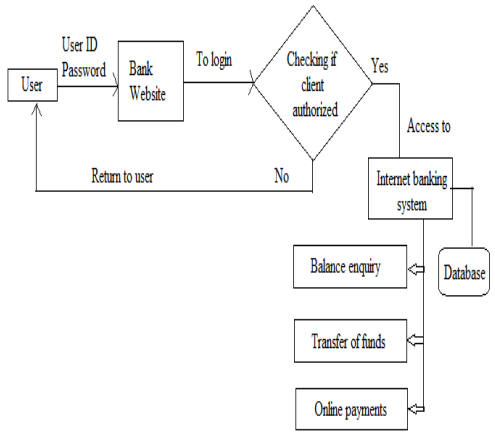


Figure 1 – Existing system flowchart

In the existing system the banking transactions are done by online using the username and password. Afterentering the amount the system sends an One time Password(OTP) on the registered mobile number and then afterentering the correct OTP the transaction is processed successfully. But it is not much secure as the OTP can bestolen or changed by anyone if our mobile is hacked or stolen. Thus, we need a more secure method for makingour online transactions. Therefore, we use a fingerprint biometric for identification of the user.

Proposed System

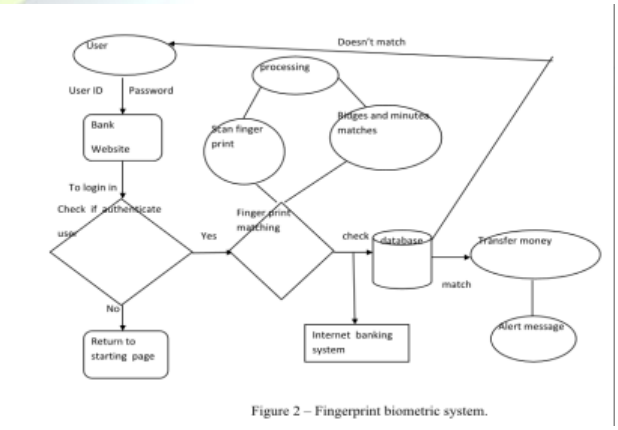


Figure 2 – Fingerprint biometric system.

The proposed system is an application developed using the fingerprint security

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

feature for device. We will discuss the importance of fingerprint security applications and the development stages of our fingerprint login authentication program in this paper. Fingerprint recognition for mobile payment transactions can deliver mobile payments safer way. As an example, Pay Pal and Sam sung Galaxy S5 users can make payments via Pay Pal using fingerprint biometric.In this paper, we present an application developed using the fingerprint security feature for a Samsung device. We will discuss the importance of fingerprint security applications and the development stages of our fingerprint login authentication program in this paper.

Advantages of Using Finger Print

- Uniqueness–Each individual has a unique fingerprint. No two people have same fingerprint patterns .
- Biometrics cannot be forgotton, lost, duplicated or stolen.
- It is more secure as it cannot be shared or used by others.
- If any one transaction an unlimited amount to others , it stored in database, easily find out the particular persons who having Black Money.

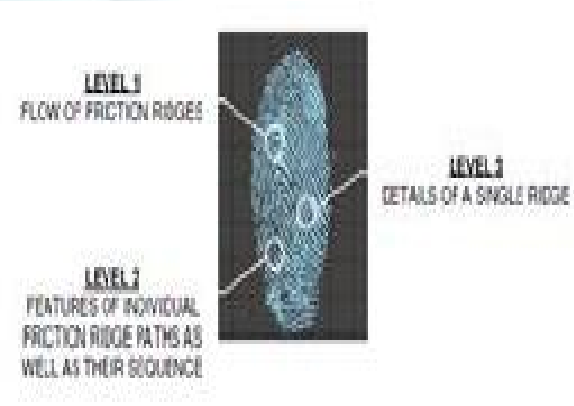
Finger Print Recognition

Finger Print technology is the initial bio metric sciences and uses unique features of the fingerprint to verify or identify of individuals. It is most deployed technology among other bio metric characteristics, used in application ranging from physical access and logical access. Each and every human have unique characteristics and patterns. A Finger Print pattern or sample consists of lines and spaces. These lines are referred as ridges while the spaces between these ridges are called valleys. These ridges and valleys are matched for verification and authorization. These unique finger print traits are referred as “minutiae” and comparisons are made on these traits. The typical live scan produces 40 “minutiae”.[5]. There are five stages in finger scan verification and identification they are finger print image acquisition, processing, location of distinctive characteristics, template creation and template matching. Image acquisition stage involves preprocessing, such as scaling. Image processing is the process of improving the appearance of an image. These results in a series of thick black ridges contrasted to white valleys [6]. In this process image features are detected and enhanced for verification against the stored minutia file. Image enhancement is used to reduce the distortion of fingerprint caused by scars, cuts and dirt [7]. The next stage in the finger process is to locate particular distinctive characteristics. Finger print ridges and valleys form particular patterns such as

i)Arch: The ridges enter from side of the finger then rise in the center which forms an arc then exit the other side of the finger.

ii) Loop: The ridges enter from side of a finger, forming curve then exit on that same side.

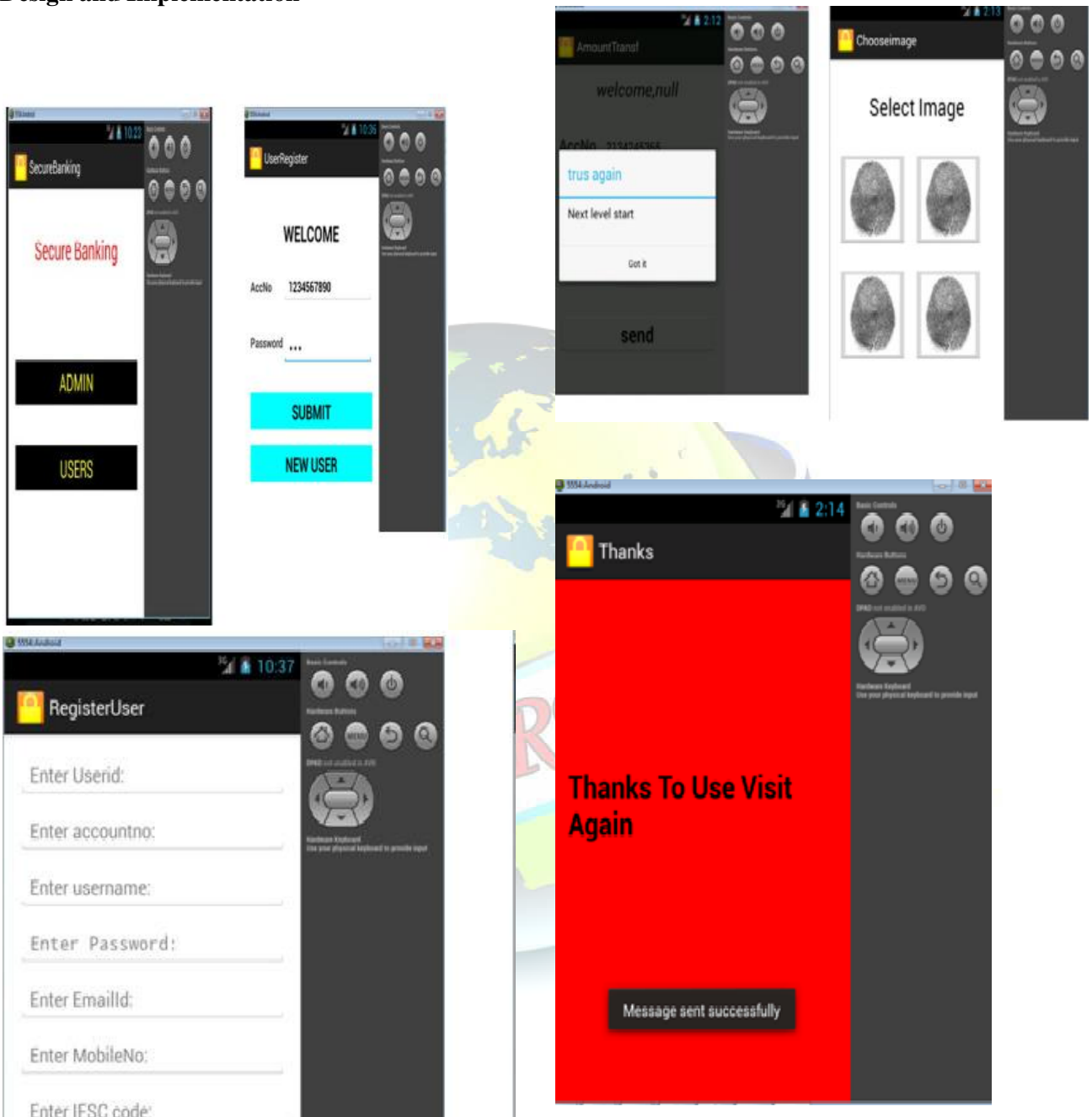
iii) Whorl: Ridges form circularly around a central point on the finger.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

Design and Implementation



The above shown Figures represents that the system for making online banking transaction

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

using a fingerprint biometric. The system first takes Username and password from the user and checks if they are correct. After successful login the system asks for the fingerprint of the user.

We design a challenge-response authentication system. That is, the system asks the user a question (challenge), to which the user has to properly respond to prove her identity. To thwart observation attacks, rather than hiding the response, we choose to hide the challenge.

Completely hiding the challenge may prove a difficult task, especially when considering usability factors. As illustrated in Figure 2, we instead choose to hide part of the challenge, by breaking it into two halves. The first half of the challenge is conveyed through a visible (and hence, observable) channel, while the second half of the challenge is conveyed through a hidden channel. The user mentally reassembles both parts of the challenge, and, using her authentication token(s) as an input, answers the reassembled challenge. The authentication system can verify the answer by combining its own knowledge of the authentication token(s) with its knowledge of what was sent on the hidden channel.

An off-line image is obtained by smearing ink on the fingertip and creating an impression of fingertip on the paper using ink. A live-scan image, is acquired by sensing tip of finger directly, using a finger app. Live-scan is done with the help of finger app .

After scanning the fingerprint the minutiae features are extracted from it and storedin form of template and matching is done further, then do process for transactions for particular account through Online via mobile phone or ATM system.

Conclusion

This project is developed on the basis of more need of security in Online Transactions system. Now-a-day's ATM is getting less secure with emerging ways to hack/crack ATM PIN or ATM card.Another important point in proposed system is that it demands lesser changes to the present system of Bank and ATM. That means lesser overhead will be required to change the whole system with enhanced security. Changes in Hardware part will be required that is one fingerprint scanner is required to be attached to ATM machines. This project will needs to explained to end user, to educate the user to use this system.

References

[1] European atmsecurity [Online]. Available: https://www.european-atm-security.eu/atm-industry. [Accessed: 12 Nov 2014].

[2] Kristin s. Fuglerud and Oystein dale "Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client" IEEE J. Security & Privacy,Volume: 9, Issue: 2, Pages 27-34, March-April 2011.

[3] Sunil Lohiya "Biometric identification and verification techniques -A future of ATM Banking System", Indian Streams Research Journal, Volume 2, Issue. 7, Aug 2012

[4] Biswas S., Bardhan Roy A., Ghosh K. And Dey N.,"A Biometric Authentication Based Secured ATM Banking System", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012