International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

BIOMETRIC BANKING TECHNOLOGY TO SECURE ONLINE TRANSACTIONS WITH FEASIBLE BIOMETRIC DEVICES

[1]V. Sai Venkatalakshmi, [2]N. Deivanayaki, [3]A. Risvanul Jannah

[1]M.E student, [2]Associate Professor, [3]Assistant Professor

[1, 2] Department of CSE, PET Engineering College, Tamilnadu, India

[1]vsaivenkat1992@gmail.com

[2]cse.deivanayaki@petengg.ac.in

Abstract— This paper deals with the design of a biometric security system based upon the fingerprint, face and voice recognition. Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices. Now a days thieves are using high tech methods to gain access to user information such as passwords, PINs and security questions. Even tokens are not safe to perform online transactions. This paper aims at enhancing the security of Internet banking system with additional Biometric Authentication combination. Internet banking now uses Static User ids and passwords along with OTP-One time Passwords to our mobile. Although this is the best security feature available to date, this security method is still vulnerable and it is very important to enhance the existing security. The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological behaviours. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. Biometrics is not into Internet banking applications yet. It is because of the practical difficulties and it is very expensive to implement and execute this technology. But, now with technology advancement and cost of Biometric devices coming down, we have probabilities to integrate Biometric Technology to Online Banking. Some important gadgets like Laptops and Mobiles are now coming with Biometric integration like inbuilt finger print sensor, face detection and voice recognition. This paper is to propose the methods and possibilities of integrating Biometric technology to Online banking applications with such gadgets thus visualizing the future possibilities of Biometric Authentication in Online Banking. Indian Government's Digilocker facility already successfully integrated fingerprint authentication feature to sign up and link aadhar card to the system.

***Keywords*— Internet Banking, One time passwords, Biometric authentication, fingerprint sensor, face detection, voice recognition.**

1 INTRODUCTION

As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems is becoming extremely important especially in the banking and finance sector. There are more and more highly fraudulent technologies in today's Internet Banking like Phishing, Fake Emails and Phone Calls imitating to be sent from Banks, Trojan Horse Programs to capture user ids and passwords, Threats like Skimmer devices to duplicate our Debit and Credit Card details etc. So it is very important and urgent need to enhance Internet Banking Security.

Biometric systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system. In this case, the biometric data obtained from the user is compared to the user's data already stored in the database. Identification occurs when the identity of the user is unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database.

Biometrics is used on several applications such as computer logon and airport security. Biometrics can be used to identify you as you. Biometrics holds the promise of fast, easy to use,

accurate, reliable and less expensive authentication for a variety of applications. Another key aspect is how "user-friendly" a system is. The process should be quick and easy such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. As biometric technologies mature and come into wide scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

2 RELATED WORKS

Utilizing biometrics for internet banking will be considerably more accurate than current methods of Verification pins and passwords. This Biometric can be an additional authentication thus enhancing the existing security. There are two types of Biometrics (Physical and Behavioral). Fingerprint, Face Detection, Iris Scan, Vein Patterns and DNA are some of the Physical Biometrics. Voice, Keystroke and Signature are some of the Behavioral biometrics. Implementing Biometrics to any application has to consider the following factors. Cost Efficiency – It has to be cost efficient to fit the budget and competition, Accuracy and acceptability – How accurate the technology is and how much it is reliable and can be accepted, Practical Implementation and execution – How practical the technology was to implement and to execute. Biometrics is not into Internet Banking Applications, considering the above factors. It was practically impossible so for. Another practical difficulty is, in the Finger Print Sensing which is the most used Biometric Technology; there is no universal or unique method or algorithm for finger print sensing. Every manufacturer of these sensors has their own verification algorithms, software's and drivers. So there are no finger print sensors to be used universally. But development of API's that is Application Programming Interface for each such sensor is now becoming a common thing with the manufacturers. Thus Universal application will be created in near future that will work with any sensors. Hence this technology can be integrated to any system with help of such APIs. Today's technology is advancing. Biometric device productions are increasing and cost of such devices are coming down. This technology is Booming. Now mobiles and Laptops are launched with inbuilt Finger Print Scanner and Face detection technology. In future we can predict every gadget will impose a biometric authentication technology with it. So implementing a Biometric Authentication for Online Banking is very much possible in near future.

3 SYSTEM ANALYSIS AND DESIGN

3.1 Biometric Modalities

Common biometric modalities are fingerprint, face, iris, voice, signature and hand geometry. 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. Signal processing algorithms perform quality control activities and develop the biometric template. Then the data storage keeps information that new biometric 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.

3.2 Fingerprint Recognition

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints have shown to be very high. Fingerprint recognition is one of the best known and most widely used biometric technologies. An image of the fingerprint is captured by a scanner, enhanced and converted into a template. Scanner technologies can be optical, silicon or ultrasound technologies Accurate automatic personal identification is critical in wide range of application domains such as national ID cards, electronic commerce and automatic banking. 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. Automatic

fingerprint identification is one of the most reliable biometric technology among the different major biometric technologies which are either currently available or under investigation.

3.3 Face Recognition Technology

Face Recognition has long been a goal of computer vision but only in recent years, reliable automated face recognition has become a realistic target of biometrics research. The facial recognition process normally has four interrelated steps. The first step is face detection, the second is normalization, the third is feature extraction and the final cumulative step is face recognition.

3.4 Detecting a face

Face Detection is the process of automatically locating human faces in visual media. A face that is detected is reported at a position with an associated size and orientation. Once a face is detected, it can be searched for landmarks such as the eyes and nose. Face tracking extends face detection to video sequences. Any face appearing in a video for any length of time can be tracked. That is, faces that are detected in consecutive video frames can be identified as being the same person. A landmark is a point of interest within a face. The left eye, right eye and nose base are all examples of landmarks. The face API provides the ability to find landmarks on a detected face. Classification is determining whether a certain facial characteristics is present. For eg, a face can be classified with regards to whether its eyes are open or closed. Another example is whether the face is smiling or not.

3.5 Normalization

Once the face has been detected, the face needs to be normalized.This means that the image must be standardized in terms of size, pose, illumination, etc., relative to the images in the gallery or reference database. To normalize a image, the key facial landmarks must be located accurately. Facial landmarks are the key to all systems, irrespective of the overall method of recognition. If the facial landmarks cannot be located, then the recognition process will fail. Recognition can only succeed if the probe image and the gallery image are the same in terms of pose, orientation, rotation, scale, size, etc., Normalization ensures that this similarity is achieved to greater or lesser degree.

3.6 Feature Extraction

Applying human visual property in the recognition of faces, people can identify face from very far distance, even the details are vague. That means the symmetry characteristic is enough to be recognized. Human face is made up of eyes, nose, mouth and chin etc. There are differences in shape, size and structure of those organs so the faces are differ in thousand ways and we can describe them with the shape and structure of the organs so as to recognize them. One common method is to extract the shape of the eyes, nose, mouth and chin and then distinguish the faces by distance and scale of those organs.

3.7 Face Recognition

Face recognition, authentication and identification are often confused. Face recognition is a general topic that includes both face identification and face authentication (also called verification). On one hand, face authentication is concerned with validating a claimed identity based on the image of a face, and either accepting or rejecting the identity claim (one-to-one matching). On the other hand, the goal of face identification is to identify a person based on the image of a face. This face image has to be compared with all the registered persons (one-to-many matching). Thus, the key issue in face recognition is to extract the meaningful features that characterize a human face. Hence there are two major tasks for that: Face detection and face verification.

3.8 Proposed System

This project is to suggest Biometric Authentication possibilities in Internet Banking. The Banks are now successfully securing the Internet banking with SSL Certification, User Ids Passwords and OTPs to customer's mobile. But still there are various security aspects and threats for internet banking. So enhancing the existing security is a must. This technology evolution is inevitable. Now there are Laptops and mobiles

have biometric verification inbuilt, for Logon with Finger Print Sensing and Face Detection. This same verification method can be integrated to Banking applications as well. The idea is, when customer opens the Internet Banking page, after the password verification the application must look for the respective Biometric Device and then the respective biometric technology's API shall be called. During our study in this paper, we were able to develop a Java application that can: (i) acquire the fingerprint/face/voice 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.

Development of an Internet Banking application: This phase has been split to sub modules like

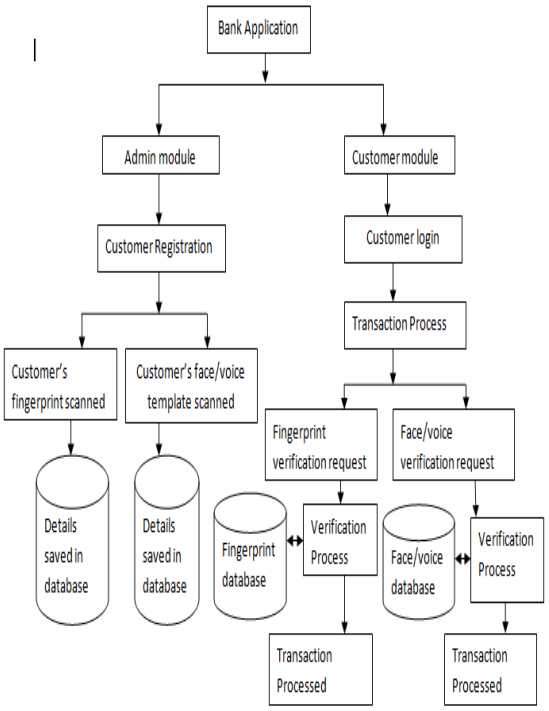
- Customer Registration Module : Customer Details are collected and registered to the Database
- Login Module: Login verification with the user name and password. After successful validation of the credentials it passes to next page.
- Details Display Module: Customer Details are extracted from the Bank Database and the Details are displayed in this module.
- Transaction Module: Transaction of amount to other accounts is to be processed after successful validation of details.

API/GUI Development:

- Developing API/GUI that is Application Program Interface or Graphical User Interface for the USB Finger Print Sensor to be used.
- Fingerprint Scanner Driver and API Source Code Collection
- Modifying the API to compatible GUI

API Integration:

- Integrating the API/GUI to the Internet Banking application such that the API is used to authenticate the Logon or Transaction process by Biometric face Verification.
- Integrating the API/GUI to respective modules of the Banking Application
- Trial and Error and Execution



VeriLook facial identification technology is designed for biometric systems developers and integrators. The technology assures system performance and reliability with live face detection, simultaneous multiple face recognition and fast face matching in 1-to-1 and 1-to-many modes. VeriLook is available as a software development skit that allows development of stand-alone and Web-based solutions on Microsoft Windows, Linux, Mac OS X, iOS and Android platforms. The VeriLook algorithm implements advanced face localization, enrollment and matching using robust digital image processing algorithms*:* Simultaneous multiple face processing. VeriLook 5.7 performs fast and accurate

detection of multiple faces in live video streams and still images. All faces on the current frame are detected in 0.01 - 0.86 seconds depending on selected values for face roll and yaw tolerances, and face detection accuracy. After detection, a set of features is extracted from each face into a template in 0.6 seconds.

4 Security Analysis

Biometrics is a rapidly developing branch of information technology. Biometric systems are becoming an important element for information security systems. Therefore biometric systems themselves have to satisfy high security requirements. Vulnerability analysis determines the imposter usage of the vulnerabilities with the aim of breaking the security policy.

Vulnerability assessment is the systematic checking of systems in order to determine the adequacy of security measures, to obtain the security weaknesses and to obtain data for forecasting effectiveness of proposed security measures. Vulnerability assessment is the sequence of the following steps and it consists of search for potential vulnerabilities, developing intrusion tests, making intrusion tests and processing of results and reporting.

There are some advantages of using biometrics keys as compared to traditional passwords. Biometric keys cannot be lost or forgotten. Biometrics keys are very difficult to copy or share. Biometrics keys are extremely hard to forge or distribute. Biometric keys cannot be guessed easily. Someone's biometrics is not easy to break than others. Offer significant cost savings. Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes.

5 Performance Evaluation

Existing Security includes SSL Certification, User Ids & Passwords, One Time Passwords(OTPs) to customer's mobile. But still there are various security aspects and threats for internet banking. So enhancing the existing security is a must. This technology evolution is inevitable. Now there are Laptops and mobiles have biometric verification inbuilt, for Logon with Finger Print Sensing and Face Detection. This same verification method can be integrated to Banking applications as well. Utilizing biometrics for internet banking will be considerably more accurate than current methods of Verification Pins and passwords. This Biometric can be an additional authentication thus enhancing the existing security.

6 Conclusion

This Paper proposes methods and possibilities of integrating biometric technology to online banking applications. In future we can predict every gadget will impose a biometric authentication technology with it. This idea has to be evolved yet. Some impaired people can't provide fingerprints. So the system must be adapted in order to satisfy this requirement, too. A more secure system shall use iris, face or other biometric characteristics, but in this case, the price of the device will increase. This fingerprint authentication shall be clubbed with existing OTP authentication method, and thus make it as a multi factor authentication for opting customers. To start, these biometric authentication methods can be implicated locally (at device level). In future it can be evolved to authenticate from server. The two fields presented in this paper (internet banking and biometrics) are really wide and the research on combining them can lead to better solutions and higher levels of security

References

[1]Anil K. Jain and Lin Hong- (1998) 'An identity Authentication System using Fingerprint' IEEE Transaction-Vol 86 No. 10 1998.

[2] Chatterjee and Nath- (2015) 'Biometric Authentication for UID Based Smart and Ubiquitous Services' - (CSNT), 5th International Conference.

[3] Green and Romney- (2005) 'Establishing Public Confidence in the Security of Fingerprint

Biometrics'-Information Technology Based Higher Education and Training.
[4] Gunajit Sarma and Pranav Kumar-(2002) 'Biometric Authentication'-International Journal of Pure Applied Sciences and Technology-ISSN 2229-6107,pp 67-68.
[5] John Daugman-(2004) 'How Iris Recognition Works'-IEEE Transactions on Circuits and Systems, Vol 14, No.1.
[6] John Trader-(2014) 'Impact of Biometrics in Banking'-IEEE Transaction-Vol 54.
[7] Kounoudes and Anastasis(2006)-'Voice Biometric Authentication for Enhancing Internet Service Security'-Information and Communication Technologies.
[8] Mangala Belkhede and Veena Gulhane(2006)-'Biometric mechanism for enhanced security of online transactions'-A Design Approach
[9] Marius Tico and Pauli Kuosmanen(2003)-'Novel Fingerprint Representation,-IEEE Transactions on Pattern Analysis and Machine Intelligence", Vol 25, No.8.
[10]Meraoumia and Bouridane-(2013) –'Multimodal Biometrics System'-IEEE Transactions on Electronic Circuits and Systems
[11]Quinghan Xiao-(2007)'Spoofing Technique'-IEEE Computational Intelligence.
[12]Raffile Cappelli and Dario Maio-(2002) 'Performance Evaluation of Fingerprint Verification System' -IEEE Transactions on pattern analysis-Vol 24, No. 3.
[13]Rohit Singh and Utkarsh Shah- (2012) 'Fingerprint Matching Techniques'-Social Behavioral and Sciences
[14]Sharath Pankanti-(2012) 'ATM Security using Fingerprint Biometric Identifier'-International Journal of Advanced Computer Science and Applications-Vol 3,No. 4.