Effective method of security measures in Virtual banking ---------- ---------- Dr.S.Arumuga perumal,Head, Department of Computer Science,S.T.Hindu College,Nagercoil-2,Tamilnadu, India, Web: http://chennai.sancharnet.in/vcec_ngc/index.html Email: visvenk@yahoo.co.in DR.S.Arumuga perumal is working as Reader and Head of the Department of Computer science in South Travancore Hindu college for the last 19 years. He has completed his M.S(Software systems) in BITS, Pilani, Rajasthan; M.Phil Computer Science degree in Alagappa university, Karaikudi and he did his Ph.D(Software Systems-Computer science) in Manonmanium Sundaranar University.He is a Senior member of Computer society of India. He is involved in various academic activities.He has attended number of national and international seminars, conferences and presented number of papers. He has also published number of research articles in national and international journals.He is a member of curriculum development in universities and autonomous colleges.His area of research is Digital Image compression, Data mining and Biometrics.

---------- Abstract

The development of Information Technology leads to the remarkable growth in the field of network security that is used in security applications, which shows the way to the development of Virtual Banking. The aim of this paper is to discuss the different security measures that are to be considered in Virtual banking system, to share the fundamental concept behind the security technology and to understand the relative advantages and limitations of different approaches. When passwords are used for authentication, the decision made is relatively straight forward, but in network security using biometric authentication the decision is made on a probability. Biometrics is not secret. Any organization considering the use of biometrics needs to understand the impact of this when reaching a trust decision. The success of a biometric authentication system will depend on the method used to combine the individual decisions or matching scores. With the increased prominence on security, there is a growing and urgent need to identify human both locally and remotely on a routine basis. Over the past decade, considerable advances have been made in algorithms for biometrics recognition. ----------

## Introduction

In E-banking system, information is considered as an asset and so worthy of protection. Information security can support a wide variety of objectives such as compliance with laws and regulations, reducing the fraud risk and reducing the risk of unauthorized access. The protection afforded to information is usually expressed in terms of confidentiality, integrality, availability and non-repudiation. Authentication has a significant contribution to provide all these services. Now days in Indian banking system, the authentication is done through password that is not up to the level of high security measure. There is an urgent need to acclimatize the security measure in the banking system.

## Virtual Banking

Any banking service delivered to the customer by means of a computer-controlled system that does not directly involve the usual bank's branch is called virtual banking. In virtual banking the traditional paradigm of a customer's integration with the bank is replaced by an electronic paradigm, which is new and innovative in banking sectors. Customer demands, commercial motivation and technological developments are the key drivers of virtual banking. In the changing environment adaptation to market realities as well as technology is causing the virtual banking revolution. Customer pull and banking push are the two engines to drive the virtualization.

## Factors to be considered in Virtual Banking

- The use of computers as accounting tool and also as a tool to expand and improve customer services
- The routine banking transaction was becoming both costly and time consuming. The banks resorted to computerization to cut cost and time overheads in handling routine transactions
- The introduction of automated teller machine (ATM) impart flexibility to bank customers and gave further boost to virtual banking
- The introduction of credit cards and debit cards helps both the consumers and retailers to be free from cash handling.

These payment systems save time and offered security in its rouse.

## Technology

Biometrics is one approach to the authentication of an individuals claimed identity. Recognizing individuals through observation of particular physical characteristics is known as biometrics. A biometrics authentication is a two-stage process. During the first stage, some sort of capture device is used to take a measurement of particular physiological or behavioral characteristics and in the second stage; the measurement is compared to a stored value. Based on the comparison result the system makes an authentication decision. Biometric technologies do not actually compare the physical traits that they are designed to use as a unique identifier, rather, they create templates for comparison. This enrollment process may require the individual to provide multiple instances of the biometric trait. The initial comparison templates are created during an enrollment process. Figure 1 shows the diagrammatic representation of a biometric authentication system.

**Figure 1 Biometric authentication system**

## Multifactor authentication

One way to increase the strength of an authentication mechanism is to use multiple factors of authentication. In the case of biometrics, this could involve requiring the user to input a password or PIN (Personal Identification Number) or to produce some sort of authentication token such as smart card that contains both the PIN and any one of the biometric systems with 1:1 matching. The advantage of such is that many are designed to operate with biometric systems and have sufficient space for storage of biometric templates with them. However, assessing the extent to which an additional authentication factor can increase the overall strength of the authentication services. When passwords are used for authentication, the decision is made relatively straightforward- if correct password is supplied the result is positive authentication, otherwise the individual is rejected. A biometric authentication is conceptually different, in that the decision is based on a probability. Any organization considering the use of biometrics needs to understand the impact of this when reaching a trust decision.

## Biometric authentication

Biometrics is a measurable physical characteristics or personal behavioral trait used to recognize the identity or verify the claimed identity of an enrollee. Examples of physiological characteristics that are used in biometric device include fingerprints, the geometry of the face or hand and patterns within the iris or retina or in the layout of veins. Behavioral characteristics include voice pattern, gait and the dynamics of handwriting or keystrokes. For the authentication process the chosen characteristics must be unique to each individual. Also it is possible to measure the characteristics with the reasonable degree of accuracy. Once the measurement has been taken the data is converted into a biometric template. A template is a representation of the measurement that retains all the relevant information but takes up far less space than the original. It is this template that is compared to a template generated in the same manner during the initial enrolment procedure and based on the similarity of the two, a decision is made whether the user should be granted access.

## Factors affected

For any particular individual, it is highly unlikely that two measurements of the same characteristics will be identical. There are simply too many factors that can affect the result. The measurement may be influenced by fluctuation in the environment such as light, heat, humidity and soon. The manner in which the users interact with the capture device also has an impact on the measurement. On different occasion; an individual is likely to behave slightly differently. So the physiological and behavioral characteristics vary over time. The following variation may cause the generation of different templates.

- Fingerprint worn with hard labor and age
- Voices are affected by illness
- Signature vary depending on the emotional state of the subject
- Face change over time by addition of glasses or by injury

## FAR/FRR

The permissible discrepancy between templates is determined by adjusting the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR gives the measure of the probability that an individual will be falsely accepted by the system (makes an incorrect identification). The FRR is the measure of probability of the rejection of legitimate user. The balance between the FAR and FRR greatly influences both the security and usability of the system. Tuning the system to make the FAR lower will improve its security will result in a higher FRR and make the system less consumable. The FAR/FRR balance may be adjusted; neither rate provides a suitable metric for expressing the overall accuracy of the biometric system. To compare the performance of the different biometric system the Crossover Error Rate (CER) can be used. The CER is defined as the error rate of the system when the FAR and FRR are equal.

## Verification and identification

Due to the advance development of technology, the cost effective, the processing power to employ and more accurate biometric identification systems are developed. There are two ways to resolve a person's identity: verification and identification. Verification involves confirming or denying a persons claimed identity, Identity is to establish a person's identity (Who am I?). Each approach has its own complexities and could probably be solved best by a specific biometric system including the following

## Physical Biometrics

- Finger print -Analyzing fingertip patterns
- Facial recognition location - Measuring facial characteristics
- Hand geometry - Measuring the shape of the hand
- Iris Scan -Analyzing features of colored ring of the eye
- Retinal scan -Analyzing blood vessels in the eye
- Vascular patterns -Analyzing vein patterns
- DNA -Analyzing genetic makeup
- Biometric data watermarking is used to store/hide biometric information

## Behavioral biometrics

- Speaker/Voice recognition system -Analyzing vocal behavior
- Signature/handwriting -Analyzing signature dynamics
- Keystroke/patterning -Measuring the time spacing of typed words

There are various biometric products and you'll encounter a plethora of fingerprint scanners, voice and facial recognition system, retina/iris scanners, hand geometry devices and signature verification systems. Table 1 illustrates the most common biometric systems in use today and their characteristics regard to accuracy, user identification and user acceptance

| Biometric system | Accuracy | Ease of use |
|---|---|---|
| Finger print | High | Medium |
| Hand geometry | Medium | High |
| Voice | Medium | High |

| | | |
|---|---|---|
| Retina | High | Low |
| Iris | Medium | Medium |
| Signature | Medium | Medium |
| Face | low | High |

**Table 1 Acceptance rate by the system**

The following is a general user acceptance list in descending order, from the most accepted to the least accepted

1. Iris scan
2. Key stroke/patterning
3. Signature/Handwriting
4. Speaker/voice recognition
5. Facial recognition/face location
6. Finger print
7. Hand geometry
8. Retinal scan

## Conclusion

The popularity which virtual banking services have won among customers, owning to the speed, convenience and round-the-clock access they offer, is likely to increase in the future. However, several issues of concern would need to be pro-actively attended. While most of electronic banking have built-in security features such as encryption, prescription of maximum monetary limits and authorizations, the system operators have to be extremely vigilant and provide clear-cut guidelines for operations. On the larger issue of electronically initiated funds transfer, issues like authentication of payments instructions, the responsibility of the customer for secrecy of the security procedure would also need to be addressed. So for the better security multifactor authentication is best so that Password with any one biometric system make the virtual banking with higher security in forth coming years. However, it needs to be recognized that such high cost technological initiatives need to be undertaken only after the viability and feasibility of the technology and its associated applications have been thoroughly examined.

## References


1. Automatic Minutiae Detection - http://bias.csr.unibo.it/research/biolab/bio_tree.html
2. Biometric Product Testing Final Report - National Physical Laboratory - http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf
3. National Institute of Science and Technology (NIST): Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability: November 2002, http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf
4. International Biometric Group - www.biometricgroup.com