International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Highly Secured Net Banking System Using Fingerprinting Recognition Technology

Pooja Diggavi[1], Pooja Patil[2], Krupa R[3], Padma S.K[4], Sridevi Malipatil[5]

[1, 2, 3, 4]Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary

[5]Assistant Professor, Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary

Abstract: ***Nowadays, the banking and financial systems have been changed due to the environment and globalization changes and competition of business services. Net banking become very popular with the general public or their availability and general user friendliness. Online banking is used to describe the banking transactions through the internet application. Web banking means user can login to his banks website by using his personal computer, smart phone or tablet etc. But one of the major problem with the internet banking is the inherent lack of security of traditional authentication techniques, passwords and passwords and pin numbers. So our system gives a solution with a fingerprint biometric of user in order to overcome from these problems.***

Keywords: secure internet banking, finger print recognition and authentication, minutiae, ridger, bifurcation and photo response

1. Introduction

In today's life style, security is one of the most important concerns. Technology is providing with this purpose. Online banking transaction is increasing everywhere in the world. users are using their credit cards ,debit cards, ATM cards etc, for making various types of online transactions. Users use their username, passwords, card number etc, for making online transactions. When users enters these details he gets a onetime password(OTP) on his registered mobile number. After entering this OTP correctly then only the transaction gets proceeded successfully. But there are many security problems like fraudulent websites, fake emails from banks, capturing user ID's and passwords, hacking personal bank accounts and ATM cards etc. So hackers can easily misuse the user's account. so security and authentication of individuals is necessary for our daily lives especially in net banking. Therefore, our system provides this authentication by using the biometrics of the user. Biometric is defined as a science which studies human's behaviors and physical characteristics to identify him/her. In our system user needs to provide his fingerprint biometric along with the username and password for further transactions. For this the bank initially stores all the users details along with his fingerprint. Our system will check for the biometrics of the user and match it with original biometrics in the bank's database. If a valid match is found then only the user is authenticated and treated as valid. Otherwise even if there is a small mismatch in the finger print the user is not allowed to access the bank account.

2. Problem Statement

- Inter**n**et Banking has relatively little effect on the current profitability of most banks.
- But hackers can easily hack the SSN(social service number) or PIN(personal identification number) using Brute force attacks

3. Biometric Overview

- Biometrics method of identification is preferred over traditional methods involving passwords and pin numbers because identification based on biometric techniques eliminates the need to remember a password or carry an identity.
- Depending on the context, in a biometric system, there are two different ways to resolve a person's identity.
  1) Verification
  2) Identification

Verification-Comparing a sample against a single stored template is called verification. Identification- Search a sample against a data base of templates

4. Types of Biometrics

There are two types of biometrics
1) Behaviour
2) Physical

Behavior Biometrics: Mostly Used for Verification
1) Speaker Recognition: Analyzing Vocal.
2) Signature: Analyzing signature dynamics.
3) Keystore: Measuring the time spacing of typed words.

Physical Biometrics: Used for either recognition or Verification
1) Fingerprint: Analyzing fingertip pattern.
2) Facial Recognition: Measuring facial characteristics.
3) Iris Scan: Analyzing feature of colored ring of the eye.
4) Retinal Scan: Analyzing Blood vessels in the eye.
5) DNA: Analyzing genetic makeup.

5. Biometric System and Devices

A biometric system is a combined hardware/software system for biometric identification or verification. Main functions of a biometric system are as follows:

- Receive biometric samples from an enroller or candidate

- Extract biometric feature from the sample.
- Compare the sample of the candidate with stored templates from individuals.
- Indicate identification or verification upon the result of the previous comparison.

6. Biometric Devices Have Three Primary Components

- One is an automated mechanism that scans and captures a digital or analog image of a living characteristic.
- The second handles comparison of the image with the stored data.
- The third interfaces with application systems.

These pieces may be configured to suit different situations. A common issue is where the stored images reside; on a card presented by the person being verified or at host computer. Recognition occurs when an individual's is matched with one of a group of stored images.

7. Fingerprint Recognition and Authentication

- The fingerprint technology is the oldest one among all biometric identification. It is based on the series of three dimensional lines, called ridges, and the space between then, called valleys. The ridges and valleys are unique to a person and therefore help to verify the identity.
- Fingerprint biometrics is largely regarded as an accurate biometric recognition method.
- Finger scan is an authentication terminal which verifies a person's identity from their finger image. When a user places their finger on the terminals scanner the image is electronically read, analyzed, and compared with a previously recorded image of the same finger which has been stored in the finger scan database.

8. Advantages

- Uniqueness ->Each individuals has a unique finger print. No two people have same finger print pattern.
- Universality->Finger print is universally available with every individual, some rare people do not have fingers.
- Permanence->finger print remain permanently user right from the development of seven months fetus until the person dies.
- Biometrics cannot be forgotten, lost, duplicated or stolen.
- It is more secure as it cannot be shared or used by others.
- No need to remember passwords or any PINs.

9. Disadvantages

- Biometric system must be able to accommodate changes to the biometric overtime which may be caused by ageing, illness or injury.
- Using the finger print scanner can lead to false rejection.
- Using finger print scanner can lead to false acceptance

10. Architecture of Proposed Model

The J2EE platform gives a multitiered distributed application model, the ability to reuse components, a unified security model, and flexible transaction control for a net banking architecture. The Figure 7 shows two multitiered J2EE applications divided into the tiers described in the following list. The J2EE application parts are presented in J2EE Components: - Client-tier components run on the clients machine. - Web-tier components run on the J2EE server. - Business-tier components run on the J2EE server for Net Banking process. - Enterprise information system (EIS)-tier software runs on the EIS server. For leveraging the security, our J2EE architecture include more modules integration for secured Net Banking process. The Java Authentication and Authorization Service (JAAS) can be used for authentication and authorization of users to ensure they have the access control rights (permissions). The J2EE application verifies the request using the JAAS authentication Modules and then initiates authentication by forwarding the request to the biometric authentication server and mobile OPT validity.

11. Conclusion

Net banking has become extremely popular among customers as a suitable method for money transaction. The proposed model has been developed for net banking system with biometric recognition and mobile process. A new technique to access the internet banking process is more secure than existing methods. Because fingerprint recognition method is unique method. If the machines are built with scanning accessories, the user can make the authentication by using user ID, password and finger print recognition. The transaction would be more secure method. In this model, unauthorized persons cannot surely hack or access the user accounts.

Fingerprint is a proven technology capable of high levels of accuracy. Strong fingerprint authentication solutions are capable of processing many users without allowing a miss match, and can verify nearly 100% of users with one or two placements of a finger. Because of this, many fingerprint technologies can be deployed in application where either security or convenience is the primary driver.

12. Future Scope

- Nowadays everyone is using Internet on mobiles. So we can develop an android App for scanning the fingerprint biometric.
- We can use our inbuilt mobile camera for capturing fingerprint image and build up algorithms for improving the image enhancement.

13. Applications

1) Can be used to make Online transaction for banking applications.
2) Can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks.

References

[1] R. Priya, V. Tamilselvi, G.P.Rameshkumar, "A Novel algorithm for Secure Internet Banking with finger print recognition", International Conference on Embedded Systems - (ICES 2014).

[2] Catalin LUPU, Vasile-Gheorghita GAITAN and Valeriu LUPU, "Security enhancement of internet banking applications by using multimodal biometrics", IEEE 13th International Symposium on Machine Intelligence and Informatics, January 2015.

[3] Verginia Espinosa, "Minutiae detection algorithm for fingerprint recognition", IEEE AESS Systems Magazine, 2002.

[4] Abinandhan Chandrasekaran and Dr.Bhavani Thuraisingham,"Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances",Second International Conference on Availability, Reliability and Security

[5] Hossein Jadidoleslamy, "DESIGNING A NOVEL APPROACH FOR FINGERPRINT BIOMETRIC DETECTION : BASED ON MINUTIAE EXTRACTION", International Journal on Bioinformatics & Biosciences (IJBB) Vol.2, No.4, December 2012.Image, Graphics and Signal Processing, 2012, 6, 29-35, Published Online July 2012 in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijigsp.2012.06.05.

[6] Bellamkonda sivaiah, Talasila Vamsidhar, Kotha Hari Chandana, "An Efficient Approach for Fingerprint Recognition by Matching Minutiae Pairings", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015, ISSN:2277 128X.

[7] Ankita Mehta, Sandeep Dhariwal, "Design & Implementation of Features based Fingerprint Image Matching System", International Journal of Multidisciplinary and Current Research, Accepted 15 Dec 2014, Available online 20 Dec 2014, Vol.2 (Nov/Dec 2014 issu

[8] Shashi Kumar D R, Kiran Kumar K, K B Raja, R. K Chhotaray, Sabyasachi Pattnaik, "Hybrid Fingerprint Matching using Block Filter and Strength Factors", 2010 Second International Conference on Computer Engineering and Applications.

[9] Om Preeti Chaurasia, "An Approach to Fingerprint Image PreProcessing", I.J.

[10] Aliaa A.A. Youssif, Morshed U. Chowdhury , Sid Ray and Howida Youssry Nafaa, "Fingerprint Recognition System Using Hybrid Matching Techniques", 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2012).