International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 4 49 - 51

Access Control Using 3 Level Authentications For E-Banking

Anuja Chandanshive
Department of Information Technology, Rajiv Gandhi Institute Of Technology, Mumbai, Maharashtra, India
anujachandanshive@gmail.com

Anuj Sureka,
Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai, Maharashtra, India
surekaanuj7@gmail.com

Jatin Gongiwala,
Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai, Maharashtra, India
jatinmg97@gmail.com

Akshay Nalawade,
Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai, Maharashtra, India
akiisr4@gmail.com

Abhay E. Patil
Department of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai, Maharashtra, India

***Abstract*:-**E-banking is used by a number of users in their day to day lives, still a lot of people refrain to use it considering its security threats. This study evaluates the potential of biometric authentication for online banking as a way of improving and making online banking more secure. Biometric verification is any means by which a person can be uniquely evaluated one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, iris, retina, voice waves, dna, signatures.These biometrics features can be used to make computer systems more secure for authentication purpose in computer based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The biometric identification overcomes all the above. The process that we are using includes face detection from the biometric domain

Keywords— *Face Recognition, Security and Protection, Hardware and Software Requirement's, Access controls.*

*****

1. INTRODUCTION

Nowadays with the network world, the way for crime is become easier than before. Because of this reason, network security has become one of the biggest concerns facing today's IT departments. We heard a lot about hackers and crackers ways to steal any password or pin code, crimes of ID cards or credit cards fraud or security breaches in any important building and then reach any information or important data from any organization or company. These problems allow us to know the need of strong technology to secure our important data and credentials.

This technology is based on a technique called "biometrics". Biometric is a form of bioinformatics that uses biological properties to identify people. Since biometric systems identify a person by biological characteristics, they are difficult to fake. Examples of biometrics are iris scanning, signature autentication, voice recognition and hand geometry.

2. GOALS AND OBJECTIVES

- The general objective of our project is to develop fully functional face recognition and verification system.

The specific objectives

- Understand the key aspects of these major technologies, namely those relating to the technological, application domain, social, environmental and performance aspects.
- Develop a fully operational face and fingerprint recognition application using an object oriented design approach with java.
- Examine the major biometric technologies of today including, iris, voice, signature, fingerprint, face and hand.
- Apply application interface standards to the application design and appreciate the need for standardization in application development.

3. STATEMENT AND SCOPE

- We propose a simple and effective approach for Biometric face & image enhancement and minutiae extraction based on the frequency and

orientation of the local ridges and thereby extracting correct minutiae points.

- The Face and Fingerprint Recognition System is designed to determine automatically whether two sets of fingerprint ridge detail come from the same finger.
- Face Recognition System is used to identify fingerprints of an individual and verify their identity.
- Face as one of many forms of special biometric characters is easy to identify individuals. The goal is to run the Fingerprint Recognition System automatically and correctly.
- The future plan is to improve the ability of this system to recognize low quality, this can used in many different fields as follows:

i. Identifying crime:
   - Private detectives
   - Keeping Federal records of criminals and suspected individual

ii. Security:
   - Secure area scanning
   - Laptop login
   - Digital information security

4. SOFTWARE REQUIREMENTS AND SCOPE (SRS):

4.1 Purpose and Scope of Document:

This document describes the functional, non-functional, software hardware requirements and the importance of a Face recognition system with briefly presenting its input and output functionalities.

4.2 Overview of responsibilities of Developer:

- Developer deals with the components of the product while describing the product perspective, functional and data requirements, input and output data, general constraints and assumptions of the application briefly.
   - It description about the functional and nonfunctional requirements of the application.

4.3 Usage scenario:

There are plenty of usage scenarios involved which given as follows:

- User login
- Image capture and tracking
- Verification
- Matching
- Authentication
- OTP Verification
- Database storage
- Logout

.

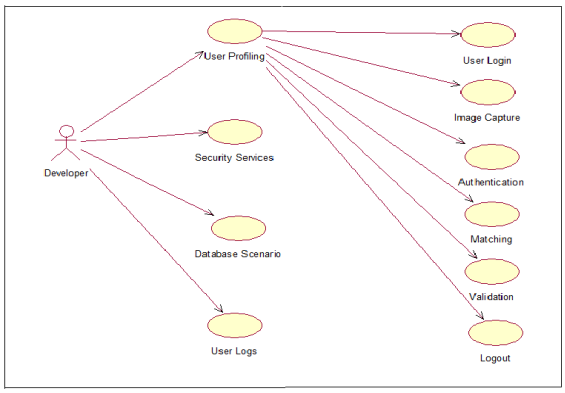
4.4 Use cases:

- Use case modeling identifies and describes the system functions by using a tool called use cases.
- Use cases describe the system functions from the perspective of external users and in a manner and terminology they understand.
- To accurately and thoroughly accomplish this demands a high level of user involvement and a subject matter expert who is knowledgeable about the business process or event.

Use Case for User:

- Login
- Capture photo
- Verification
- Matching
- Authentication
- OTP Verification
- Display information (transaction)

Logout



5. METHODOLOGY

The methodology of developing this system took a number of stages:

1. User faces camera
2. Biometric reader
3. Feature Extractor
4. Algorithms for processing
5. Matcher
6. Database
7. Decision Maker

The steps involved in face recognition:

1) Capture: A physical sample is captured by the system during enrollment and also in identification or Verification process.

2) Extraction: unique data is extracted from the sample and a template is created.

3) Comparison: the template is then compared with a new sample.

4) Match/Non match:-the system decides if the features extracted from the new

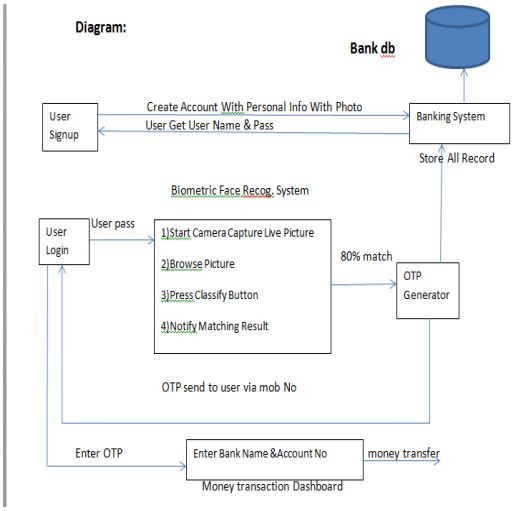


Fig2. Block Diagram

CONCLUSIONS

The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of a person. These physical characteristics of a person include the features like fingerprints, face, hand geometry, voice, and iris biometric features. These biometrics features can be used to make computer systems more secure for authentication purpose in computer based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The biometric identification overcomes all the above. Additional security barriers can be provided using those characteristic of a person which are unique in nature.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on ‘Access Control Using Three Level Authentication’.

We would like to take this opportunity to thank my internal guide Mr. Abhay E. Patil for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

REFERENCES

[1] "Facial Recognition Applications". Animetrics. Retrieved 2008-06-04.
[2] "Airport Facial Recognition Passenger Flow Management". hrsid.com.
[3] [Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
[4] Smith, Kelly. "Face Recognition" (PDF). Retrieved 2008-06-04.
[5] R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", IEEE Trans. on PAMI, 1993, (15)10:1042-1052
[6] Williams, Mark. "Better Face-Recognition Software". Retrieved 2008-06-02.
[7] Crawford, Mark. "Facial recognition progress report". SPIE Newsroom. Retrieved 2011-10-06.