International Innovative Research Journal of Engineering and Technology
ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

Multifactor Authentication to Enhance Security in Banking System

Shivam Kumar[1], Dr. Agilandeeswari L[2], Muralibabu K[3]
[1]MCA Student, [2]Assoictae Professor, [3]Vice Principal, School of Information Technology and Engineering, VIT University. [3]Podhigai College of Engineering and Technology, Thirupattur.
[1]kshivam213@gmail.com, [2]agila.l@vit.ac.in, [3]mail2muarli05@yahoo.co.in

Abstract

In modern era, online technologies are growing so fast. Every companies use networking to replace their works in online, which in contrary the chances of stealing data also increases. To secure the data of most important industry which is backbone of any country like bank, defence where data is the main asset we need highly secure interface which protect system unauthorized access. Bank is the important industry of any country so the data of each customer need to be protected from intruders. Intruders can steal data of either any particular customer and steal all money of that customer, or they can steal the employee username and password and instead of that employee intruder access the system which is very formidable for bank. Mostly bank uses username and password to authenticate their employee to enter into system. But it is not significant as many incidents have shown that these authentications are easily broken by intruder. This paper proposes the multifactor authentication using face recognitions and biometrics to enhance security in banking systems. The experimental result on multiple databases shows the increased accuracy

Keywords - **Intruders, Face recognitions, biometrics.**

I. Introduction

Online technologies give industries the facility of anywhere anytime connectivity as the work can done from anywhere across the globe and also any time. Now the industries like bank can connect to the customer in all times [1]. Although online technologies like transaction, balance transfer, balance withdrawal provides customer to do anywhere in their computer or mobile but same time if it is not secure then intruders can enter into network of bank and steal all money of customer. An unsecure system is like calling inviting intruder to access and steal important data. The data of bank may be password of customers, customers personal details if these data steal by intruders then it affect bank by losing trust of customer as they fear to take risk in depositing money and assets in bank. The aim of intrusion is to gain and alter confidential data or to steal money from bank. Intruders can done their evil purpose either by targeting particular customer by accessing username and password or entire bank. To target entire bank the employee may take crucial part for intruders, as if they have employee authentication details they can access system instead of them. There are many encryption algorithm which secure customer details but not many efficient algorithm to protect intruders from accessing employee details. Employee can be biggest threat for any institution as employee are accessing the system, if intruders knows the details of employee then they can access system and steal confidential details or alter details. There are various ways using intruders can hacks employee details like official email id, password, employee can sell confidential details to competitor bank for money. Intruder can also hacks details by employee social media profiles, if employee post videos, images regarding their profession [2]. So there must be a secure interface or application that restricts unauthorized entry into bank system. In this paper we propose an application where along with username and password it also recognizes face with biometrics. If employee is valid then only it allowed entering into application.

II. Literature survey

In this paper [3] they indicate to improve the authentication of person in mobile environment using multiple authentications by adding combination of face recognition and speech. They uses specially designed database called MOBIO to use to test the accuracy of their work. The average of facial biometrics achieved EER of 33.4 %. According to this paper the multiple modals biometrics system reduces error rate of 21.0 % which shows usefulness of their project called face and speech information.

In this paper [4] they proposed a biometrics based

authentication systems where they use combination of face and fingerprint authentication. They proposes a method called Gabor filter bank along with 2 scales and 8 orientations, which is used to extract directional features from source data. Their framework enables them to use only 39 features for input to classifier stage of system. There system achieved 99.25 % recognition accuracy.

In this paper [5] they proposed a schema to decrease the retraction rate of an ATM by using face recognition methods. Their method use ATM's inbuilt camera. Their project differ from ordinary face authentication and recognition by short time frame of ATM usage and severe motion artefacts. The evaluate there project under real challenging condition of real ATM usage. By using multiple databases their experiment result shows the promising for mitigating card/cash forgetting issue and improving ATM user experience. In this paper [6] they revels the problems like fraudulent website, fake emails, capturing id and password, stealing money of customers, fake calls from bank asking user id and password etc from bank and financial institutions. They proposed a solution using novel algorithm using biometric In this paper [7] they revels the problem of fake currency all around the world. Fake currency are harder to track also because they rapidly adopt the new technology and come of with the highly advanced technology. They come with a core software system to build a advanced robust automated fake currency detection tool for their Bangladeshi bank notes. Their software detects fake currency by extracting some features of Bangladeshi notes like optically variable ink (OVI), micro printing, water-mark, etc.

In this paper [8] they emphasize the importance of one time password (OTP) because most of the transaction done now a day's using OTP. They come up with enhanced OTP system model using ECC with finger print biometrics. They also suggest more security with decrease the key strength. Their focuses on create and share secret key without transmitting any private key so that no one could access the secret key except valid user.

In this paper [9] they found a novel method to extract optimal discriminant features from FKP images. They use ID-Log Gabor filter, the Gabor filter bank and Linear Discriminant Analysis (LDA) in their method.

III. Existing method for Employee Authentication

In existing method the user should first enter user ID and password which will verified in bank database. If user ID and password matches the employee can enter into bank system. Else it will not allow and says Invalid User. If valid employee can use system and access customer details and perform certain task like deposit customer balance, update account etc. Fig 1 shows the existing module.

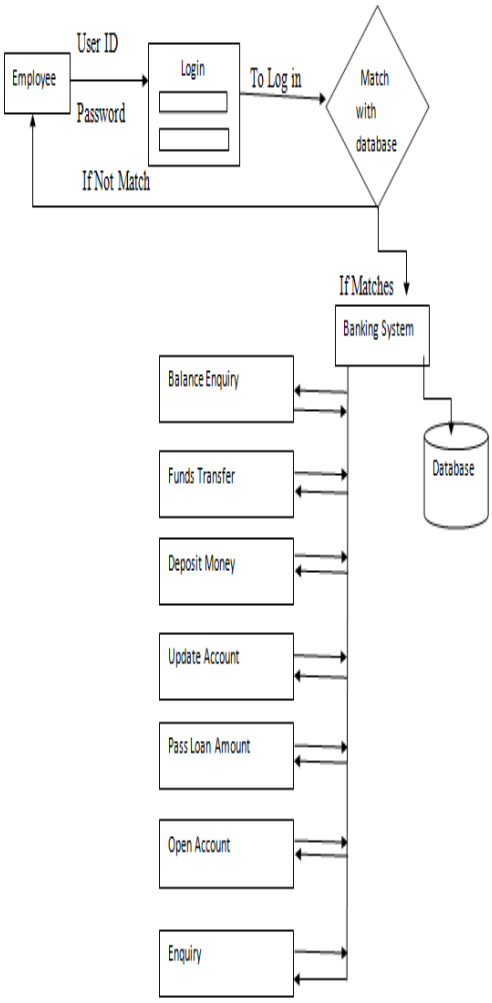

Fig 1. Existing System Architecture

IV. Existing system for Finger print recognitions

In this paper [10] their proposed methodology is when employees want to enter into system they have to identify himself using print sensor, print sensor is attached using Arm Processor. The Arm processor access the finger print sensor using certain commands. The operations done by finger print sensors is Adding the new members, matching the members, checking valid and invalid members. The user have to put thumb on print sensors, matching is done using database; if match found then access is granted, otherwise not.

International Innovative Research Journal of Engineering and Technology
ISSN NO: 2456-1983

V. Proposed System

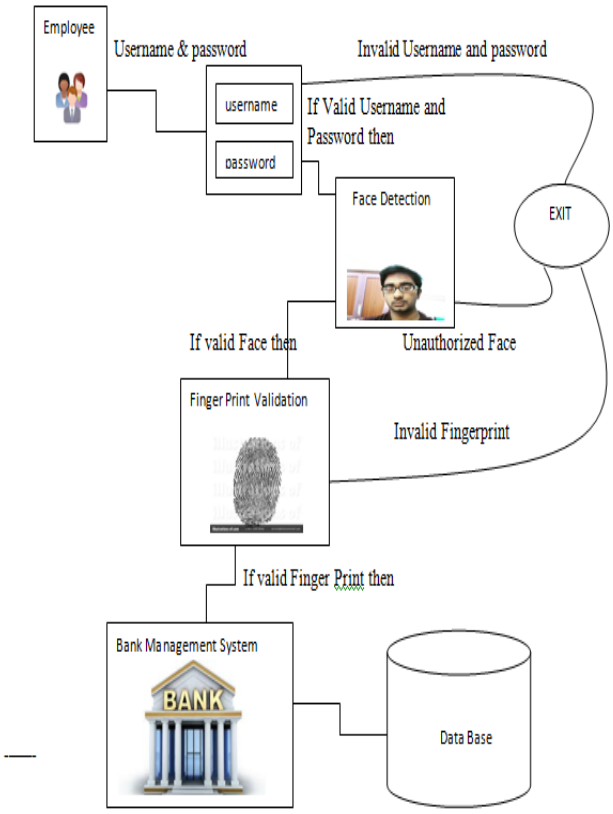

Fig 2. Proposed System Architecture.

In existing system, if hacker knows employee id and password of employee they can easily enter into system so there must be an efficient and secure entry page to restrict unauthorized entry. In this project I proposed an efficient and secured interface for banking system to restrict unauthorized entry. There are three steps for login process first one is employee have to give their user name and password if valid then they can enter into second step for face recognition they have to show their face into camera and software matches their face with database if it found then they can enter into third step for finger print matching if it matches then only they can enter into system. This is also called multifactor authentication system. In this project there is no chance for intruders to enter into system as they can't hack face or finger print.

VI. Methodology

For new Employees, they have to create new account. For creating new account they have to go through three steps first step is they have to give their details like username, password, name, email Id, country and state. All these details stored in bank database. Second step is they have to register their face in database using web cam, the image of their face are register in database. Third step is to register their finger print in database.

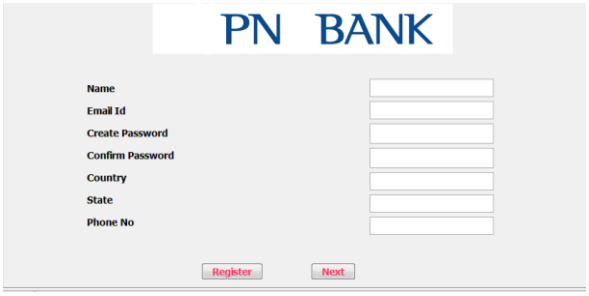

Fig 3. Creating new account

Fig 4. Registering new Employees Face

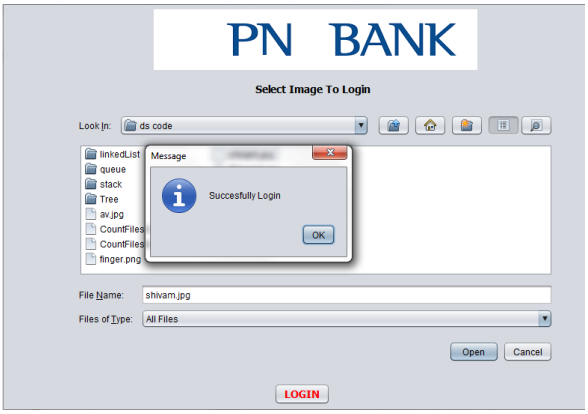

Fig 4. Login Using Face recognition

Second methodology is login, After successfully creating the new account the user can access the system by three step login process. First step user have to give their unique username and password if it matched with database then second step is to match their face with registered image in database , if it match then the third step is to match their finger print if their finger print matches then only they can enter into system.

Third methodology is the entire bank system which is connected with database, a system where employees can perform various operations like creating new account, updating balance, performing transaction, granting loan, transferring funds, taxes etc. This system is connected with database, each and every account details are stored in

database, if any transaction occurs it directly updated into databases. Every transaction are performed using OTP (one time password) so that there is no chance of compromises in transaction. All the methodologies are implemented using java 8, along with OpenCv 2.4 jar file which contains all libraries needed for implementation. The database is used in implementation is Oracle 11 g. The IDE used to run the code is net beans

.VII. Algorithms used in System

Algorithms for signup

1. set database with necessary fields
2. create procedure for storing details in database
3. procedure signup()
   {
   Extract details from interface and stored into variable
   Initialize oracle driver
   Using Driver Manager get connection
   Using connection variable create prepare statement
   Execute that statement
   }
4. It will store employee details into database

TABLE 1
Algorithm for login

1. import all necessary package
2. Extracts username and password from login interface
3. procedure login()
   {
   String name := username
   String pass := password
   Extract details from interface and stored into variable
   Initialize oracle driver
   Using Driver Manager get connection
   Using connection variable create prepare statement
   Prepare statement to select all username and password from database
   Execute query
   Match name and pass from all database
   If matches then valid authentication
   }
4. if match then it goes to next phase for face detection.
5. close connection

TABLE 2
Algorithms for storing face in database

```
1. Install openCv jar file in library of your projrct
2. Import all package in your project
3. Create a thread which run every time when you run
project
4. procedure DaemonThread()
    {
     webSource.retrive(frame1);
     Highgui.imencode(".bmp",frame,mem);
     Image                    im=ImageIO.read(new
ByteArrayInputStream(mem.toArray()));
     BufferedImage buff=(BufferedImage) im;
     Graphics g=jPanel1.getGraphics();
     }
5. procedure takeSnapshot()
    {
    int returnval=jFileChooser1.showSaveDialog(this);
    if(returnval==JFileChooser.APPROVE_OPTION)
    {
    File file=jFileChooser1.getSelectedFile();
    Highgui.imwrite(file.getPath(),frame);
    }
    else
    System.out.println("Fie access cancelled by user");
    }
6. Now when you click take snapshot it will take snap and
store in database.
```

TABLE 3
Algorithm for face recognition

```
1. set Boolean status:= false
2. create instance of File and store the selected file
   Of jFileChooser
3. now store the path of directory which is databases of images
4. now store all image files in array of files using listFiles()
5. for int i:=0 to length of directory
   Now call check method which check whether image are present in directory or not
   Check (file 1, str)
6. procedure check (String file, String str)
      Set Boolean status:=false
      Create instance of Image for both file and str and name them img1 and img2
      Grab both image img1 and img2 using PixelGrabber
      Now store width and height using getWidth and getHeight method of both
      Now store both width and height in array data1 and data2 respectively.
      If both data 1 and data2 match then return true
7. If check return true then login and turn interface to next step for fingerprint
```

VIII. Comparison of existing model and proposed model

Existing model uses single authentication system for authentication of employee where employee give username and password in login field if username and password is valid then employee directly access banking system**.** It also use SMS system in every transaction which secure it further. But in proposed system we use multifactor authentication along with username and password employee face and finger print also matches if it matches then only employee can enter into system otherwise it says “invalid user reported”. Existing system easily hacked since it using single authentication only username and password. In proposed system we are using multifactor authentication it is more secured and cannot hacked. Security level of existing system is “not secured” while proposed system is “ fully secured”.

IX. Conclusion

Our proposed model has been developed for banking system to authenticate their employee with multifactor authentication. We use novel technique to protect system from unauthorized access. Since combination of face detection and finger print validation is unique it gives us highly secure interface to protect system. In this method unauthorized access surely not possible.

References

[1] Mohd Khairul Affendy Ahmad, Rayvieana Vera Rosalium, Lean Yu Beng. "Security Issues on Banking Systems", ISSN:0975-9646.

[2] https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[3] Linlin Shen, Nengheng Zheng, Songhao Zheng, Wei Li "Secure Mobile Services by Face and Speech Based Personal Authentication"

[4] Amit Deshmukh, Sheetal pawar, Dr Mrs. Madhuri Joshi, "Feature Level Fushion of face and fingerprint Modalities using Gabor Filter Bank"

[5] Ekberjan Derman, Y.Koray Gecici, Albert Ali Salah, "Short Term Face Recognition for Automatic Teller Machine Users”.

[6] R.Priya, V.TamilSelvi, G.P. RameshKumar, "A novel algorithm for secure Internet Banking with finger print recognition'.

[7] Zahid Ahmed, Sabina Yashmin, Md Nahidul Islam, Raihan Uddin Ahmed "Image processing based Feature Extraction of bangladeshi Banknotes".

[8] Dindayal Mahto, Dilip kumar yadav, "Enhancing Security of One-Time Password Using Elliptic curve Cryptography with Finger-print Biometric".

[9] Mourad chaa, Naceur-Eddine Boukezzoula, Abdallah Meraoumia, Maarouf korichi "An efficient Biometric based personal authentication System using finger Knucke prints Features"

[10] Shaikh J.A 1 ShubhangiA.Mali2," Advanced Authentication and Security System for Call Centre Employee's with Live GPS Tracking".