International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1628-1633 www.ijaem.net ISSN: 2395-5252

Hybrid Password authentication Using Bio-Metric Verification for Smart Atm

[1]Divya K, [2]Boopathi S, [3]Jagadeeshwaran S, [4]Sathiyamoorthi M,

[1]Assistant Professor, Department of Computer Science and Engineering, Paavai College of Engineering
[2,3,4]Undergraduate student, Department of Computer Science and Engineering, Pavai College of Technology

Submitted: 05-06-2022 Revised: 17-06-2022 Accepted: 20-06-2022

ABSTRACT: The importance of security in the authentication process as well as the increase in threat level posed by such malware has attracted many researchers to the field. Many attacks are successful in accessing social network accounts since the current password-based authentication paradigms are not efficient and robust enough as well as vulnerable to automated attacks. The simplest alternative is complementing the single factor (password-based) authentication process with additional identification elements, such as one-time PIN codes, generated by the user's own device (e.g. the smartphone) or received via SMS. In this project, a novel method using three layer based authentication is proposed to address the problem of shoulder-surfing attacks on authentication schemes. First layer based on biometric based authentication system, which provides new solutions to address the issues of security and privacy. So implement real time authentication system using face biometrics for authorized the person for ATM system. Second layer provide OTP verification with reverse processing. Then implement PIN-based authentication method that operates on ATM Application. Hybrid keypad uses the technique to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter the PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad. The three layer authentication process enabled when user login into the application and also when a transaction is done.

KEYWORDS: Authentication Process, PIN-Based Authentication, ATM Application, Online Networking, Network Protocols.

I. INTRODUCTION

Networking is the exchange of information and ideas among people with a common profession or special interest, usually in an informal social setting. Networking often begins with a single point of common ground. Networking is used by professionals to expand their circles of acquaintances, to find out about job opportunities in their fields, and to increase their awareness of news and trends in their fields or in the greater world. The interconnections between nodes are formed from broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies. The nodes of a computer network may include personal computers, servers, networking hardware, or other specialized or general-purpose hosts. They are identified by hostnames and network addresses. Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol.

Computer networks may be classified by many criteria, for example, the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanism, and organizational intent. A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

[1]. Computer networks support many applications and services, such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and

instant messaging applications. Most modern computer networks use protocols based on packet-mode transmission. A network packet is a formatted unit of data carried by a packet-switched network.

[2]. The physical link technologies of packet network typically limit the size of packets to a certain maximum transmission unit (MTU). A longer message is fragmented before it is transferred and once the packets arrive, they are reassembled to construct the original message. Packets consist of two types of data: control information and user data (payload). The control information provides data the network needs to deliver the user data, for example, source and destination network addresses, error detection codes, and sequencing information.

[3]. Control information is found in packet headers and trailers, with payload data in between. With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from other users, and so the cost can be shared, with relatively little interference, provided the link isn't overused. Often the route a packet needs to take through a network is not immediately available. In that case, the packet is queued and waits until a link is free.

[4]. Small business owners network to develop relationships with people and companies they may do business with in the future. These connections help them establish rapport and trust among people in their own communities. Successful business networking involves regularly following up with contacts to exchange valuable information that may not be readily available outside the network. Business owners and entrepreneurs often join their local chamber of commerce in an effort to promote their business interests and to help others in their community do the same. There are many additional benefits to joining a chamber of commerce, such as receiving deals and discounts from other chamber members, having one's business listed in the chamber directory, and the ability to influence policies related to the area's business and economic activity.

[5]. The number of block chain systems is steadily increasing, however the electronic voting domain is very slow to adapt to changes in technology with a relatively low number of systems devised so far, which introduce a fresh look on the electronic voting scene, based on our observation of the state of the Electronic voting has been a topic of active debate, with significant number of people believing that electronic voting cannot be trusted enough to be used for significant elections due to uncertainty in the authenticity and integrity of the machines, and the votes that have been cast using them.

A communication protocol is a set of rules for exchanging information over a network. In a protocol stack (also see the OSI model), the protocol is divided up into layers, where each protocol layer leverages the services of the protocol layer below it until the lowest layer controls the hardware that sends information across the media.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

Present programs also undergo from other skills security vulnerabilities. One outstanding difficulty is safety towards offline guessing attack (often referred to as offline dictionary assault). The reason of offline guessing attack is to compromise a customer’s password through exhaustive search of all possible password values. In a password-established atmosphere, passwords are viewed to be brief and human memorisable, and the corresponding password house is so small that an adversary is in a position to enumerate all possible values within the area within some cheap period of time. For example, most of the ATM deployments use PINs (personal identification numbers) of simplest 4 to 6 digits long, so the password space has no a couple of million possible values. Hence, an additional security requirement for wisecard-established password authentication is security towards offline guessing attack.

In particular, compromising a patron’s sensible-card must not allow an adversary to launch offline guessing attack in opposition to the patron’s password. In observe the adversary may just steal the wise-card and extract the entire information stored in it through reverse engineering. This concept is paying homage to password-founded authentication protocols.

PROPOSED SYSTEM

The proposed scheme is implementing on a combination of the concept of multilevel password security and the multi user access in ATM application. Multi users can share the same account with individual face image verification process. The user has to type the account number and password for first level verification, if failing to login they have to enter it again. Users only need to capture their face image using web camera. The ATM server matches the face image with the one stored on the database (the template). Along with normal OTP system, an additional face image verification to ensure tight security. If every entered detail is correct then user continues with face verification process then PIN is verified using illusion. If registered user is verified the face then an OTP (one time password) is being sent to the customer's phone. Now the customer has to enter this OTP, if the entered reverse OTP is correct he/she can just proceed with the transaction. A hybrid keyboard method is implementing to address the problem of shoulder-surfing attacks on authentication schemes.

This is a PIN-based authentication method that operates on touch screen devices. Hybrid keypad uses the technique to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter the PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad.

Based on this analysis, it seems practically almost impossible for a surveillance camera to capture the PIN of a smartphone user when hybrid keypad is in use. This method is implemented in a banking application. The hybrid keypad will be enabled when the PIN is entered while login into the application.

III. SYSTEM SPECIFICATION

HARDWARE REQUIREMENTS

Processor	: Intel core processor 2.6.0 GHZ
RAM	: 1GB
Hard disk	: 160 GB
Compact Disk	: 650 Mb
Keyboard	: Standard keyboard
Monitor	: 15 inch color monitor

SOFTWARE REQUIREMENTS

Operating system	: Windows OS
Front End	: C#.NET
Back End	: SQL SERVER
IDE	: VISUAL STUDIO

FEASIBILITY STUDY

The feasibility Analysis is an analytical program through project manager determines the project success ratio and through feasibility study project manager able to see either project.

TECHNICAL FEASIBILITY

Software Technologies used are Python and MySQL. In the educational institutions, it is possible to update the system in future. No special hardware is required for the purpose of using this system. Hence it is declared that this project is technically feasible. Hence this project is economically feasible there is no need to involve any cost for this project.

OPERATIONAL FEASIBILITY

In training phase, easy to train the animal datasets and provide alert system in real time environments. Hence it is easy to operate with training. Therefore it is operationally feasible for implementation

IV. SOFTWARE DESCRIPTION

FRONT END: PYTHON

The .NET Framework (pronounced dot net) is a software framework developed by Microsoft that runs primarily on Microsoft Windows. It includes a large library and provides language interoperability (each language can use code written in other languages) across several programming languages. Programs written for the .NET Framework execute in a software environment (as contrasted to hardware environment), known as the Common Language Runtime (CLR), an application virtual machine that provides services such as security, memory management, and exception handling. The class library and the CLR together constitute the .NET Framework.

The .NET Framework's Base Class Library provides user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. Programmers produce software by combining their own source code with the .NET Framework and other libraries. The .NET Framework is intended to be used by most new applications created for the Windows platform. Microsoft also produces an integrated development environment largely for .NET software called Visual Studio

The purpose of the Common Language Infrastructure (CLI) is to provide a languageneutral platform for application development and execution, including functions for Exception handling, Garbage Collection, security, and interoperability. By implementing the core aspects of the .NET Framework within the scope of the CL, this functionality will not be tied to a single language but will be available across the many languages supported by the framework. Microsoft's implementation of the CLI is called the Common Language Runtime, or CLR.

The CIL code is housed in CLI assemblies. As mandated by the specification, assemblies are stored in the Portable Executable (PE) format, common on the Windows platform for all DLL and EXE files. The assembly consists of one or more files, one of which must contain the manifest, which has the metadata for the assembly. The complete name of an assembly (not to be confused with the filename on disk) contains its simple text name, version number, culture, and public key token. Assemblies are considered equivalent if they share the same complete name, excluding the revision of the version number.

A private key can also be used by the creator of the assembly for strong naming. The public key token identifies which public key an assembly is signed with. Only the creator of the keypair (typically the .NET developer signing the assembly) can sign assemblies that have the same strong name as a previous version assembly, since he is in possession of the private key. Strong naming is required to add assemblies to the Global Assembly Cache

The Framework Class Library (FCL) is a superset of the BCL classes and refers to the entire class library that ships with .NET Framework. It includes an expanded set of libraries, including Windows Forms, ADO.NET, ASP.NET, Language Integrated Query, Windows Presentation Foundation, Windows Communication Foundation among others. The FCL is much larger in scope than standard libraries for languages like C++, and comparable in scope to the standard libraries of Java.

V. SYSTEM DESIGN

SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system. In this architecture, user can set the pin, face and phone number. At the time of verification, user type the PIN and view as Illusion format. Then verify the face using Grassmann algorithm. Finally provide the OTP in reverse format. After successful verification, user can access the applications.

USER CREDENTIALS

Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID. This process is simple and easy to implement.

PASSWORD AUTHENTICATION

Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered are easy to guess. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. In this module we can implement authentication phase. After registration, user enters into the system using login setting. At first, face image capture and recognize the face.

FACE IMAGE VERIFICATION

After registration, user can set password using face capture process. At first, camera is enabling in system for capture the face. Face identification is a one-to-many matching process that compares a query face image against all the template images in a face database to determine the identity of the query face. The identification of the test image is done by locating the image in the database that has the highest similarity with the test image. Here feature vector is made from important values of the image from each filter Energy, mean and standard deviation forming a 40 value feature vector for every image. The input facial features are matching with database using grassman learning algorithm

REVERSE OTP VERIFICATION

A One Time Password is a string of characters or numbers automatically generated to be used for one single login attempt. One Time Passwords can be sent to the user's phone via SMS is used to protect web-based services, private credentials and data. OTP's will minimize the risk of fraudulent login attempts and come in all shapes and sizes, but always add an extra layer of authentication. The risk of fraud is drastically reduced if the user doesn't only have to fill in his user name and password but also needs OTP have to complete the login**.**

HYBRID PIN WITH SHUFFLING

The User PIN Authentication page enables user to add user PIN records into the device one at a time. If the details entered matches with the details available, the user will be allowed to process further transaction. If no match found, the user have to re enter the details again. PINs are used in secure banking transactions. Hiding Password is process on hiding numeric digits into digital patterns. While entering the PIN, the keypad will be changed to a hybrid keypad. The hybrid keypad is a combination of two keypads. Shuffling Patterns is used for hiding the PINs from unauthorized access. The user entered pin will get hide on keyboard and that may be shuffled after every authentication process.

ATM APPLICATION

Users are allowed to access ATM application, when they are completing PIN verification. Admin has permission to view user details and user transaction details. The user should select the receiver name and the account number. Then, the amount to be transferred should be entered. The normal keypad will change to hybrid keypad while entering transaction password. The transaction details will be reflected in the corresponding accounts.

SOURCE CODE FOR PYTHON:

```
Using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Data.SqlClient;

namespace IllusionPin {     public partial class
BankHome : Form    {

     SqlConnection      con      =      new
SqlConnection(@"Data
Source=.\SQLEXPRESS;AttachDbFilename=
IllusionPin\IllusionPin\illusiontb.mdf;Integrated
Security=True;User         Instance=True");
SqlCommand cmd;


     public   BankHome()              {
InitializeComponent();      }

     private void BankHome_Load(object sender,
EventArgs e)      {

     }

      private    void    textBox4_KeyDown(object
sender, KeyEventArgs e)        {        if
(e.KeyCode < Keys.D0 || e.KeyCode > Keys.D9)
{             if (e.KeyCode < Keys.NumPad0 ||
e.KeyCode > Keys.NumPad9)               {
if (e.KeyCode != Keys.Back)             {
//nonnumberenter = true;            string abc
=     "Please     enter     numbers     only.";
textBox5.Text = "";

             DialogResult      result1      =
MessageBox.Show(abc.ToString(),      "Validate
numbers", MessageBoxButtons.OK);            }
}          }          if (Control.ModifierKeys ==
Keys.Shift)       {          //nonnumberenter =
true;          string abc = "Please enter numbers
only.";                  DialogResult result1 =
MessageBox.Show(abc.ToString(),      "Validate
numbers", MessageBoxButtons.OK);

          }       }

     private void textBox6_Enter(object sender,
EventArgs e)       {          string pattern = null;
pattern    =    "^([0-9a-zA-Z]([-\\.\\w]*[0-9a-zA-
Z])*@([0-9a-zA-Z][-\\w]*[0-9a-zAZ]\\.)+[a-zA-
Z]{2,9})$";

          if
(System.Text.RegularExpressions.Regex.IsMatch(t
extBox5.Text, pattern))          {
   //MessageBox.Show("Valid Email address ");
}          else          {          textBox4.Text =
"";

             MessageBox.Show("Not a vali3d Email
address ");          }       }

     private                              void
dateTimePicker1_ValueChanged(object     sender,
EventArgs  e)          {          int age =
DateTime.Today.Year                         -
dateTimePicker1.Value.Year;

          textBox3.Text = age.ToString();


          if  (age  <  18)                  {
//MessageBox.Show("Age Limit Low!");         }

     }

     private   void   button1_Click(object   sender,
EventArgs e)      {

          string   gender;                      if
(radioButton1.Checked == true)
  {    gender = radioButton1.Text;
  }
```

VI. CONCLUSION

The main goal and importance of the ATM system using face image is to provide security. ATM system using fingerprint is secure, but it still has some demerits. To overcome the challenges of the technology it can be combined with more secure features. In this project we are using biometric security measure in the ATM system. The proposed system explains a hybrid keypad is implemented in an ATM application. The main goal of our work was to design a PIN-based authentication scheme that would be resistant against shoulder surfing attacks. To this end, we created Illusion PIN. The proposed system has quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance. This means that even if a person perceives the digits on a hybrid keypad to be equally visible to the digits on a digital keypad, the distortion in the hybrid keypad is bigger and the visibility index has a lower value. This is something logical, because when the reference buttons are all same color, a digit that is even slightly visible is considered a big distortion.

FUTURE ENHANCEMEN

Future work of this project is to propose an android based application for banking process also implement high secure measurements using Digital PIN based authentication or Bright Pass based authentication. Also have plan to improve more security to the system with low computation time and also this have been develop in android application for mobile based social network access.

SOME OF THE ADVANAGES FROM THE ABOVE RESULTS

a) Computational cost and processing time are low.
b) Text passwords combined with face biometric enhance the security of user access in ATM application.
c) Face biometric provides complete security of the proposed method.
d) Overcome the guessing attacks and dictionary attacks.
e) No need to implement additional sensors.
f) SMS alert to know about transactions details up to date.

REFERENCES

[1]. Wazid, Mohammad. "Secure three-factor user authentication scheme for renewable-energybased smart grid environment." IEEE Transactions on Industrial Informatics 13, no. 6 (2017): 3144-3153.

[2]. Chatterjee, Santanu, "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment." IEEE Transactions on Dependable and Secure Computing 15, no. 5 (2016): 824-839.

[3]. Gope, Prosanta. "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions." IEEE Transactions on Information Forensics and Security 13, no. 11 (2018): 2831-2843.

[4]. Han, Lidong, Qi Xie, Wenhao Liu, and Shengbao Wang. "A new efficient chaotic maps based three factor user authentication and key agreement scheme." Wireless Personal Communications 95, no. 3 (2017): 3391-3406.

[5]. Chen, Chien-Ming. "Comments on “An improved secure and efficient password and chaosbased two-party key agreement protocol”." Nonlinear Dynamics 87, no. 3 (2017): 2073-2075.

[6]. Jiang, Qi, et al. "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks." Ieee Access 5 (2017): 3376-3392.

[7]. Amin, Ruhul, et al. "Cryptanalysis and improvement of an RSA based remote user authentication scheme using smart card." Wireless Personal Communications 96.3 (2017): 4629-4659.

[8]. Das, Ashok Kumar, et al. "An efficient multi- gateway- based three- factor user authentication and key agreement scheme in hierarchical wireless sensor networks." Security and Communication Networks 9.13 (2016): 2070-2092.

[9]. Jiang, Qi, et al. "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles." IEEE Transactions on Vehicular Technology 69.9 (2020): 9390-9401.