BI-LEVEL AUTHENTICATION FOR ATM USING IOT

[1]K.Arputha Ajitha Rose., [2]A.Nishiya Kanimozhi. [3]C.Pavin. [4]K.Prithiga

[1] Assistant Professor, [2] UG scholar[3] UG scholar[4] UG scholar
Department of Computer Science & Engineering, Rathinam Technical campus,coimbatore

ABSTRACT

Numerous researchers have been attracted to the field due to the significance of security in the authentication process and the growing threat posed by such malware. The current password-based authentication paradigms are insufficiently efficient and robust, as well as susceptible to automated attacks, resulting in the success of numerous attempts to access social network accounts. The simplest alternative is to supplement 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. a smartphone) or SMS. This project proposes a novel method employing hybrid keyboards to combat shoulder-surfing attacks on authentication schemes. This is an ATM application that uses a PIN-based authentication method. The hybrid keypad combines two keypads with different digit orderings in such a way that the user entering the PIN sees one keypad while an attacker viewing the device from a greater distance sees only the other. Since an attacker may memorize the spatial arrangement of the pressed digits, the user's keypad is shuffled for every authentication attempt. Based on the analysis, it appears nearly impossible for a surveillance camera to capture a user's PIN when a hybrid keypad is in use. In a banking application, this method is implemented. The hybrid keypad will be activated when the PIN is entered during application login and when a transaction is performed. Then, provide the Reverse OTP for transactions to be completed. The experimental results demonstrate that the proposed system provides a higher rate of accuracy.

I.INTRODUCTION

The intrusion prevention is a combination of different security technologies. Its purpose is to anticipate and prevent attacks. IDSs of recent vintage apply intrusion prevention. Instead of analyzing traffic logs, which reveals attacks after they have occurred, intrusion prevention attempts to warn against such attacks. While intrusion detection systems attempt to provide an alert, intrusion prevention systems block potentially hazardous traffic. Over many years, the philosophy of network intrusion detection has been to detect as many attacks and potential intrusions as possible and report them so that others can take the necessary precautions. In contrast, network intrusion prevention systems have been developed in accordance with the new philosophy of "taking the necessary measures to counter attacks or detectable intrusions with precision." In general, the IPS is always online on the network to monitor traffic and actively intervene by limiting or deleting hostile traffic by interrupting suspicious sessions or taking other measures in response to an attack or intrusion. The IPS functions similarly to the IDS; additionally, it analyses connection contexts, automates log analysis, and suspends suspicious connections. Contrary to conventional IDS, signatures are not used to detect attacks. Before taking action, The IDS must make a timely decision regarding the action to be taken. If the action conforms to the rules, execution permission will be granted and the action will be carried out. If the action is illegal, however, an alarm will sound. In most instances, the other network detectors will be notified in order to prevent other computers from opening or executing particular files. In contrast to other prevention methods, the IPS is a relatively new method. It is based on the principle of integrating disparate technologies, such as firebreak, VPN, IDS, anti-virus, and anti-Spam. Although the detection portion of an IDS is the most complex, the goal of an IDS is to increase network security, so the prevention portion of an IDS must achieve this objective. After identifying malicious or unwanted traffic, prevention techniques can stop it. All traffic must pass through an IDS sensor in an inline configuration. When unwanted traffic is identified, the IDS does not forward it to the remainder of the network. However, for this effort to be effective, all traffic must pass through the sensor.

II.EXISTING SYSTEM

Existing applications suffer from additional skill-based security vulnerabilities. A significant difficulty is offline guessing attack security (often referred to as offline dictionary assault). The objective of an offline guessing attack is to compromise a user's password by exhaustively searching for all possible passwords. In a password-based environment, passwords are considered short and human-memorable, and the corresponding password space is so small that an adversary can enumerate all possible values in the area in a reasonable amount of time. For instance, the majority of ATM deployments utilise PINs (personal identification numbers) between 4 and 6 digits in length, so the password space contains fewer than two million possible values. An additional security requirement for wise-card-based password authentication is therefore protection against offline guessing attacks. Specifically, compromising a customer's smart card should not allow an adversary to launch an offline guessing attack against the customer's password. In plain view, the adversary may simply steal the smart card and use reverse engineering to extract all the information stored on it. This idea pays tribute to password-based authentication protocols.

Drawbacks of Existing System

- Passwords are viewed by other persons during verification.
- Passwords are easily tracked by dictionary based attacks.
- PIN and OTP are not providing valid authentication.

III.PROPOSED SYSTEM

To counter shoulder-surfing attacks against authentication schemes, a hybrid keyboard method is being implemented. This is a PIN-based authentication system for touch-screen devices. The hybrid keypad combines two keypads with different digit orderings in such a way that the user entering the PIN sees one keypad while an attacker viewing the device from a greater distance sees only the other. Since an attacker may memorise the spatial arrangement of the pressed digits, the user's keypad is shuffled for every authentication attempt. To evaluate the security of illusion PINs, we created an algorithm based on human visual perception that estimates the minimum distance from which an observer cannot interpret the user's keypad. It appears practically impossible for a surveillance camera to capture the PIN of a smartphone user using a hybrid keypad, according to our analysis. In a banking application, this method is implemented. The hybrid keypad will be activated when the PIN is entered during application login. Then, using the Reverse OTP system to grant access to the ATM application

IV.SYSTEM DESCRIPTION

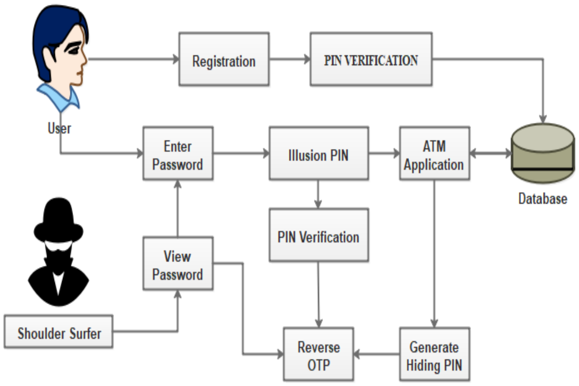


Figure.4.1 Block Diagram

Figure 4.1 explains that users can register information such as their name, age, and gender. This password authentication system allows users to select their own passwords while encouraging the use of stronger passwords. After registering, users enter the system using their login credentials. Shuffling Patterns is used to prevent unauthorized access to PINs.

The user's entered PIN will be concealed on the keyboard and may be rearranged after each authentication procedure. The risk of fraud is drastically reduced if, in addition to his username and password, the user must also enter an OTP to complete the login.

V.MODULES

A.USER CREDENTIALS

In this module, the User can register personal information such as name, age, and gender. This information is stored in a database. Username and password are required to complete the user authentication process. The majority of applications provide knowledge-based authentication, which includes both alphanumeric and graphical passwords. Bio-metric password systems have been proposed as a possible alternative to text-based passwords in order to combat various security flaws, primarily because humans can remember images better than text.

B PASSWORD AUTHENTICATION

Authentication is the process of determining if a user should be granted access to a system or resource. The user has difficulty remembering strong passwords, and those that can be remembered are easy to crack. A password authentication system should incentivize the use of robust, less predictable passwords while maintaining security and memorability.

This password authentication system allows users to select their own passwords while encouraging the use of stronger passwords. After registering, users enter the system using their login credentials.

C. HYBRID PIN WITH SHUFFLING

The User PIN Authentication page allows users to add individual user PIN records to the device. If the entered information matches the available information, the user will be permitted to proceed with the transaction.

Hiding Password is a method for concealing numeric digits within digital patterns. During PIN entry, the keypad will transform into a hybrid keypad. The hybrid keypad combines two separate keypads. Shuffling Patterns is used to prevent unauthorized access to PINs. The user's entered PIN will be concealed on the keyboard and may be rearranged after each authentication procedure.

D. REVERSE OTP VERIFICATION

A One Time Password is a string of randomly generated characters or numbers that can only be used for a single login attempt. Protecting web-based services, private credentials, and data with One-Time Passwords sent to the user's phone via SMS. OTPs reduce the risk of fraudulent login attempts, come in a variety of forms, and always add an additional layer of authentication.

The risk of fraud is drastically reduced if, in addition to his username and password, the user must also enter an OTP to complete the login. The user must enter their OTP in reverse order in this field. This will be more efficient than the current OTP-based authentication system.

E. *ATM APPLICATION*

Users are permitted to access the ATM application once PIN verification is complete. Admin has access to user information and transaction details. The user must enter the recipient's name and account number. The amount to be transferred should then be inputted. The corresponding accounts will reflect the transaction details. After using the logout option to end a session, the keypad will be shuffled.

VI. OUTPUT

The primary objective and significance of the ATM face recognition system is security. The fingerprint-based ATM system is secure, but it has some drawbacks. To overcome the obstacles presented by the technology, it can be combined with more secure characteristics. In this project, biometric security measures are implemented in the ATM system. The proposed system describes the implementation of a hybrid keypad in an ATM application. Our primary objective was to develop a PIN-based authentication scheme that is resistant to shoulder surfing attacks. To achieve this, we developed Illusion PIN. By introducing the concept of safety distance, the proposed system quantifies the level of resistance to shoulder-surfing. Even if a person perceives the digits on a hybrid keypad to be as visible as the digits on a digital keypad, the distortion in the hybrid keypad is greater and the visibility index is lower. When the reference buttons are all the same colour, a digit that is even slightly visible is regarded as a significant distortion.

A.USER CREDENTIALS

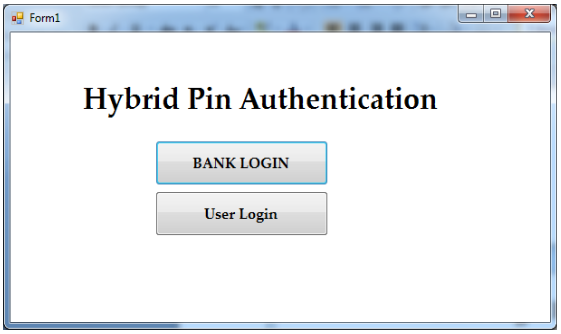
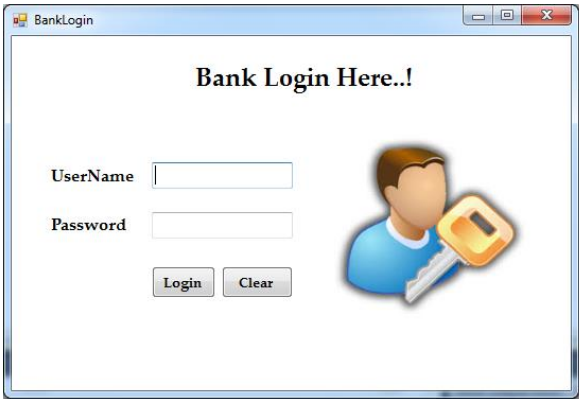
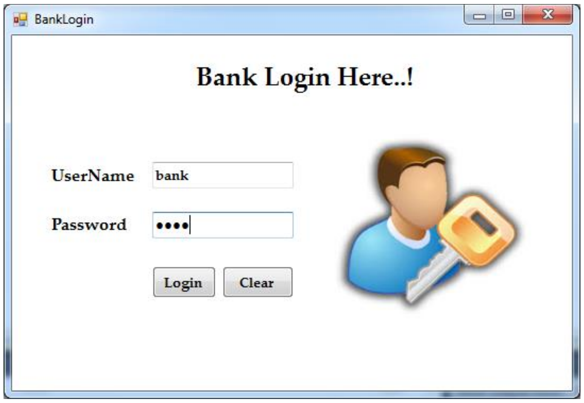


Figure6.1 Login form

User can register their details such as name, age, gender and so on. These details are stored in database.

B PASSWORD AUTHENTICATION

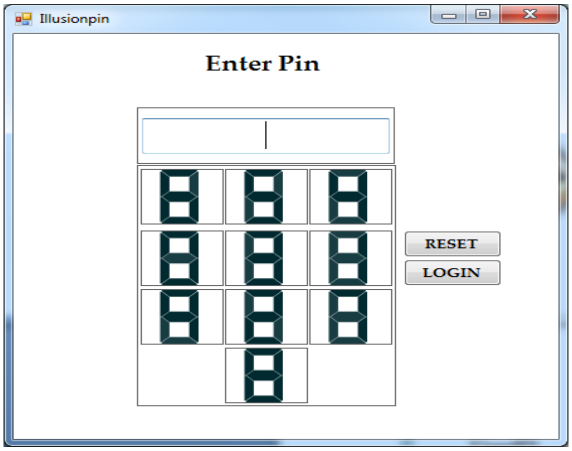




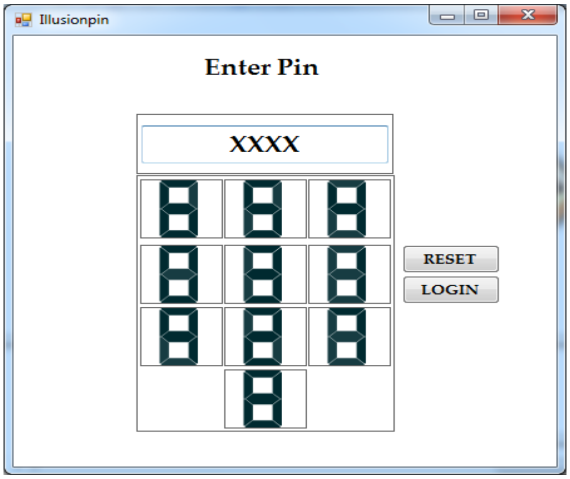
Bank Login Here..!

UserName: bank

Password: ••••

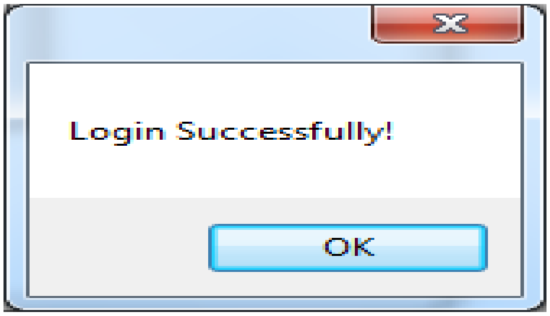


Enter Pin



Enter Pin

XXXX

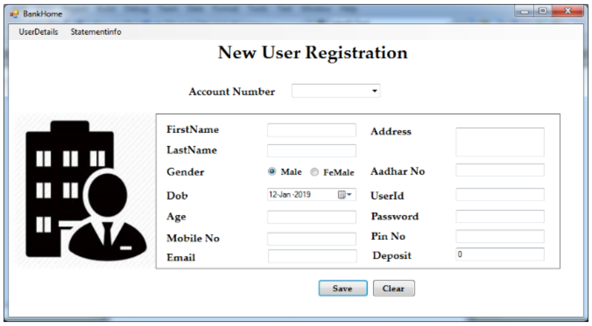


Login Successfully!

Fig 6.2 verification process

SQL Server Query Analyzer gives a graphical presentation of the execution arrangement of a question and a programmed segment that recommends which list ought to be utilized for a chose inquiry

C. HYBRID PIN WITH SHUFFLING



New User Registration

Account Number

FirstName

LastName

Gender ● Male ○ FeMale

Dob 12-Jan-2019

Age

Mobile No

Email

Address

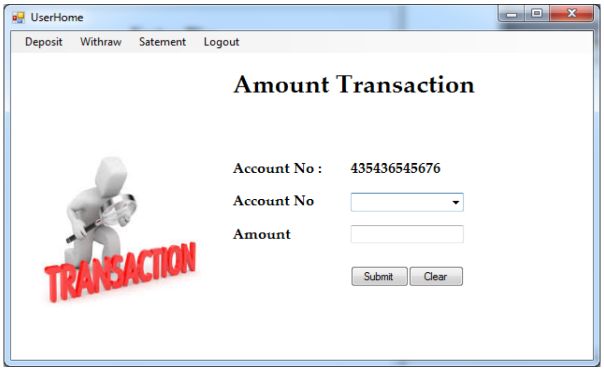
Aadhar No

UserId

Password

Pin No

Deposit 0

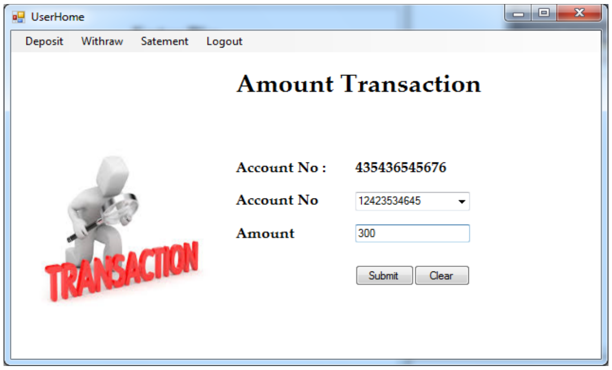


Amount Transaction

Account No : 435436545676

Account No

Amount



Amount Transaction

Account No : 435436545676

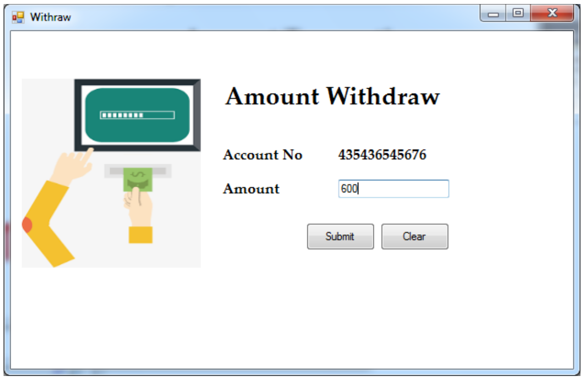
Account No 12423534645

Amount 300

Fig 6.3 Transaction using dual pin verification

After verification in a strong manner the amount will be transferred. It provides more security than regular authentication. The unknown person intrusion will be prevented

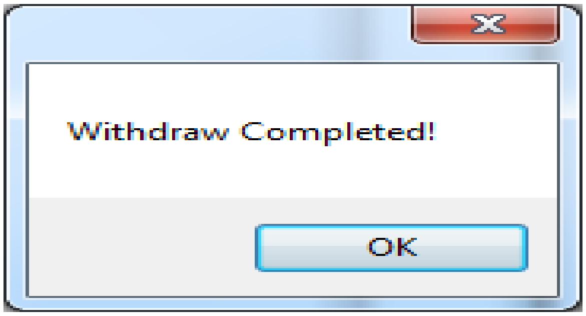
D . REVERSE OTP VERIFICATION



Amount Withdraw

Account No 435436545676

Amount 600

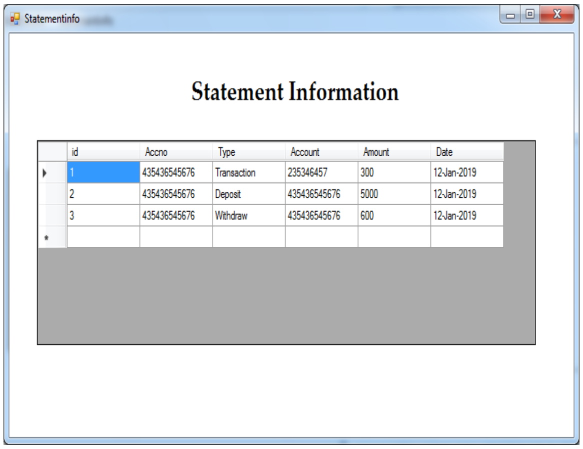


Withdraw Completed!

Fig 6.3 OTP is verified

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

E. *ATM APPLICATION*



Statement Information

id	Accno	Type	Account	Amount	Date
1	435436545676	Transaction	235346457	300	12-Jan-2019
2	435436545676	Deposit	435436545676	5000	12-Jan-2019
3	435436545676	Withdraw	435436545676	600	12-Jan-2019

Fig 6.5 Bank statement is provided

Admin has permission to view user details and user transaction details. The user should select the receiver name and the account number.Then only bank statement provided

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.

REFERENCES

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

[2] Chatterjee, Santanu, Sandip Roy, Ashok Kumar Das, Samiran Chattopadhyay, Neeraj Kumar, and Athanasios V. Vasilakos. "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, Jemin Lee, and Tony QS Quek. "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, Weicheng Fang, King-Hang Wang, and Tsu-Yang Wu. "Comments on “An improved secure and efficient password and chaos-based 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] Zhang, Hao, et al. "FDN: Feature decoupling network for head pose estimation." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34. No. 07. 2020.