



# AN EFFECTIVE CARDLESS ATM TRANSACTION USING COMPUTER VISION TECHNIQUES

<sup>1</sup>P.Vengatesan, <sup>2</sup>I.Mayil Vaganan, <sup>3</sup>K.Rajasekar, <sup>4</sup>D.Chinnadurai, <sup>5</sup>S.Sakthi

<sup>1</sup>Assistant Professor, <sup>2,3,4,5</sup>Student

<sup>1</sup>Computer Science and Engineering,

<sup>1</sup>Sri Ramakrishna College Of Engineering, Perambalur, Tamil Nadu, India

**Abstract :** The providers of ATM banking services must be more responsive towards security requirements. Now days with the network world, the way for cybercrime is become easier for hacking purpose. Because of this reason, network security has become one of the biggest facing today's IT departments securities. While there is no doubt that ATM banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings. And heard a lot about hackers and crackers ways to steal any logical password or pin code number character, crimes of ID cards or credit cards fraud or security breaches. In existing framework, Identification can be equated to a username and is used to authorize access to a system. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he or she claims to be – the authentication process. Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. The Face Recognition is the study of physical or behavioural characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. So, implement real time authentication system using face biometrics for authorized the person for online banking system.

**IndexTerms** -Cardless Transaction,Hybrid pin,Face recognition

## INTRODUCTION

Managing security means understanding the risks and deciding how much risk is acceptable. Different levels of security are appropriate for different organizations. No network is 100 percent secure, so don't aim for that level of protection. If you try to stay up-to-date on every new threat and every virus, you'll soon be a quivering ball of anxiety and stress. Look for the major vulnerabilities that you can address with your existing resources.

Here present numerous advantages of computer networks and the Internet. Connecting your network to the Internet provides access to an enormous amount of information and allows you to share information on an incredible scale. However, the communal nature of the Internet, which creates so many benefits, also offers malicious users easy access to numerous targets. The Internet is only as secure as the networks it connects, so we all have a responsibility to ensure the safety of our networks

## TYPES OF SECURITY MEASUREMENTS

### 2.1 AUTHENTICATION

Authentication is used by a server when the server needs to know exactly who is accessing their information or site. Authentication is used by a client when the client needs to know that the server is system it claims to be. In authentication, the user or computer has to prove its identity to the server or client. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints. Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.

### 2.2 AUTHORIZATION

Anomaly detection involves identifying unusual patterns or events in a dataset that deviate from the norm. Machine learning algorithms can be used for tasks such as fraud detection and intrusion detection. For example, machine learning algorithms can be used to detect credit card fraud or identify network intrusions.

## 2.3 ENCRYPTION

Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key. The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. The SSL drives the secure part of “https://” sites used in e-commerce sites (like E-Bay and Amazon.com.)

## 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 memorizable, 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.

They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. While QR codes have many advantages that QR code is an image of a matrix barcode that stores data in two dimensions. Hence, an additional security requirement for wise-card-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.

## 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. Card-less ATM security can implement using QR code technology. A QR code method is implementing to address the problem of shoulder-surfing attacks on authentication schemes. Here propose a system for efficient authentication of automatic teller machine (ATM) by QR code system.

Quick Response (QR) codes are two dimensional barcodes that can be used to efficiently store small amount of data. They are increasingly used in all life fields, especially with the wide spread of smart phones which are used as QR code scanners. While QR codes have many advantages that QR code is an image of a matrix barcode that stores data in two dimensions. Data is presented as square dots with specific pattern in both horizontal and vertical dimensions. Specific imaging devices (QR scanners) can read this image and retrieve the stored data based on the pattern of square dots.

The user has shown the QR code and to type the PIN for first level verification, if failing to login they have to enter it again. A hybrid keyboard method is implementing to address the problem of shoulder-surfing attacks on authentication schemes. 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.

## IV. MODULE DESCRIPTION

### 4.1 User Credentials

In this module, User can register their details such as name, age, gender and so on. These details are stored in database. In user authentication the process which we have to pass through is username and password. Most of the application provides knowledge-based authentication which include alphanumeric password as well as graphical password.

### 4.2 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. "PasswordAuthentication" typically refers to a setting in SSH (Secure Shell) configurations. When set to "yes," it allows users to authenticate using a password when connecting via SSH.

### 4.3 FACE IMAGE RECOGNITION

After registration, user can set password using face capture process. At first, camera is enabling in system for capture the face. Face can be detected in captured image using iterative closest point algorithm. The main contribution of our approach is the use of dimensional information which is lost by projection in the two dimensional photos. The intuitive way for face recognition is to utilize HAAR Cascade classification process. Many solutions are developed for this task especially for range image registration.

### 4.4 PIN VERIFICATION

In this module implement classification algorithm to predict the diabetic and heart diseases. And using machine learning algorithm such as Support vector machine algorithm to predict the diseases. A MLP is a feed forward vector model that maps sets of input data onto a set of appropriate outputs. It consists of multiple vectors of nodes in a directed graph, and each layer is fully connected to the next one. In the MLP algorithm, we plot each data item as a point in n-dimensional space (where n is a number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiates the two classes very well. MLPs are simply the coordinates of individual observation. The MLP classifier is a frontier that best segregates the two classes (hyper-plane/ line). User can provide the features and automatically predict the diseases.

#### 4.5 ATM APPLICATION

Users are allowed to access ATM application, when they are completing QR code 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 transaction details will be reflected in the corresponding accounts. After closing the session using logout option, the keypad will get shuffled. If you're storing user account information, transactions, and other data, use a database like MySQL, PostgreSQL, or MongoDB. Design a schema to store user accounts, including fields such as account number, PIN, balance, transaction history, etc.

#### CONCLUSION:

The main goal and importance of the ATM system using face image is to provide security. ATM system using pin 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 QR code with biometric security measure in the ATM system. The proposed system explains Card-less ATM 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 QR code with Face biometrics. The proposed system has quantified the level of resistance against shoulder-surfing by introducing the notion of safety distance.

Furthermore, computer vision techniques enable seamless and intuitive user experiences, allowing customers to initiate transactions simply by presenting their faces to the ATM's camera. This streamlined process enhances convenience, particularly for individuals who may have difficulty remembering PINs or handling physical cards.

#### REFERENCES

- [1] Aljuaid, Shumukh M., and Arshiya S. Ansari. "Automated Teller Machine Authentication Using Biometric." *Comput. Syst. Sci. Eng.* 41, no. 3 (2022)
- [2] P. Arun Kumar, N. Sathya Priya. "Enhanced Security in Cardless ATM Transactions using Biometric Authentication" Coimbatore, India, 2019.
- [3] N. S. Aswathi, G. Lakshmi, N. P. Hima. "Cardless ATM System: An Automated Transaction Using QR Code and Image Processing" Coimbatore, India, 2020.
- [4] Ayo, C. K., C. M. Mac-Eze, A. A. Adebisi, A. Oni, J. O. Okesola, and I. Odun-Ayo. "Developing a Multi-Factor Authentication-Based Cardless Electronic Payment System." In *IOP Conference Series: Earth and Environmental Science*, vol. 665, no. 1, p. 012009. IOP Publishing, 2021.
- [5] Brinthavathi, S., and Mr P. Anbumani. "ATM Transaction Using Retinal and Face Recognition." *Journal homepage: www.ijrpr.com* ISSN 2582: 7421.
- [6] A. S. Dhara, A. S. Bhaisare, V. R. Biradar. "A Secure ATM Transaction using QR Code and OTP" Pune, India, 2019.
- [7] Marietta, J., B. Chandra Mohan, and V. Hari Haran. "Prototype for Card-less Electronic Automated Teller Machine using Internet of Things."
- [8] Phothikitti, Kittti. "Factors influencing intentions to use cardless automatic teller machine (ATM)." (2020).
- [9] Princess, Ms M. Ramya, and R. Umamaheswari. "An Advanced ATM Machine Proposal: Contactless Cash Dispenser and Depositor."
- [10] Priyadarshini, B., T. Kanagalakshmi Nithyasree, and J. Sherin. "Ai Based Card-Less Atm Using Facial Recognition."
- [11] K. A. M. L. Ranga Senarathne, Roshan Fernando, Indika Perera. "Secure Cardless ATM Transactions using QR Code" Moratuwa, Sri Lanka, 2020.
- [12] Samuel O. Onyango, Stephen O. Ondieki, Caroline W. Koech. "Development of a Cardless ATM System with Biometric Security Features Using a Web Application" Novi Sad, Serbia, 2020.
- [13] S. S. Shirur, V. G. Dharaskar. "Smartphone-based Cardless ATM Transaction System using QR Code and OTP" Noida, India, 2020.
- [14] Sonam Shakya, Nischal Pandey, Prashant Pandey, et al. "Secure Cardless ATM Withdrawal System Using Mobile Application" Erode, India, 2019.
- [15] L. Soundarya, M. Sowmiya, S. Udhaya Shree. "Secure ATM Transaction using Cardless Authentication and OTP Verification" Pondicherry, India, 2019.
- [16] Teshome, Abebaw, and Temtim Assefa. "Designing E-Banking Cardless Transaction Services Framework for Banking Sectors in Ethiopia." (2021).
- [17] Tobias-Mamina, Rejoice, and Eugene Tafadzwa Maziriri. "Modelling to use Card-Less Banking Services: An Integration of TAM and TPB." *International Journal of Business and Management Studies* 12,
- [18] M. Vijayakumar, M. Rajasekar, N. Sathish. "Cardless ATM Transaction System using Facial Recognition and QR Code" Tirunelveli, India, 2018.
- [19] Vinayakumar R., S. Saravanakumar, M. Senthilkumar. "Cardless ATM Transaction System Using QR Code" Volume 3, Issue 4, July-August 2018.
- [20] Yadav, Khushboo, Suhani Mattas, Lipika Saini, and Poonam Jindal. "Secure card-less atm transactions." In *2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA)*, pp. 1-4. IEEE, 2020.