



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

# Cardless ATM Using Face Detection and OTP

Alpesh Dhoke, Hasarat Kazi, Kunal Pandhare, Jay Ranpura, Sankalp Sakat, Prof. Shubhangi bhagat

Department of Computer Engineering, Bhivrabai Sawant College of Engineering & Research, Narhe, Pune, Maharashtra, India

**ABSTRACT:** Automated Teller Machine (ATM) transactions are found safe, reliable and inevitable these days for fulfilling our financial commitments. Traditional approach for using ATM mandates involvement of Debit card. But however, people do experience times when their account lacks balance amount or they forget to carry card and struggle to complete transaction. We know that, parallel to ATM usage, mobile phones' usage has also been an inevitable trend. Establishing a connection between these e-gadgets has ignited a simple and effective approach to withdraw cash without the involvement of debit card which can be referred to as card less cash withdrawal. Face detection and OTP is used for authentication of user. This along with Face detection comprises two levels of security. When Face and OTP are matched then customer's account will open in ATM machine.

**KEYWORDS:** ATM, OTP, Face detection CNN algorithm

## I.INTRODUCTION

Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Facial recognition is a category of biometric security. Other forms of biometric software include voice recognition, fingerprint recognition, and eye retina or iris recognition. The technology is mostly used for security and law enforcement, though there is increasing interest in other areas of use.

Many people are familiar with face recognition technology through the FaceID used to unlock iPhones (however, this is only one application of face recognition). Typically, facial recognition does not rely on a massive database of photos to determine an individual's identity — it simply identifies and recognizes one person as the sole owner of the device, while limiting access to others. Beyond unlocking phones, facial recognition works by matching the faces of people walking past special cameras, to images of people on a watch list. The watch lists can contain pictures of anyone, including people who are not suspected of any wrongdoing, and the images can come from anywhere — even from our social media accounts.

The technology is used for a variety of purposes. These include:

Unlocking phones, Law enforcement, Airports and border control, Reducing retail crime, Improving retail experiences, Banking Marketing and advertising, Healthcare

### Objective:

Crime prediction is of great significance to the formulation of policing strategies and the implementation of crime prevention and control. Machine learning is the current mainstream prediction method. However, few studies have systematically compared different machine learning methods for crime prediction. This paper takes the historical data of public property crime from 2021 to 2022 from a section of a large coastal city in the southeast of China as research data to assess the predictive power between several machine learning algorithms. Results based on the historical crime data alone suggest that the GEO FENCING model outperformed CNN, random forest, support vector machine, naïve Bayes, and Convolutional neural networks. In addition, the built environment data of points of interests (POIs) and urban road network density are input into GEO FENCING model as covariates. It is found that the model with built environment covariates has better prediction effect compared with the original model that is based on historical crime data alone. Therefore, future crime prediction should take advantage of both historical crime data and covariates associated with criminological theories. Not all machine learning algorithms are equally effective in crime prediction. To detect face from Camera footage and remove all unwanted background using pre-processing To recognized face of criminal by comparing uploaded photo (from Camera) with database

## II.LITERATURE SURVEY

In recent years, cash withdrawal through ATM cards has seen an increase in the number of card related frauds; card cloning, shoulder surfing, fake keyboard, skimming etc. being a few of them. To combat these problems, KhushbooYadav et al [1] proposed a Secure Cardless Transaction System- a method which would eliminate the usage of ATM PIN and physical cards altogether and hence provide a secure environment for cash withdrawal. The concept of User-Generated One Time Password (OTP) has been introduced in this project. With all these modification in existing systems, the robustness of the machines will increase.

Md. Al Imran et al [2] analyzed their protocol and found some flaws on this. This protocol doesn't specify what if it is off us transaction. Besides, customers get different categories of services but this protocol cannot determine which customer will get which category of services. That is why, inspired by this protocol we have proposed a modified model for getting same transaction facilities as exists which uses BPIN that will determine the bank identity (B) and a random Personal Identification Number (PIN) and One Time Password for authentication of the customer instead of biometric fingerprint because of major disadvantage of biometric authentication. And obviously it will use no card for accomplishing the transaction.

"OTP Based Cardless Transaction using ATM" [3] proposed a secure, robust and flexible biometric authentication system which combines two methods that use a Biometric and a proximity sensor. To increase the security level in ATM transaction this proposal integrates a biometric fingerprint technique along with a shuffling keypad method. Here the card is replaced with the fingerprint, which is registered during the opening of a bank account and PIN number is entered in a shuffling keypad. To avoid the shoulder-surfing attacks with or without concealed cameras in PIN entry, this approach uses a shuffling keypad which uses a proximity sensor to shuffle the keypad during the PIN entry. The system is tested with multiple users and has obtained 100% accuracy. This system avoids the misuse of electronic cards and supports a secure transaction.

An automated teller machine (ATM) is an electronic telecommunications device that helps customers of banking departments in transactions and transfer of money in their accounts. The customer enters their unique personal identification number (PIN), i.e. stored in the chip of the card. Due to an increase in the installation of ATM and the number of ATM cardholders, the number of cases of fraudulence has also increased radically. The advancement in technology has resulted in an increase in various skimming activities. So, developments are incorporated in the existing systems to make it more secure, convenient and reliable. The employed secured system must have high speed and must be durable. The design presented in [4] is unique because of biometric scanners such as Iris scanner and the two-way check with fingerprint scanner makes it more reliable. The iris scanner being the primary security check lets the system access the further steps for transaction. Fingerprint scanner embedded in the ATM card acts as the secondary security check for the system. The transaction procedure is successful only if the input data by the card holder matches with the database. It consumes less energy that makes it suitable for use. The suggested modified system is pragmatic moreover economical when correlating to the alternative existing classification and affirmation processes of ATMs.

Nowadays iris recognition is getting more popular in terms of security. Iris pattern is more stable with ages, uniqueness and acceptability. Because of its high reliability and good rates of recognition, iris recognition is therefore used for highly secure locations. With the arrival of ATM banking has become much easier and it has also become more accessible. The product (ATM) it is manifold due to the highly increasing risk of intelligent criminals. Due to which the banking services are in danger and not secure. This situation is getting progressed as huge progress is made in biometric recognition techniques like fingerprint and iris scanning. Customers password can be encrypted using selective article points. Therefore, a system is needed which is more secure and provides safe transactions and also help from various frauds. System described in [5] is more secure and fast and helps to provide better facilities.

The objective of [6] is to consider smart phone in Near-Field Communication (NFC) Card Emulation mode as an alternative to ATM cards. In NFC the distance between the respective devices needs to be very small (typically less than 4 cm) which makes NFC ideal for making payments and for other transactions involving sensitive/private data. In the proposed system, in order to authenticate at the ATM kiosk, the user needs to swipe his/her smart phone in front of the NFC reader. An ATM card is not required for authentication and the system will still have a stronger security compared to the system in which ATM card was used. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

Paper [7] aims to prevent the crime related to ATM card frauds and secure transaction. In this paper, two options are included like One Time Password (OTP) and Fingerprint detection for a successful transaction. The user can use any of the two options mentioned above for ATM transactions. We know that the OTP is valid for only one transaction and a specific duration. Thus, the Global System for Mobile (GSM) is used for the generation of OTP and that OTP is sent to the mobile number to which the bank account is linked. In case, if the user does not have the mobile to which the bank account is linked or else the mobile is switched off or network problem the second option of fingerprint authentication can be used. The fingerprint of the user must be linked with the bank account so that the unique pattern of the fingerprint can be used to make a successful transaction. Hence this project will increase security and add privacy by making use of biomedical authentication that is fingerprint pattern detection. Therefore this added feature helps to reduce the crimes related to ATM cards.

The proliferation of ATM Fraud case in Indonesia is still the main concern for the society especially bank customers. In March 2017, a total loss of 5 billion rupiah was recorded as a result of ATM Frauds. While the only solution which ensures security of ATM machines is a 6-digit PIN, there are still a lot of security cracks that can be used by the criminals to steal customer data and the 6-digit PIN itself. One of the most frequent method of ATM Fraud is skimming. Therefore, the authors bring the concept of Fingershield ATM, ATM Machine that implements biometric identification in the form of fingerprints which is integrated with smart card and database server. Fingerprint technology is powerful identification because of its unique characteristics of each of the minutiae. Despite the fact that customers have to add additional authentication time around 1.5 seconds for fingerprint verification, the security is much improved and guaranteed. Research “Fingershield ATM – ATM Security System using Fingerprint Authentication” [8] used experimental descriptive method. With this method, hopefully ATM Fraud can be minimized so that the customers can feel more secure while using ATM Machines. Based on implementation and test results which had been done before, Fingershield ATM functions run well and some security parameters have passed the test, as well as almost all specifications are met.

In [9], a PIN is generated by the user and this PIN is made available to the ATM system by the means of a Subscriber Identity Module (SIM) in the user's Mobile Phone. This information is communicated to a Global System for Mobile Communications (GSM) module embedded into the ATM's functional framework. This method of security is more stable than the traditional methods presently in use. The method presented is dynamic due to the possibility of changing the User Defined PIN (UDPIN) in each and every transaction. Losing the access card no longer becomes a big problem to the user and the need for immediate deactivation is also eliminated. It can also be enhanced by including other security features without large number of modifications. A simple prototype employing this security function has been implemented and the results are verified. The proposed system has been tested extensively and proves to be a simpler and better security measure.

There is a tremendous increase in the ATM fraud incidents in recent years. Card fraud reports stated that \$16.31 billion are the losses from payment card frauds in 2014, and expected to reach \$35.54 billion in 2020. There is a real demand to find robust security methods, devices, and technologies to safeguard ATM transactions. Paper [10] proposed two steps model to complete ATM transactions using a closed end-to-end fraud prevention system. By adding a smartphone as an additional layer for ATM transactions and using legitimate user smartphone ID number to robust ATM secure transactions using the available technologies.

#### Gap Analysis:

Traditional approach for using ATM mandates involvement of Debit card. But however, people do experience times when their account lacks balance amount or they forget to carry card and struggle to complete transaction. We know that, parallel to ATM usage, mobile phones' usage has also been an inevitable trend. Establishing a connection between these e-gadgets has ignited a simple and effective approach to withdraw cash without the involvement of debit card which can be referred to as card less cash withdrawal.

### III. PROPOSED SYSTEM

#### Existing System Architecture

The mobile app consists of a special code which flashes on the screen for a period of 1 minute. This code provides strong authentication by dynamically generating a one-time security code. This code can be generated even if there is no network or internet connection.

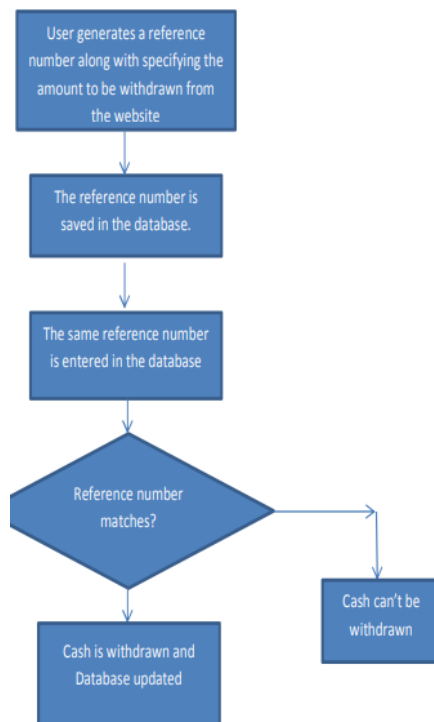


Figure .1Existing System

Here the user will first login to the mobile app using the details such as user-id and password. After this the user generates a reference number as per his choice and also specifies the amount to be withdrawn. This reference number would remain valid for a certain period of time and can be used only once. Having generated the reference number, the user visits the nearest ATM and enters the user-id and password along with the code in the app to sign in. If the authorized user is present, he/she would be logged in and would be required to enter the reference number to withdraw the specified amount. If the reference number is correct, the amount is withdrawn else transaction fails. This idea is an amalgamation of current ATM system and online transactions involving OTP. By eliminating the use of OTP the problems related to sharing of OTP are successfully overcome.

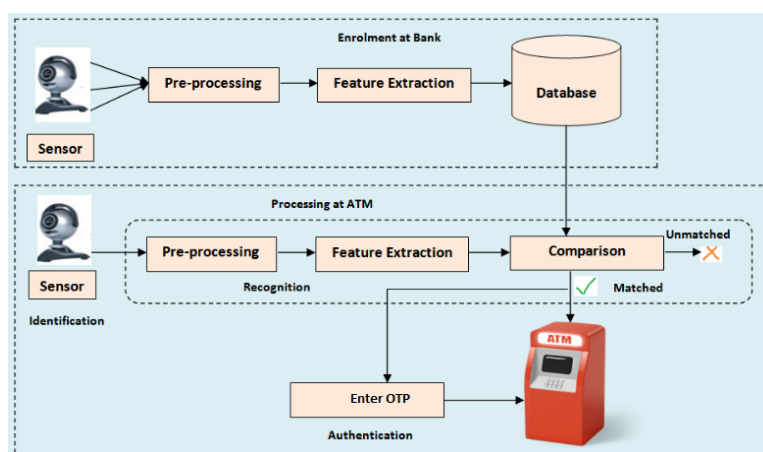


Figure. 2:Architecture of the proposed system

Camera is used for authentication of user. We are using Keypad and camera of PC/laptop. Whenever a person enters in ATM camera captures image and display information about him. GUI (Graphical User Interface) is developed for user and system interactions. An OTP, which along with face recognition comprises two levels of security. When face and

OTP are matched then customer's account will open in ATM machine. GUI will display user name, debited money, authentication status etc.

#### Novelty / Innovative Idea / Contribution

Secure Cardless Transaction System is proposed in [1] which eliminate the usage of ATM PIN and physical cards altogether and hence provide a secure environment for cash withdrawal. The concept of User-Generated One Time Password (OTP) has been introduced in this project. In proposed system we are using fingerprint, face as well as OTP for better security.

#### IV. RESULT AND DISCUSSION



Figure. 3 Registration Page



Figure.4 Camera Page

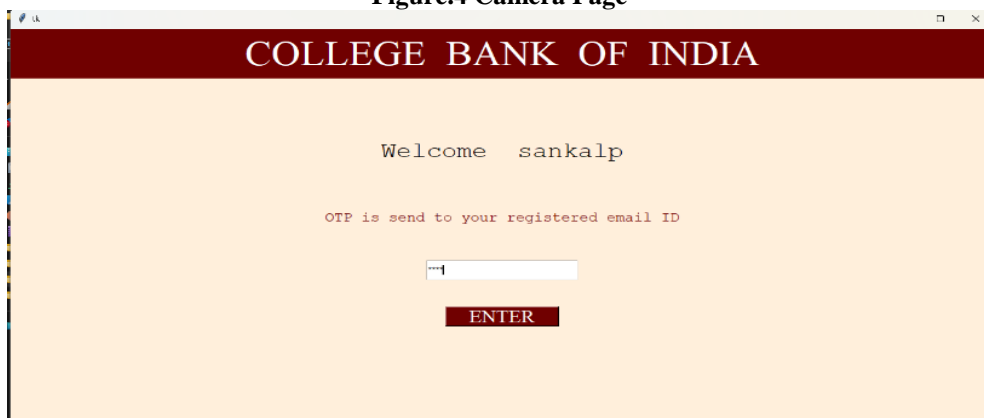


Figure.5 Login page



Figure .6 Home Page

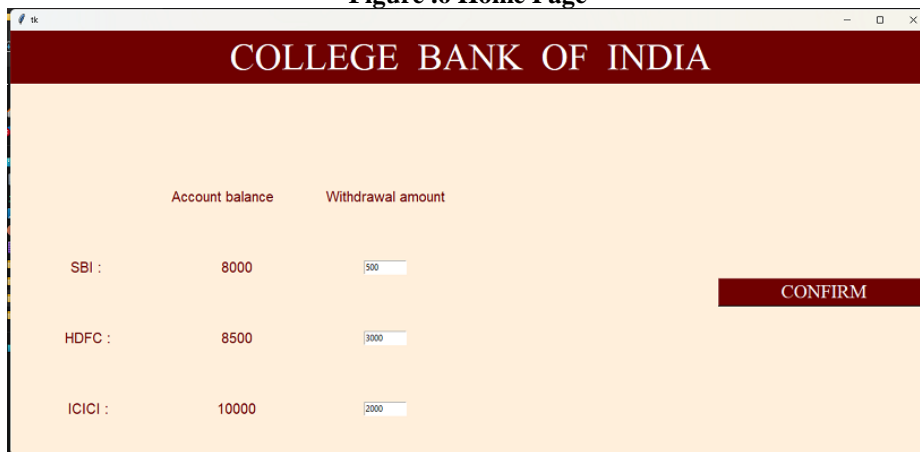


Figure.7 Bank Page 1

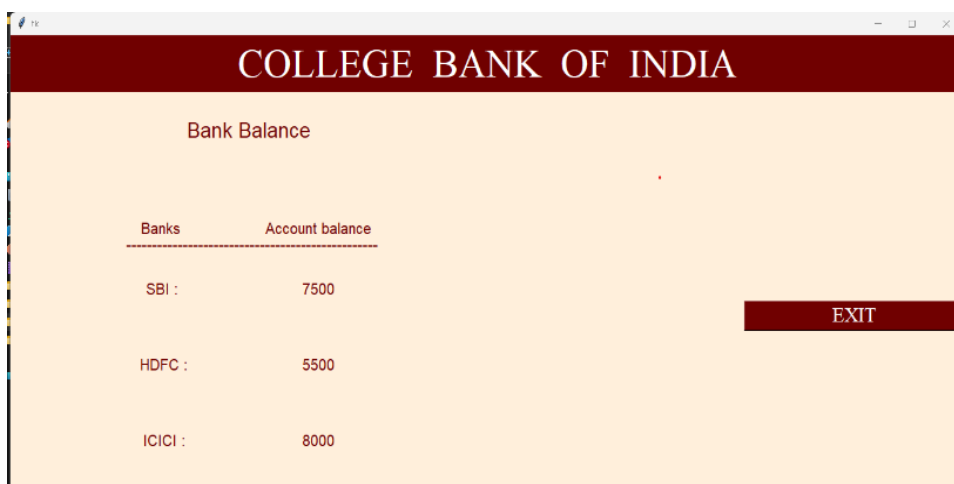


Figure. 8 Bank Page 2

#### IV. CONCLUSION

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The proposed system can provide a practical and workable solution that addresses the requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the face detection authentication technique

because it utilizes the components of the existing system. The model can also provide for high withdrawal limits to cater for the demands of a cash-focused customer base. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions.

## REFERENCES

- [1] KhushbooYadav; SuhaniMattas; LipikaSaini; Poonam Jindal, "Secure Card-less ATM Transactions", 2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA)
- [2] OTP Based Cardless Transaction using ATM Md. Al Imran, M.F. Mridha, Md. KamruddinNur 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), doi:10.1109/ICREST.2019.8644248
- [3] Hassan, Ahsana; George, Aleena; Varghese, Liya; Antony, Mintu; K.K, Sherly (2020). [IEEE 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) - Coimbatore, India (2020.7.15-2020.7.17)] 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA) - The Biometric Cardless Transaction with Shuffling Keypad Using Proximity Sensor. , (), 505–508. doi:10.1109/ICIRCA48905.2020.9183314
- [4] Banerjee, Indranil; Mookherjee, Sjivangam; Saha, Sayantan; Ganguli, Souradeep; Kundu, Subham; Chakravarti, Debduhita (2019). [IEEE 2019 International Conference on Opto-Electronics and Applied Optics (Optronix) - Kolkata, India (2019.3.18-2019.3.20)] 2019 International Conference on Opto-Electronics and Applied Optics (Optronix) - Advanced ATM System Using Iris Scanner. , (), 1–3. doi:10.1109/OPTRONIX.2019.8862388
- [5] Tyagi, Abhishek; Ipsita, ; Simon, Rajbala; khatri, Sunil Kumar (2019). [IEEE 2019 4th International Conference on Information Systems and Computer Networks (ISCON) - Mathura, India (2019.11.21-2019.11.22)] 2019 4th International Conference on Information Systems and Computer Networks (ISCON) - Security Enhancement through IRIS and Biometric Recognition in ATM. , (), 51–54. doi:10.1109/ISCON47742.2019.9036156
- [6] Mahansaria, Divyans; Roy, Uttam Kumar (2019). [IEEE 2019 International Carnahan Conference on Security Technology (ICCST) - CHENNAI, India (2019.10.1-2019.10.3)] 2019 International Carnahan Conference on Security Technology (ICCST) - Secure Authentication for ATM transactions using NFC technology. , (), 1–5. doi:10.1109/CCST.2019.8888427
- [7] Kale, PriyankaHemant; Jajulwar, K. K. (2019). [IEEE 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19) - Nagpur, India (2019.11.1-2019.11.2)] 2019 9th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-19) - Design of Embedded Based Dual Identification ATM Card Security System. , (), 1–5. doi:10.1109/ICETET-SIP-1946815.2019.9092027
- [8] Fingershield ATM – ATM Security System using Fingerprint Authentication Christiawan1 , BayuAji Sahar2 , Azel Fayyad Rahardian3 , ElvayandriMughtar doi:10.1109/ISESD.2018.8605473
- [9] Swathi, H; Joshi, Suraj; Kiran Kumar, M.K. (2018). [IEEE 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAIECC) - Bangalore, India (2018.2.9-2018.2.10)] 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAIECC) - A Novel ATM Security System using a User Defined Personal Identification Number With the Aid of GSM Technology. , (), 1–5. doi:10.1109/ICAIECC.2018.8479533
- [10]Embarak, Ossama H. (2018). [IEEE 2018 Fifth HCT Information Technology Trends (ITT) - Dubai, United Arab Emirates (2018.11.28-2018.11.29)] 2018 Fifth HCT Information Technology Trends (ITT) - A two-steps prevention model of ATM frauds communications. , (), 306–311. doi:10.1109/CTIT.2018.8649551





Impact Factor: 8.379



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details