

## AI BASED CARDLESS ATM TRANSACTION USING FACE RECOGNITION

**Sathish Kumar P**  
Computer Science and  
Engineering  
Francis Xavier Engineering  
College  
Vannarpettai – Tirunelveli  
[sathishkumarp.ug19.cs@francisc Xavier.ac.in](mailto:sathishkumarp.ug19.cs@francisc Xavier.ac.in)

**Rajamanickam R**  
Computer Science and  
Engineering  
Francis Xavier Engineering  
College  
Vannarpettai – Tirunelveli  
[rajamanickamr.ug19.cs@francisc Xavier.ac.in](mailto:rajamanickamr.ug19.cs@francisc Xavier.ac.in)

**Sudhakar S**  
Computer Science and  
Engineering  
Francis Xavier Engineering  
College  
Vannarpettai – Tirunelveli  
[sudhakars.ug19.cs@francisc Xavier.ac.in](mailto:sudhakars.ug19.cs@francisc Xavier.ac.in)

**Mrs. Priskilla Angel Rani J**  
Asst. Professor / Dept. of Computer  
Science and Engineering  
Francis Xavier Engineering College  
Vannarpettai – Tirunelveli  
[priskillaangelranij@francisc Xavier.ac.in](mailto:priskillaangelranij@francisc Xavier.ac.in)

### **Abstract:**

*Nowadays we are experiencing a radical increase in skimming in the Automated Teller Machine (ATM) systems. So, actuation in advancement and security of the ATM machines is required. 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. In order to recognise a person's face in a photo or video, face recognition*

*technology is utilised. The fundamental difficulty in face recognition is correctly identifying a person's face even under challenging circumstances, including dim illumination or blurry photos. Face recognition is a major issue because it needs to accurately identify and align facial features such as the mouth, nose, eyes, and jawline in order to extract the necessary data for identification. In addition, the use of facial recognition technology raises ethical and privacy problems that have been a problem in recent years. As a result, sophisticated algorithms and methods are required to increase the reliability and accuracy of face recognition systems*

**Keywords – Face Recognition, 4-digit pin number, Bank details.**

### **I. INTRODUCTION**

Detection of single-trial EEG of the neural correlates of familiar faces recognition using machine learning algorithms [1] Facial

Verification Technology for Use in ATM Transactions [2] Cash withdrawals via ATMs are still a common practise today, although they can encounter a number of problems. We suggest using card-less transactions to address issues like skimming and card cloning brought on by the use of cards. The system demands that ATMs be used, and those ATMs must have software installed that allows users to verify their identities using a reference number, login ID, and password. My SQL-created databases served as record sheets for each account user, storing information such as user ids, passwords, account balances, reference numbers, and withdrawal amounts among other things. Recognition Application for Automatic Teller Machines (ATM) [3].

Short Term Face Recognition for Automatic Teller Machine (ATM) Users [4]. The system's fundamental operation is to use a mobile application that has been installed for cash withdrawals, sign in, and generate a reference number of the user's choosing that includes the amount to be withheld together. SEPIA: Secure-PIN-authentication-as-a-service for ATM using Mobile and wearable devices [5]. Multiple Level Information Security Using Image Steganography and Authentication [6]. Once generated by the user, this reference number would be good for about a half-hour, depending on the bank's preference. The user must then proceed to the ATM, sign in using their user name, password, and a code that will flash in their mobile application, and then finish the transaction. For each user, this code is modified minute by minute in the application. The user will be approved if the user id, password, and code are for entering the reference number. The ATM will dispense the cash if the reference number is also a match.

As a result, the system will offer three levels of protection, starting with a password or lock on the mobile app to confirm the user's identity. The user will login to the ATM machine using their user ID, password, and the code that is present in the mobile app at the second stage of

authentication. The user would then complete the final step of authentication by keying in the reference number into the ATM. So, the suggested approach totally abolishes the use of ATM cards and resolves related issues. As the reference number is produced by the user each time a transaction is made, the security is further increased. Moreover, this resolves the issues brought on by OTP sharing.

### **A. History:**

The debut of Automated Teller Machine (ATM) dates back to 1967. The first machine was installed in Barclays' Enfield Town in London. In Europe at that time, banks were already searching for ways to make cash withdrawal services to be made available to general public after working hours. This is when John Shepherd-Barron thought about vending machines which sold chocolate bars and the idea struck as to why a similar mechanism wasn't being used to withdraw cash. This is the revolutionary idea which changed the face of retail banking. The Personal Identification Number (PIN) was introduced much later in 1970. James Goodfellow was the person behind the concept of PIN which could be stored on cards. This was one of the most important moments in the history of ATM since it meant that the humans could be identified and verified by machines without the need of human intervention. Support vector machine the most fruitful algorithm for prognosticating heart disorder [7]. Overview Of Techniques For Face Recognition [8].

### **B. Existing Problems:**

In recent past, the banking frauds have been on a constant rise. The fraudsters aim at looting money through online banking methods and also target transactions via debit, credit and ATM cards. ATM card frauds have been present since the time ATMs were invented but the number and types of fraud cases have increased drastically. The fraudsters are robbing the people of their hard-earned money

via these methods. There are two things which are required to access the account of an individual- card issued by the bank and the PIN. With the rise of cybercrime various means have been developed to intercept the user's PIN and the card details stored in the magnetic strip. Fake cards can then easily be created and funds can be withdrawn from the account of the unsuspecting individual. In such times it is essential to be well informed about such frauds and dedicate the research towards overcoming these problems. Pedestrian Re- Identification Using Deep Learning [9]

- **Card Skimming:** This is one of the most popular and common technique. Skimming essentially refers to stealing or duplicacy of the data present in the electronic card which ultimately enables the criminal to forge the ATM card. During this process the customer can use their card normally and won't be notified of any suspicious activity till the time the amount has been withdrawn and the account has been defrauded. This cloning technique is responsible for maximum number of frauds taking place. Here the card details are stolen by placing a foreign device in the ATM machine. The PIN is also then captured and eventually the card is cloned.

- **Eavesdropping:** Similar to its contextual meaning, eavesdropping is a technique via which the card data is stolen by a foreign device placed by the criminal on the card. This can be achieved via methods like wire trap, reading the card reader functionality or having a magnetic reader installed within the reader. The principle of this method is the use of proper card reading functionality.

- **Cash shimming:** In Card Shimming method, the data is targeted which is present on the chip of the ATM card. Here, a foreign material is placed between the ATM card and the card reader present in the ATM machine. By using this method, the fraudster can capture the data of multiple cards. Also, the attacks can be

carried out in multiple ways like capturing the data equivalent magnetic strip or relay etc.

### C. Motivation:

Keeping the above-mentioned problems in mind, we wanted to devise a solution which would enable customers to use their cards without any fear in a secure environment. This was the motivation behind this project. Some measures which have been included to boost the safety of ATM cards involve chip enabled cards which are used to verify whether the card is fake or genuine. Other methods like CNN (Convolutional neural network), have been implemented for debit and credit card purchasing methods but for ATM services such a method is still not available which is what motivated us to develop something which could omit the contact of the ATM card with the machine altogether. Many ideas have been proposed to solve the issues related to banking frauds. face recognition techniques have been a topic of research for a long time. A Novel Data Privacy- Preserving Protocol for Multi-data Users by using genetic algorithm [10]. This includes authentication using face recognition, secondary 4-digit pin number. In the author has proposed the use of image recognition to verify the identity of the user. The system requires that the dataset images be installed in all ATMs. In the author proposes to provide three tier security system involving the use of CNN and OTP verification. Encryption techniques to provide secure exchange of data over cloud have been discussed.

## II. LITERATURE REVIEW

### 1. Resolution Invariant Face Recognition using a Distillation Approach (IEEE 2020).

In this study, they suggest employing both HR and LR pictures to train a network under the supervision of a fixed network that has already been trained on HR face photos. By dividing the Soft max weights between the two networks and minimising the KL-divergence between the output Soft max probabilities of the pretrained

(i.e., Teacher) and trainable (i.e., Student) networks, the advice is provided.

## 2. Advanced ATM System Using Iris Scanner (IEEE 2019).

The biometric scanners used in the offered design, such as the iris scanner and the two-way check with the fingerprint scanner, give it a distinctive quality. The system can access the subsequent stages for the transaction since the iris scanner is the primary security check. The ATM card's inbuilt fingerprint scanner serves as the system's secondary security check. Only when the cardholder's inputted data matches what is in the database is the transaction process considered successful. It is appropriate for usage since it uses less energy. Comparing the proposed modified approach to the other current categorization and affirmation procedures for ATMs, it is practical and inexpensive.

## 3. A Constraint-based Biometric Scheme on ATM and Swiping Machine (IEEE 2016).

Biometric process for a single little debit? and "What may be the greatest loss if one's card is used fraudulently?" We suggest a restriction on ATM transactions employing biometrics as a solution to enhance system performance and address the stated problems. The suggestion is broken up into two sections. By imposing a restriction on the amount of cash that may be withdrawn and the number of transactions, the first portion addresses the sensor performance issue. If one seeks to withdraw several little amounts OR needs to withdraw a large amount, they must first produce their biometric.

## III. SYSTEM IMPLEMENTATION

### EXISTING SYSTEM

The ATM using Face Recognition System is indicate the way to a lot of forgery attempt and abuse through card theft and pin theft of customer account details. In this system they are used many components like Face Detector, Face Recognizer, 2-D, 3-D Technique and Surface Texture Analysis. In the existing

System they use some of the machine learning techniques to predict the facial expression but the output accuracy is very low it may be < 70%.

### PROPOSED SYSTEM

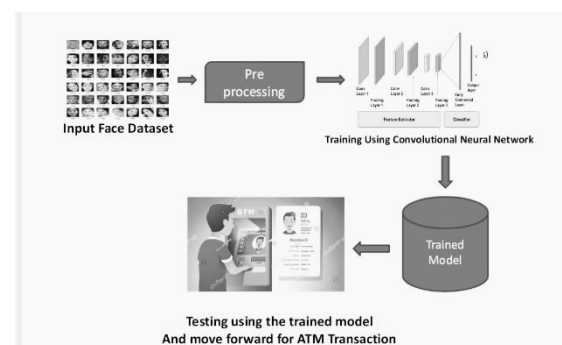
The proposed system we use Convolutional Neural Network to predict the face recognition. It consists of the following steps:

- the face in image is detected and cropped,
- the cropped image is pre-processed in order to provide further illumination invariant,
- the convolutional neural network is applied to predicted features.

### PROCESS OF (CNN) TECHNIQUE

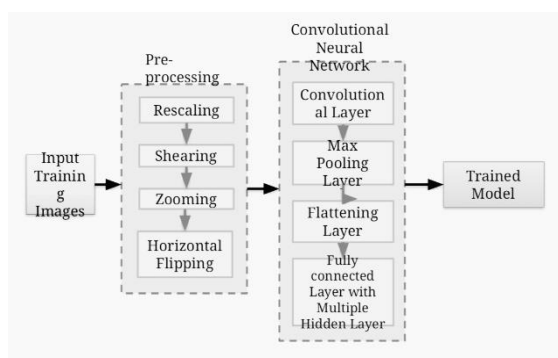
In the beginning of our project, we will gather user face images. We will take 50 pictures of each user's face, and each of those 50 pictures will be kept in a separate folder. The user faces that have been gathered are used for training and validation purposes. After data collection, pre-processing methods like zooming, shearing, rescaling, and horizontal flipping are used on the user's face photos. We next feed these pre-processed data into our convolutional neural network model. Convolutional neural networks are used for the training process, and the trained model is saved as a file for testing.

### Proposed System Architecture:



To get the 97% accuracy in our project, we shall train the image data more than 100 times. Using the trained model, we can classify the users' faces in real time after training. A 97% accurate result will likewise be obtained when testing an image using our trained model. Following the prediction of the user's image and receipt of their banking information, the machine next requests the user's four-digit secret pin in order to complete the transaction. In the event that their face and 4-digit pin number match, they are able to conduct transactions; otherwise, they are unable to do so.

### Training Model:



## IV. CONCLUSION AND FUTURE SCOPE

### A. Conclusion:

By doing away with card swiping, the suggested solution intends to address the issues of card cloning at numerous locations, including ATM machines, shopping centres, retail stores, etc. It enables the user to create a reference number based on their needs. The exchange of data is safe when encryption software like b crypt is used. Also, there will be three layers of protection provided by the checks being made to confirm the user's identity: authentication at the time of signing in to the website, via the password and the code flashing on the smartphone screen, and through the reference number. The degree of vulnerability is diminished by the reference number expiring after a set period. This essay

aims to address the problem of banking frauds and assaults, which can be developed and improved a lot further.

### B. Future Scope:

There is always room for improvement because no suggested solution can be considered to be perfect for the vulnerability of the banking system to assaults. This system, like all others, has benefits and problems of its own.

It is possible to enhance the cryptography method being utilised here. Moreover, a mobile application might be developed in place of a website to make this system more portable and to make signing in repeatedly easier.

The creation of a mobile application as well as modifications to ATMs are necessary for the proposed idea to be implemented properly. The biggest problem that will prevent the system from functioning correctly is the slow internet. So, adjustments might be made to get rid of the issue. Hence, even though the concept tries to There are several factors that must be taken into account for the system to operate successfully and efficiently, including the card cloning issue.

## V. RESULT

The problem of cardholder impersonation can be solved by this project. Similar to two-factor authentication, facial recognition is used to verify that the transaction was carried out by the cardholder or other individuals they have trusted. It restricts the use of cards by unauthorised individuals who know a cardholder's password.

As a result, this ATM model offers protection against identity exploitation by implementing a verification system that uses face recognition to certify the user's identity and greatly reduce forced transactions.

```

Python 3.7.3 Shell
File Edit Shell Debug Options Window Help

5.29474978943622
[0. 1.]
D Numpy Array:
0. 1.]

0. 1.]
.0
rue
athish Kumar

03.41367031645382
[0. 1.]
D Numpy Array:
0. 1.]

0. 1.]
.0
rue
athish Kumar

ello Sathish Kumar, You are logged in, to your account

lease Enter the 4 digit Code : 4321
assword Matched
lease Enter Amount: 100
nt64Index([1], dtype='int64')
nt64Index([1], dtype='int64')
9206

Unnamed: 0  Account_No  ...      Branch  Total_Amount
0  7836489347  ...      Palayamkottai  4290
1  7860574006  ...      Vannarapettai  19100
2  7564839756  ...      Town  32000
3  9067453647  ...      Perumalpuram  5100
4  9687463957  ...      Palayamkottai  2800

5 rows x 6 columns]
lease collect your cash
our Available Balance is : 19100

```

**Fig: Bank Transaction**

## VI. REFERENCE

[1] Abdulmajeed, Alsufyani<sup>1</sup>, Alrooba<sup>ae1</sup>, Ahmed, Rooba<sup>ae1</sup>, **Detection of single-trial EEG of the neural correlates of familiar faces recognition using machinelearning algorithms**, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.2855-2860.

[2] Aru, O.Ezeand I.Gozie, **Facial Verification Technology for Use in ATM Transactions**, in American Journal of Engineering Research (AJER), [Online] 2013, pp. 188-193. <https://doi.org/10.30534/ijatcse/2019/28862019>

[3] H.R.Babaei, O.Molalapata and A.A.Pandor, **Face** MurugesanM.*et al.*, International Journal of Advanced Trends in Computer Science and Engineering, 9(2), March - April 2020, 1295 – 1299 **Recognition Application for Automatic Teller Machines (ATM)**, in ICIKM, 3rdvol.45, November–December 2012, pp.211-216.

[4] E.Derman, Y.K.Gecici and A.A.Salah, **Short Term Face Recognition for Automatic Teller Machine (ATM) Users**, in ICECCO

2013, Istanbul, Turkey, pp.111-114. <https://dx.doi.org/10.21172/1.841.20>

[5] JinfangXu, Khan, Rasib and RasibHasan, **SEPIA: Secure-PIN-authentication-as-a-service for ATM using Mobile and wearable devices**, 3rdIEEE International Conference on Mobile Cloud Computing, Services, and Engineering IEEE, June 2015, pp. 41-50.

[6] Marilou O. Espina<sup>1</sup>, Arnel C. Fajardo, Bobby D. Gerardo, RujiP. Medina, **Multiple Level Information Security Using Image Steganography and Authentication**, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.3297-3303. <https://doi.org/10.30534/ijatcse/2019/100862019>

[7] M.Murugesan, R.Elankeerthana, **Support vector machine the most fruitful algorithm for prognosticating heart disorder**, International Journal of Engineering and Technology, Volume 7, pp.48 – 52, 2018. <https://doi.org/10.14419/ijet.v7i2.26.12533>

[8] M.Murugesan,S.Thilagamani, **Overview Of Techniques For Face Recognition**, International Journal Of Life Science and Pharma Reviews, pp.66 - 71, 2019, ISSN2250 – 0480. <https://dx.doi.org/10.22376/ijpbs/10.SP01/Oct/2019>

[9] M.Murugesan, R.Elankeerthana, **Pedestrian Re- Identification Using Deep Learning**, International Journal Of Life Science and Pharma Reviews, pp.71 - 78, 2019, ISSN 2250 – 0480.

[10] P.Pandiaraja, N. Deepa, **A Novel Data Privacy- Preserving Protocol for Multi-data Users by using genetic algorithm**, Journal Soft Computing Volume 23 Issue 18, pp8539-8553, 2019.