IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.12509

Real Time Secure Clickbait and Biometric ATM User Authentication and Multiple Bank Transaction System

Mr. Jimson.L[1], Vishwa S[2], Rayner Raj A[3], Vimal Marccus R[4]

Assistant Professor, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[1]

B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[2]

B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[3]

B.E, Department of Computer Science and Engineering, DMI College Of Engineering, Chennai, India[4]

Abstract: ATM or Automated Teller Machines are widely used by people nowadays. Performing cash withdrawal transaction with ATM is increasing day by day. ATM is very important device throughout the world. The existing conventional ATM is vulnerable to crimes because of the rapid technology development. A total of 270,000 reports have been reported regarding debit card fraud and this was the most reported form of identity theft in 2021. A secure and efficient ATM is needed to increase the overall experience, usability, and convenience of the transaction at the ATM. In today's w kl, orld, the area of computer vision is advancing at a breakneck pace. The recent progress in biometric identification techniques, including finger printing, retina scanning, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. Specifically, the goal of this project is to give a computer vision method to solve the security risk associated with accessing ATM machines. This project proposes an automatic teller machine security model that uses electronic facial recognition using Deep Convolutional Neural Network (DCNN). If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Clickbait Link will be generated and sent to bank account holder to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of account safety making it possible for the actual account owner alone have access to his accounts. This eliminates the possibility of fraud resulting from ATM card theft and copying. The experimental results on real-time datasets demonstrate the superior performance of the proposed approach over state-of-the-art deep learning techniques in terms of both learning efficiency and matching accuracy. By using this real time dataset, the proposed system achieves the highest accuracy with 97.93%

Keywords: AI, ATM, CNN, DCNN, FVCL

I. INTRODUCTION

A. Overview

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. ATMs allow banking customers to avail quick self-serviced transactions, such as cash withdrawal, deposit, and fund transfers. ATMs enable individuals to make banking transactions without the help of an actual teller. Also, customers can avail banking services without having to visit a bank branch. Most ATM transactions can be availed with the use of a debit or credit card. There

In 1960, an American named Luther George Simian invented the Bank graph, a machine that allowed customers to deposit cash and checks into it. The first ATM was set up in June 1967 on a street in Enfield, London at a branch of Barclays bank. A British inventor named John Shepherd-Barron is credited with its invention. The machine allowed customers to withdraw a maximum of GBP10 at a time.

B. Types of Automated Teller Machines (ATMs)

Automated Teller Machines (ATMs) are mainly of two types. One is a simple basic unit that allows you to withdraw cash, check balance, change the PIN, get mini statements and receive account updates. The more complex units provide facilities of cash or cheque deposits and line of credit & bill payments. There are also onsite and offsite Automated Teller

DOI: 10.17148/IJARCCE.2023.12509

Machines: the onsite ATMs are within the bank premises, unlike the offsite ones which are present in different nooks and corners of the country to assure that people have basic banking facilities and instant cash withdrawals if they can't go to a bank branch. ATMs can also be categorized based on the labels assigned to them. Some of these labels are listed below-

- Green Label ATMs- Used for agricultural purposes
- Yellow Label ATMs- Used for e-commerce transactions
- Orange Label ATMs- Used for share transactions
- Pink Label ATMs- Specifically for females to help avoid the long queues and waiting time
- White Label ATMs – Introduced by the TATA group, white label ATMs are not owned by a particular bank but entities other than the bank
- Brown Label Banks- Operated by a third party other than a bank

C. Uses of an Automated Teller Machine

Automated Teller Machines have revolutionized the banking sector by providing easy access to customers and loading off the burden from bank officials. Some of the uses of an ATM are-

The most common uses of an Automated Teller Machine include withdrawing money, checking balance, transferring money, or changing the PIN (Personal Identification Number) Newer and advanced ATMs also provide options to open/withdraw a Fixed Deposit (FD), or to apply for a personal loan. You can also book railway tickets, pay the insurance premiums, income tax & utility bills, recharge mobile, and deposit cash. Some of these facilities require you to register at the bank branch Customers can now do money transactions at their convenience. ATMs today are installed in public spaces, highways, malls, market places, railway/airport stations, hospitals, etc.

Automated Teller Machines provide 24×7 access anywhere ATMs help to avoid the hassle of standing in long queues at the bank even for simpler transactions like withdrawing money. It has also helped in reducing the workload of the bank officials.

II. LITERATURE SURVEY

Piyumi Seneviratne; Dilanka Perera, (2020 ATM is one of the common information systems in use and often ATM keypad entries include the PIN of an ATM user. The PIN is a piece of confidential customer information which uses for the authentication of a transaction. The banking system operates mainly under the trust assumption that the PIN is secured and kept in private by both the system and the customer to ensure the security requirement of confidentiality. The author developed an experimental design to show that it is possible to infer the PIN using video footage during the situations where both the keypad and fingertips are not visible to the attacker. A lab study was conducted to infer the PIN by human observers. Further, an OpenCV Python program was used to automate the PIN inference. PIN is one factor of the two-factor authentication system used in ATM transactions. Banks invest heavily to ensure that a PIN is generated inside an HSM and revealed only to the customer. This indicates that banks operate under the assumption that the PIN is known only to the customer. However, surveillance cameras installed inside ATM cubicles to improve physical security open up a side-channel that can potentially reveal the PIN to third parties.

Khushboo Yadav; Suhani Mattas, (2020) In the current system, user needs to visit the nearest ATM, swipe the card in the ATM machine there to withdraw money. This physical contact of card and machine makes it easier for the fraudsters to capture the data and misuse it. The proposed solution eliminates this physical contact. 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. 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. This system provides a three-level security, first when user's identity is verified while logging in the system, second through user-id, password and the code present in the mobile app – when entered in the ATM machine and last via the reference number.

DOI: 10.17148/IJARCCE.2023.12509

Rahul Patil; Sagar Salunke; Rajesh Lomte (2019) Nowadays, dependency on banking in the virtual world has been increased to the peak position. To make it consistent advanced technologies should be used. As OTP is currently used worldwide for security purposes, it can be overruled by QR code. A QRcode scanner is required to detect code and decrypt information in stored in QRcode. Scanner need to be installed in the ATM machine to take input credentials from the user. We will provide extra feature to an existing system, so traditional withdrawing option is also there. On other end, ATM machine will scan the QRcode generated by 'GetNote'- android application and decrypt it with the key stored in the database. After decryption ATM will get required credentials such as card number, amount, pin, cvv number on card etc. It will authenticate all the details with the banks database. After successful authentication, cash will be dispensed by the ATM machine. ATM machine will responsible for validating the QRcode such as difference in generation time and scanning time is not more than five minutes. ATM will able to detect QRcode from image uniquely, duplicate QRcode will be rejected. System will detect QRcode generated by GetNote (android application) only.

Priyanka Hemant Kale; K. K. Jajulwar (2019) As we know day by day the usage of ATM cards and crimes related to it has been increased in huge amount. The number of cases related to ATM fraud has been registered in the past 3 years from 2016-2018. There are some techniques used by criminals to steal your card information and ATM card. ATM skimming, Shoulder surfing, Card trapping, Cash trapping are some of the popular techniques for executing such ATM card frauds. Sometimes the intimation from the bank through Short Message Service (SMS) is also blocked by the hackers/fraudsters. If our ATM card information or ATM card itself is stolen and transaction is executed by the fraudster, the ATM card owner receives SMS only after completion of the transaction. Hence the transaction can’t be retrieved easily. To overcome such crimes the new authentication features of fingerprint and OTP must be added to the ATM. Whenever the ATM transaction has been processed the ATM asks to enter PIN. After entering PIN, the OTP is sent to the number to which your bank account is linked and the transaction can be possible. But in this system, only entering PIN is not enough, after entering a PIN the user needs to choose any one option to make the whole transaction successful that option is fingerprint or OTP. If the user chooses the option of OTP generation, then an OTP is sent to the user’s mobile number to which the bank account is linked this OTP is generated using the GSM module. After entering the OTP, the transaction is executed successfully if the wrong OTP is entered then the process for making transaction is stopped. OTP is safe as per security purpose because OTP is available for a specific duration and for every new transaction a new OTP is generated. If the user chooses another option that is fingerprint, then the user needs to scan their fingerprint on the fingerprint scanner and the user can do future transactions if the fingerprint is not matched with the user’s fingerprint than the transaction process is stopped. A person's finger consists of a unique pattern which involves more security to the current ATM. Even the Europay, Mastercard and Visa (EMV) chip cards which are replaced by magnetic strip ATM cards are not that much secured. EMV-capable chip reader card generates a unique code for each transaction. EMV card provides more security to ATM cards but still the cardholder needs to take some precautions as they used to take before.

Abhishek Tyagi, Ipsita; Rajbala Simon; Sunil Kumar khatri (2019) Nowadays iris recognition is getting more popular in terms of security. Iris pattern is more stable with ages, uniqueness, 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. Customer’s 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.

Divyans Mahansaria; Uttam Kumar Roy (2019) The most important goal of an authentication system is to protect users’ privacy, i.e. the attackers cannot pretend to be the real user. To achieve this goal, in the existing method of authentication in ATM, the attackers should not be able to get the PIN and the corresponding ATM card at the same time. Also, the authorized actions after a successful authentication should be secure as well. The objective of our proposed work is to replace physical ATM cards by smart phones in NFC Card Emulation mode during an ATM transaction to counter the issues prevalent with the use of ATM cards. The combination of NFC with smart devices has led to widening the utilization range of NFC. In card-emulation mode, a NFC device behaves like a contactless smart card. In this mode, the mobile phone does not generate its own RF field; the NFC reader creates this field instead. At the ATM kiosk, in order to authenticate, the user needs to swipe his/her mobile phone in front of the NFC reader. During an ATM transaction, an ATM card is not required and the system will still have a stronger security compared to the system in which ATM card was used. Through data encryption and secure channels, NFC technology keeps the customer information safe. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

DOI: 10.17148/IJARCCE.2023.12509

M.K. Kiran Kumar Year: 2018 The objective of this paper is to provide a more secured method using bio-metric features and message authentication technique. In our proposed method, PIN verification is combined with fingerprint recognition, to identify a customer during ATM transaction. Fingerprint is verified using efficient minutiae feature extraction algorithm. To assure the security while doing transaction through swipe machine, the client will confirm the transaction by an approval message through GSM technology. In both cases, location will be identified through GPS. If any illegitimate person tries to use the card it will automatically be blocked by the system and detail information will be sent to the customer through the message.

H Swathi; Suraj Joshi; (2018) Presently, ATM systems use no more than an access card which usually has a magnetic stripe (magstripe) and a fixed Personal Identification Number (PIN) for identity verification. Some other cases utilize a chip and a PIN which sometimes has a magstripe in case the chip fails as a backup for identification purposes. This method is not very secure and prone to increase in criminal activities. The need for a novel, simple as well as secure method of access is thus imperative. In the present work, 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. In this method, the users register and enroll themselves with the bank and decide on a biometric authentication process that can be carried out on their phone and a capture tool has to be installed. The authentication phase includes an added security layer which is the biometric authentication phase. A brief summary of the authentication process is as follows: The system generates an OTP and the user has to enter this OTP into the system. When the OTP is received by the banking system, it is encrypted (using a secure key) and sent to the ATM terminal. Here it is encoded into a QR code image which is displayed on the screen and must be scanned by the user. The mobile phone decodes the QR code image and the user is prompted to complete a biometric test using the mobile phone. This is followed by the decryption of the OTPs by the mobile phone and finally the user enters the OTP into the system to begin the transaction.

Shivangi Gupta; Sunil Kumar Chowdhary

(2017) The basic concept of this biometric technology consists of phases of feature extraction and classification of features. As good quality heartbeat is captured and traced through fingerprints. Then pre-processing of ECG signals is conducted which is followed by feature extraction through non-fiducial approach. In classification phase, emotions are studied to determine the various emotional conditions of the human being (fear, anxiety, stress, etc.). Therefore, this will help machine to differentiate between threat and anxiety condition of a person and will instruct machine whether or not to perform ATM transaction. This paper mainly proposes and highlights.

III. PROPOSED SYSTEM

Facial Biometric Authentication System using Deep Learning Techniques Deep learning is a subset of machine learning, which, in turn, is a subset of artificial intelligence (AI). When it comes to Face recognition, deep learning enables us to achieve greater accuracy than traditional machine learning methods.

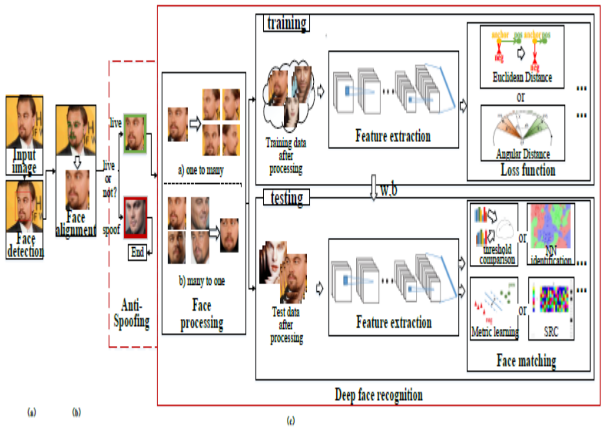


Figure 1 Facial Biometric Authentication System using Deep Learning Techniques

DOI: 10.17148/IJARCCE.2023.12509

Deep FR system with face detector and alignment. First, a face detector is used to localize faces. Second, the faces are aligned to normalized canonical coordinates. Third, the FR module is implemented. In FR module, face anti-spoofing recognizes Whether the face is live or spoofed; face processing is used to handle variations before training and testing, e.g., poses, ages; Different architectures and loss functions are used to extract discriminative deep feature when training; face matching methods are used to do feature classification after the deep features of testing data are extracted.

CNN Face Recognition Step

Filters=32: This number indicates how many filters we are using to look at the image pixels during the convolution step. Some filters may catch sharp edges, some filters may catch color variations some filters may catch outlines, etc. In the end, we get important information from the images. In the first layer the number of filters=32 is commonly used, then increasing the power of 2. Like in the next layer it is 64, in the next layer, it is 128 so on and so forth.

kernel size=(5,5): This indicates the size of the sliding window during convolution, in this case study we are using 5X5 pixels sliding window.

strides= (1, 1): How fast or slow should the sliding window move during convolution. We are using the lowest setting of 1X1 pixels. Means slide the convolution window of 5X5 (kernal_size) by 1 pixel in the x-axis and 1 pixel in the y-axis until the whole image is scanned.

input shape= (64,64,3): Images are nothing but matrix of RGB color codes. during our data pre-processing we have compressed the images to 64X64, hence the expected shape is 64X64X3. Means 3 arrays of 64X64, one for RGB colors each.

kernel_initializer=’uniform’: When the Neurons start their computation, some algorithm has to decide the value for each weight. This parameter specifies that. You can choose different values for it like ‘normal’ or ‘glorot_uniform’.

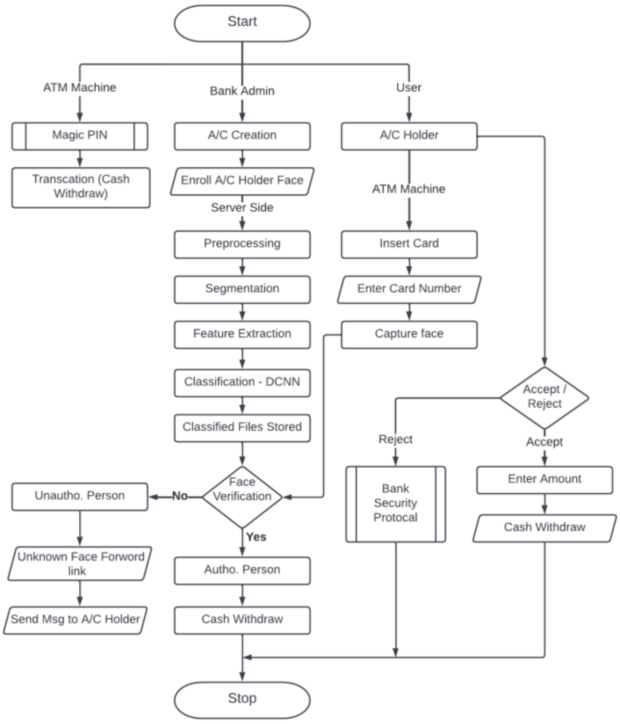
activation=’relu’: This specifies the activation function for the calculations inside each neuron. You can choose values like ‘relu’, ‘tanh’, ‘sigmoid’, etc.

optimizer=’adam’: This parameter helps to find the optimum values of each weight in the neural network. ‘adam’ is one of the most useful optimizers, another one is ‘rmsprop’

batch_size=10: This specifies how many rows will be passed to the Network in one go after which the SSE calculation will begin and the neural network will start adjusting its weights based on the errors. When all the rows are passed in the batches of 10 rows each as specified in this parameter, then we call that 1-epoch. Or one full data cycle. This is also known as mini-batch gradient descent. Hence a proper value must be chosen using hyperparameter tuning.

Epochs=10: The same activity of adjusting weights continues for 10 times, as specified by this parameter.
Unknow Face Verification Link Generator When the stored image and the captured image don't match, it means that he is an unauthorized user. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the transaction appropriately or signals a security-violation alert to the banking security system.

Biometrics measure the unique physical or behavioral characteristics of an individual as a means to recognize or authenticate their identity. Common physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Biometrics may be used for identity establishment. A new measurement that purports to belong to a particular entity is compared against the data stored in relation to that entity. If the measurements match, the assertion that the person is whom they say they are is regarded as being authenticated. The algorithms were trained and tested using well-known biometric database which contains samples of face and speech and similarity scores of five face and biometric Experts.



ATM Fraud

Over the last two decades, automated teller machines (ATMs) have become as much a part of the landscape as the phone booths made famous by Superman. As a result of their ubiquity, people casually use these virtual cash dispensers without a second thought. The notion that something could go wrong never crosses their minds. Most ATM scams involve criminal theft of debit card numbers and personal identification numbers (PINs) from the innocent users of these machines. There are several variations of this confidence scheme, but all involve the unknowing cooperation of the cardholders themselves.

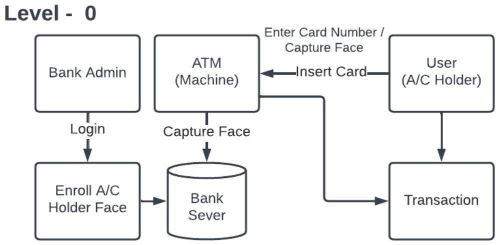
ATM fraud is described as a fraudulent activity where the criminal uses the ATM card of another person to withdraw money instantly from that account. This is done by using the PIN. The other type of ATM fraud is stealing from the machine in the ATM by breaking in. Skimming: This type of ATM scam involves a skimmer device that criminals place on top of or within the card slot. To record your PIN number, the criminals may use a hidden camera or an overlay that covers the original PIN pad. Using the card numbers and PIN's they record; thieves create duplicate cards to withdraw money from consumers' accounts. Unlike losing your debit card or having it stolen, you won't realize anything is amiss until unauthorized transactions take place. Take a look at these so you know how to detect ATM skimmers.

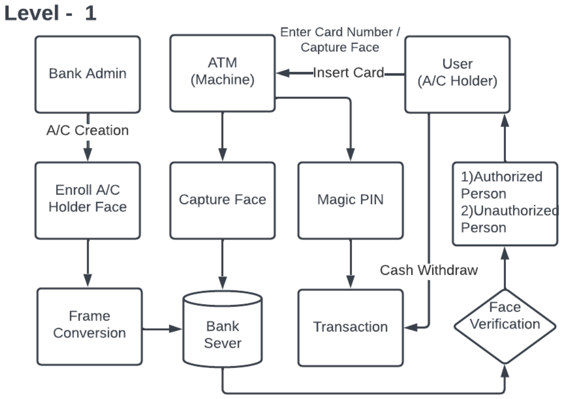
Shimming: This is the latest update to skimming. Instead of reading your card number, criminals place a shimming device deep inside the ATM to record your card's chip information. The end result is the same as skimming because thieves use the stolen chip data to create "cloned" versions of your debit card.

Cash-out**:** This scam targets multiple accounts from the same financial institution. Armed with a hacked bank employee's credentials, the criminal alters account balances and withdrawal limits. Using stolen debit card numbers captured from a separate skimming attack, they can "cash out" the ATM until it's out of money.

Jackpotting**:** While there are multiple types of jackpotting attacks, typically, these incidents involve gaining physical access to the inside of the machine. The criminals may replace hardware or install malicious software giving them control of the cash dispensing function. Jackpotting is similar to a cash out scam, but it does not require the criminal to have any customer account details or stolen debit card information.

DOI: 10.17148/IJARCCE.2023.12509



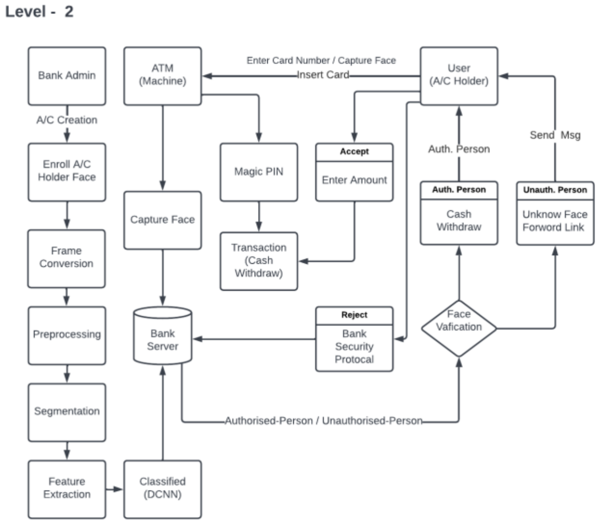


Problem Identified

Nowadays, crimes at ATMs have become an alarming issue. Security for the customer's account is not guaranteed by PIN. Many people, who aren't familiar with the concept of PIN are unlikely to memorize and recognize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel unsafe that their account could be accessed by others and they would lose all their money.

Deep Learning

Deep learning attempts to mimic the human brain—albeit far from matching its ability—enabling systems to cluster data and make predictions with incredible accuracy. Deep learning is a subset of machine learning, which is essentially a neural network with three or more layers. These neural networks attempt to simulate the behavior of the human brain—albeit far from matching its ability—allowing it to "learn" from large amounts of data. While a neural network with a single layer can still make approximate predictions, additional hidden layers can help to optimize and refine for accuracy.



DOI: 10.17148/IJARCCE.2023.12509

Deep learning drives many artificial intelligence (AI) applications and services that improve automation, performing analytical and physical tasks without human intervention. Deep learning technology lies behind everyday products and services (such as digital assistants, voice-enabled TV remotes, and credit card fraud detection) as well as emerging technologies (such as self-driving cars).

IV. RESULT AND DISSCUSSSION

Face recognition can be used to secure ATM transaction and is used as a tool for authenticating users to confirm the card owner.Financial fraud is a very important problem for Banks and current secure information in the ATM card magnetic tape are very vulnerable to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be confirmed as the card owner. Face Based ATM login Process the ATMs which are equipped with Face recognition technology can recognize the human face during a transaction. When there are “Shoulder Surfers" who try to peek over the cardholder’s shoulder to obtain his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be cautious. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are removed.

Touchless - There is no need for remembering your passwords. Only looking at the ATM camera will login the card holder instantly. No physical contact is needed.

Secure - Since your face is your password, there is no need to worry for your password being forgotten or stolen. In addition, the face recognition engine locks access to the account and transaction pages for the card holder as the card holder moves away from the camera of the ATM and another face appears.

V. CONCLUSION

Biometrics as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this project, we have developed to proffer a solution to the much-dreaded issue of fraudulent transactions through Automated Teller Machine by biometrics and Unknown Face Forwarder that can be made possible only when the account holder is physically or far present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a biometric feature for identification is strong and it is further fortified when another is used at authentication level. The ATM security design incorporates the possible proxy usage of the existing security tools (such as ATM Card) and information (such as PIN) into the existing ATM security mechanisms. It involves, on real-time basis, the bank account owner in all the available and accessible transactions

REFERENCES

[1] J. Liang, H. Zhao, X. Li, and H. Zhao, ``Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.

[2] I. Taleb, M. E. Amine Ouis, and M. O. Mammar, ``Access control using automated face recognition: Based on the PCA & LDA algorithms," in Proc. 4th Int. Symp. ISKO-Maghreb, Concepts Tools Knowl. Manage. (ISKO-Maghreb), Nov. 2014, pp. 1-5.

[3] X. Pan, ``Research and implementation of access control system based on RFID and FNN-face recognition," in Proc. 2nd Int. Conf. Intell. Syst. Design Eng. Appl., Jan. 2012, pp. 716-719, doi: 10.1109/ISdea.2012.400.

[4] A. A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, ``Raspberry Pi and computers-based face detection and recognition system," in Proc. 4th Int. Conf. Comput. Technol. Appl. (ICCTA), May 2018, pp. 171-174.

[5] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, ``Full impedance cardiography measurement device using raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informat., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.

[6] A. Li, S. Shan, andW. Gao, ``Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315, Jan. 2012.

[7] C. Ding, C. Xu, and D. Tao, ``Multi-task pose-invariant face recognition," IEEE Trans. Image Process., vol. 24, no. 3, pp. 980-993, Mar. 2015.

[8] J. Yang, Z. Lei, D. Yi, and S. Li, ``Person-specific face antispoofong with subject domain adaptation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 797-809, Apr. 2015.

[9] H. S. Bhatt, S. Bharadwaj, R. Singh, and M.Vatsa, ``Recognizing surgically altered face images using multi objective evolutionary algorithm," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.

[10] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring system using RFID and IOT using cloud," in Proc. Online Int. Conf. Green Eng. Technol. (IC-GET), Nov. 2016, pp. 1-4.