International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

BIOMETRIC AND MAGIC PIN AUTHENTICATION SYSTEM FOR ATM

Ms. V. Kejapriya[1], Ms. S.V. Ahalya[2], Ms. R. Meera[3], Ms. T. Vijayalakshmi[4], Mr. J. Jeba Stanly [5]

[1,2,3,4] UG Scholar, Department of CSE, N.S.N. College of Engineering and Technology, Karur.
[5]Assistant Professor, Department of CSE, N.S.N. College of Engineering and Technology, Karur, Tamil Nadu, India.

Abstract - *Automated Teller Machines also known as ATMs are extensively used by each and everyone at the moment. There is a crucial need to ameliorate security in the banking zone. Due to the prodigious increase in the number of lawbreakers and their pursuit, the ATM has become unconfident. ATM systems at present use no more than an access card and PIN for recognition justify. The contemporary progression in biometric identification techniques, together with retina scanning and face identification has made a substantial effort to ransom the precarious circumstances at the ATM. This project put forward an automatic teller machine security model that would consolidate a physical access card, a MagicPIN, and electronic facial recognition using DCNN. If this technology becomes widely used, faces would be preserved in addition to their accounts. Face Verification Link will be originated and sent to the user to confirm the status of the unauthorized user through some customized artificial intelligent agents, for remote certification. However, it is conspicuous that man's biometric features cannot be reproduced, the approach will go a long way to solve the problem of Account welfare making it possible for the real account owner alone to have access to his accounts.*

Key Words: Automated Teller Machine (ATM), Personal Identification Number (PIN), Deep Convolutional Neural Network (DCNN).

1. INTRODUCTION

ATM: Overview: Automated Teller Machines, desired mention to as ATMs, are one of the most useful extension in the banking sector. ATMs allow banking customers to benefit sprightly self-serviced transactions, such as cash take out, deposit, and fund transfers. ATMs authorize solitary to make banking transactions without the help of an actual teller. Also, customers can ease banking services without having to look in on a bank branch. Most ATM transactions that need no debit or credit card.

Automated Teller Machines Types: Automated Teller Machines (ATMs) are mainly of two kinds. One is a simple fundamental unit that allows you to withdraw cash, check balance, change the PIN, get mini statements and collect account updates. The more complex units provide service of cash or cheque deposits and line of credit and bill payments. There are also onsite and offsite Automated Teller Machines: the onsite ATMs are within the bank premises, unlike the offsite ones which are adjacent in different nooks and corners of the country to assure that people have elemental banking facilities and instant cash withdrawals if they can't go to a bank branch.

Project scope: At the moment, offence at ATMs have become an alarming point at issue. Security for the customer's account is not pledge by PIN. Countless people, who aren't confidential with the concept of PIN are unlikely to remember and recognize it. There are many people who mistrust PIN, such as, if they have lost their card, they would feel dangerous that their account could be explosion by others and they would lose all their cost. Face recognition can be used to assured ATM transaction and is used as a tool for authenticating users to validate the card owner. Financial trickery is a very predominant problem for Banks and present secure information in the ATM card magnetic tape are very exposed to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be authenticated as the card owner. Face Based ATM login undertaking the ATMs which are provide with Face recognition technology can perceive the human face during a transaction. When there are "Shoulder Surfers" who try to peek over the cardholder's shoulder to acquire his PIN when the cardholder enters it, the ATMs will spontaneous remind the cardholder to be careful. If the user wears a mask or sunglasses, the ATM will refuse to serve him until the covers are take out.

Secure - Since your face is your password, there is no need to panic for your password being unremembered or stolen. In addition, the face recognition engine locks entrance to the account and transaction pages for the card holder as the card holder walk away from the camera of the ATM and one more face appears. Face based card holder authentication can be used as primary or as a secondary authentication calculate along with ATM PIN. Face based authentication intercept ATM fraud by the use of fake card and take PIN or take card itself. Face verification is implant with security features to intercept fraud, as well as liveness -detection technology that detects and blocks the use of

photographs, videos or construct during the verification process.

Connect less - There is no require for recollect your passwords. Only looking at the ATM camera will login the card holder immediately. No physical connection is needed.

2. LITERATURE SURVEY

ATM is one of the impolite information systems in use and often ATM keypad appearance include the PIN of an ATM user. The PIN is a piece of privileged purchaser information which uses for the authentication of a transaction. The banking system handle mainly under the belief assumption that the PIN is secured and kept in private by twain the system and the customer to ensure the security demand of confidentiality. The author progress a fact-find design to show that it is practicable to infer the PIN using video footage during the affairs where both the keypad and fingertips are not visible to the striker. A lab study was manage to infer the PIN by human discern. Further, an Open CV Python program was used to automate the PIN speculation. PIN is one factor of the two-factor authentication system second-hand in ATM transactions. Banks charge heavily to ensure that a PIN is prefer about inside an HSM and revealed only to the customer. This desirable that banks control under the arrogance that the PIN is known only to the customer. However, observation cameras installed inside ATM cell to improve physical security open up a side-channel that can practically reveal the PIN to third parties. Nowadays, protectorate on banking in the virtual world has been grow to the peak position. To make it compatible advanced technologies should be second-hand. As OTP is nowadays used worldwide for security purposes, it can be countermand by QR code. A QR code scanner is required to detect code and decrypt information in keep in QR code. Scanner need to be installed in the ATM machine to take input capability from the user. We will supply extra feature to an existing system, so conventional withdrawing option is also there. On other end, ATM machine will scan the QR code cause by 'Get Note'- android application and decrypt it with the key stored in the database. After decryption ATM will get be in need of credentials such as card number, amount, pin, CVV number on card etc. It will authenticate all the particular with the banks database. After successful authentication, cash will be distribute by the ATM machine. ATM machine will responsible for validating the QR code such as dissimilarity in generation time and scanning time is not more than five minutes. ATM will able to detect QR code from image uniquely, identical QR code will be rejected. System will detect QR code generated by Get Note (android application) only. In the ongoing system, user needs to visit the at hand ATM, swipe the card in the ATM machine there to pull out of money. This physical connection of card and machine makes it effortless for the fraudsters to capture the data and embezzle it. The proposed infusion eliminates this physical contact. The mobile app be made up of a special code which flashes on the screen for a period of 1 minute. This code prepare strong authentication by dynamically give rise to 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 squad such as user-id and password. After this the user generates a testimonial number as per his alternative and also specifies the amount to be withdrawn. This testimonial number would remain valid for an explicit period of time and can be used only once. Having generated the reference number, the user come upon the nearest ATM and throw oneself into the user-id and password along with the code in the app to sign in. If the authorized user is instant, he/she would be logged in and would be essential to enter the reference number to withdraw the specified amount. If the reference number is exact, the amount is withdrawn else transaction stop. This idea is a combination of current ATM system and online transactions assume OTP. By terminate the use of OTP, the problems related to sharing of OTP are successfully get the better. This system donate a three-level security, first when user's identity is corroborate while logging in the system, second through user-id, password and the code present-day in the mobile app – when entered in the ATM machine and last via the testimonial number.

ATM security system architecture that amalgamate both the finger print and GSM technology inside the existing PIN-based authentication operation: PIN verification is integrate with fingerprint recognition, to recognize a customer through ATM transaction. Fingerprint is corroborate using well organized particulars attribute extraction algorithm. To reassure the security while achieve transaction through strike machine, the client will authenticate the transaction by an acceptance message through GSM technology. In both cases, location will be analogous through GPS. If any illegitimate person make an effort to use the card it will automatically be obstruct by the system and particular information will be sent to the customer through the message.

QR cash withdrawals were authorize so customers could ditch their ATM cards and directly scan a QR-code on ATMs using the QR app to withdraw cash: A QR code scanner is be in require of to detect code and decrypt information in keep in QR code. Scanner require to be installed in the ATM machine to take input capability from the user. We will provide additional feature to an existing system, so traditional withdrawing possibility is also there. On other end, ATM machine will scan the QR code bring about by 'Get Note'- android application and decrypt it with the key set aside in the database. It will authenticate all the details with the banks

database. After fortunate authentication, cash will be dispensed by the ATM machine.

The algorithm pre-owned in the existing system for biometric authentication are Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs): Biometrics calculate the distinctive physical characteristics of an independent as a means to recognize or authenticate their identity. Ordinary physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Biometrics may be used for identity establishment. A new quantification that purports to belong to a particular entity is set side by side against the data set aside about that entity. If the measurements match, the declaration that the person is whom they say they are is regarded as being authenticated. The algorithms were instructed and tested using a well-known biometric database that contains a representative of face and speech and similarity scores of five face and three speech biometric experts.

The existing ATM authentication method is the use of password-PINs and OTP: Currently, ATM systems utilize no more than an access card which generally has a magnetic stripe (magnetic stripe) and a fixed Personal Identification Number (PIN) for identification verification. Some other cases make use of a chip and a PIN which sometimes has a mag stripe in case the chip fails as assistance for identification purposes.

3. PROPOSED SYSTEM

The design is to put forward an automatic teller machine a few modal security model that would mingle of a physical access card and electronic facial recognition utilizing Deep Convolutional Neural Network.

Facial Biometric Authentication System using Deep Learning Techniques: Deep learning is a department of machine learning, which, in turn, is a subdivision of artificial intelligence (AI). When it comes to face recognition, deep learning authorize us to attain greater accuracy than traditional machine learning methods. Deep FR system in the company of face detector and adjustment. First, a face detector is used to cramped faces. Second, the faces are line up to normalized canonical harmonize. Third, the FR module is carry out. In FR module, face anti-spoofing appreciate Whether the face is live or spoofed; face clarifying is used to handle variations before instruction and testing, e.g., poses, ages; Different architectures and loss motivation are used to take out differentiate deep feature when training; face complement methods are used to do feature classification take the place of the deep features of testing data are bring out.

Verification Link Generator for Unknown Face: When the keep image and the get hold of prisoner image don't match, it measure that he is an unauthorized user. Face Verification Link will be conduct about and sent to user to substantiate the identity of unauthorized user through a few committed artificial intelligent agents, for faraway certification, which either authorizes the transaction congruously or signals a security-violation practicing to the banking security system.

Problem Description: Financial trickery is a very important problem for Banks and current certain information in the ATM card magnetic tape are very endangered to theft or loss. By using face recognition as a tool for authenticating users in ATMs can be established as the card owner. Face Based ATM login operation the ATMs which are provide with Face recognition technology can recognize the human face through a transaction. When there are “Shoulder Surfers" who try to peek over the cardholder’s shoulder to acquire his PIN when the cardholder enters it, the ATMs will automatically remind the cardholder to be careful.

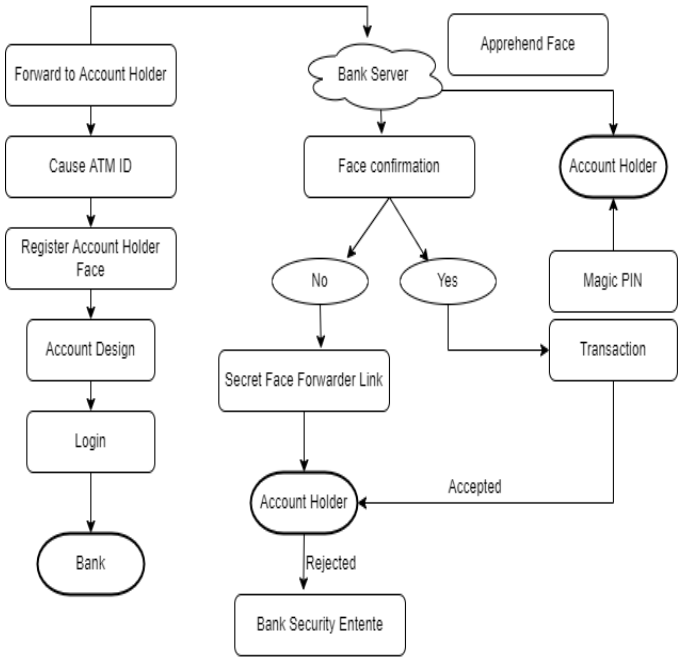

Fig 1: System Architecture

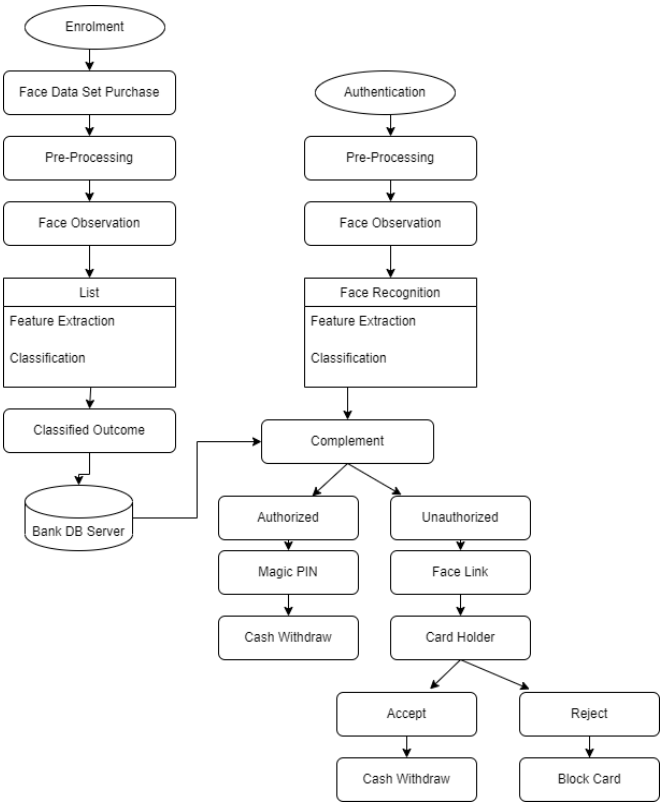

Fig 2: System Flow

With facial recognition, Bank can now warranty its customers the most punctilious security along with the satisfaction of open bank. The process used by the bank is to apprehend the facial images of their customers in the bank branch and then cache the images in a certain biometric database. When the customer cock their ID card or place their bank card at the ATM, Deep Face operate biometric software contribute by DL Model. In the event that none are consider to be suitable, the customer will be occasion to move closer, step back, separate their hat or sunglasses or whatever is needed to apprehend a suitable image. If the user have on a mask or sunglasses, the ATM will decline to serve him until protect are separate. The use of facial recognition authorize to deliver more advanced transactions at its ATMs for the reason that facial recognition supply an additional layer of security for both the cardholder and the bank. Bank customers can utilize their Debit/Credit card at the ATM to ingress their accounts, rather than being restricted to only those accounts connected with their ATM card. Robust Internet and GSM networks are require to enable multimedia messaging services (MMS) for acceptance and authorization processes. There are a great many anti-fraud measures built toward the system to add to its certainly. One such compute is the keep up of an infra-red lens to take prisoner additional facial details to put a stop to fraud attempts. The apprehend image is sent to the biometric clarifying system where it is differentiate to the customer's image set aside in the bank's ID database. Once corroborate, the customer can approach their accounts and bring about authorized transactions. It's not Verified, ATM Camera to take prisoner the user facial image. Internet-friendly mobile communication device, which is approachable on 24/7 bases, is be in need of for the bank account owner to control the remote certification. Dedicated intelligent agents for intelligent observe of take action on transactions and real-time feedbacks (alerts) to connected banking security.

Description of Modules: ATM Simulator- ATM Simulator is the following Generation testing implementation for XFS-based ATMs. ATM Simulator is a web technology to permits ATM testing with a virtualized variety of any ATM.ATM Simulator uses virtualization to supply realistic ATM simulation, combine with automation for faster, more well-organized testing for face authentication and unknown Face Forwarder approach.

Face Identification- After apprehending the face image from the ATM Camera, the image is specified to the face detection module. This module detects the image domain which is likely to be human. After the face detection make use of the Region Proposal Network (RPN), the face image is given as a capture to the feature extraction module to discover the key features that will be used for categorization. The module devises a very short feature vector that is well enough to constitute the face image. Here, it is done with DCNN with the help of a decoration classifier, the take-out features of the face image are set side by side with the ones kept in the face database.

The face image is then categorized as either known or unknown. If the image face is known, the corresponding Card Holder is associated and begins further.

Face Enrollment- This module starts by registering a few anterior faces of Bank Beneficiary templates. These templates then flatter the reference for evaluating and recording the templates for the other poses: tilting up/down, moving closer/further, and turn-off left/right.

Prediction- In this module, the complement process is done with trained classified consequence and test Live Camera Captured Classified file. Hamming interval is used to calculate the dissimilarity according to the result the prediction correctness will be displayed.

Unknown Face Forwarder Mechanism- Unknown Face Verification Link will be brought about and sent to the cardholder to verify the specification of the unauthorized user through some committed artificial intelligent negotiator, for faraway certification, which

either authorizes the transaction relevant or signals a security-violation aware to the banking security system.

Magic Pin Generator- This module utilizes a hybrid-image keyboard that tricks the eye when observe from a distance of hardly any feet or more. The particular technology amalgamates an image of a keyboard with a high spatial frequency and a contrasting image of a keyboard with a low dimensional frequency. The visibility of each image depends on the interval from which it is seen and results in a mirage that deceives the eye of a "shoulder surfer" so that the keyboard materializes to be usual when, in fact, it isn't. The keypads are been staggered to avoid further charge if the attacker can remember the situation of the keypads. The algorithm builds on human visual discernment and calculates the minimum interval between the attacker and the user.

Face Image segmentation using the region growing (RG) method: The region growing methodology and the latest related work of region growing are narrated here. RG is a simple image segmentation method found on the seeds of the region. It is also categorized as a pixel-based image segmentation method since it necessitates the selection of beginning seed points. This takes aside to segmentation inspect the neighboring pixels of beginning "seed points" and determines whether the pixel neighbors should be attached to the region or not based on definite conditions. In a standard region growing technique, the neighbor pixels are examined by using only the "intensity" constraint. A threshold level for potency value is set and those neighbor pixels that content this threshold is chosen for the region growing.

4. RESULTS AND DISCUSSIONS

To access the performance of our method, we collate our method opposed to the state-of-the-art methods in FDDB. The evaluation measure include: recall rate is used to judge the proportion of the identified face to the total face of the selected mark; false useful is the number of errors in the described face. These two indicators are communicate by the ROC (Receiver Operating Characteristic) curve.

5. CONCLUSION AND FUTURE SCOPE

Conclusion: It concludes that the standard ATM system required to be placed back with biometric systems where the transaction constructs become easier, well-founded, secure, and eliminate the be in need for carrying any style of hit cards. Face print is one of the multitude forms of biometrics used to identify individuals and confirm their identity. It is found in the characteristics of the user's fingerprint, like stability, dependability, Etc. Face-print allows the recognition of an indicated person through quantifiable physiological characteristics that confirm the identity of an individual.

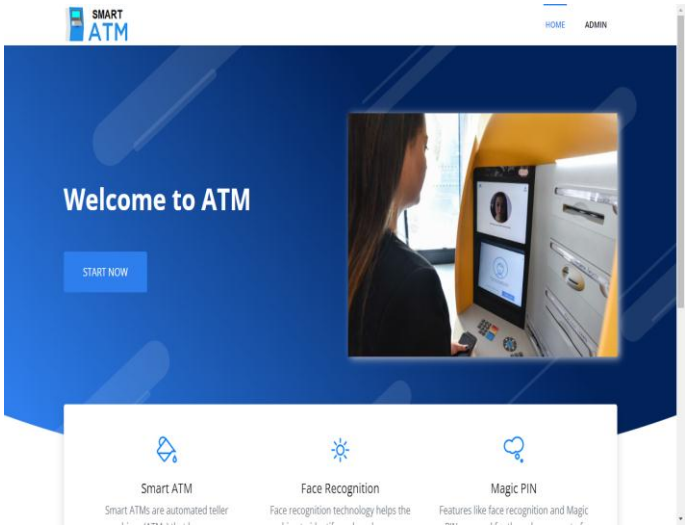

Fig 3: Home Page of the Project

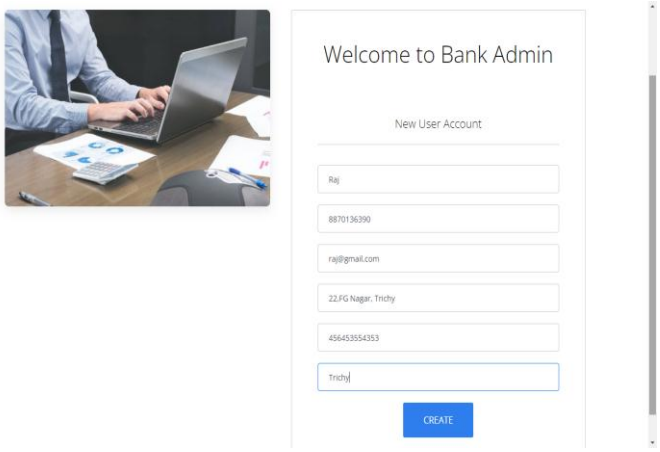

Fig 4: Bank Admin Page

It can get the better of the issue of impersonation of a cardholder. This is like a two-factor authentication method that is used to authenticate that the transaction is done by the card owner or the person believed in by the owner utilizing face recognition. It ceiling the card operation of the unauthorized user who holds the password of someone's card. Thus, this ATM model supplies security as opposed to the exploitation of associates by using a verification system that operates face recognition to the identity and confirms the user and it will scale back involuntary transactions to an excellent.

Future Work: In the future, this the make conversation with face recognition technique appears more challenging in a contrast to other biometrics, thus well-organized algorithm can be grown. The flaws in face recognition technology like the incapacity to detect a face

when beard, aging, glasses, and caps can be put to right and eliminated or lessen. If the cost of retina or iris recognition reduces, it can be used alternatively for face recognition.

REFERENCES

[1] A. Had, S. Benouar, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, "Full impedance cardiography quantification implement utilize raspberry PI3 and system-on-chip biomedical instrumentation solutions," IEEE J. Biomed. Health Informatics, vol. 22, no. 6, pp. 1883-1894, Nov. 2018.

[2] A. Wazwaz, A. O. Herbawi, M. J. Teeti, and S. Y. Hmeed, "Raspberry Pi and computers-found face observation and recognition system," in Proc. 4th Int. Conf. Compute. Technology. Appl. (ICCTA), May 2018, pp. 171-174.