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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

Face PIN: Biometric Authentication System For ATM Using Deep Learning

K. PRIYANKA, N. LAKSHMI, G. MAMTHA, V. SINDHU

[1]Assistant professor Department of Computer Science And Engineering,

Sri Bharathi Engineering College For Women, Pudukkottai.

[2,3,4]Department of Computer Science And Engineering, Sri Bharathi Engineering College For Women, Pudukkottai.

Abstract: Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. There is an urgent need for improving security in banking region. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM system today use no more than an access card and PIN for identity verification. 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. This project proposes and automatic teller machines security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts. 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. 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.

Keywords: This project proposes and automatic teller machines security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network.

I. INTRODUCTION

Automated Teller Machines, popularly referred to as ATMs, are one of the most useful advancements in the banking sector. [1] 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 are some transactions that need no debit or credit card [2].

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., accounting [3].

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. Some of these labels are listed below-Green Label ATMs- Used for agricultural purposes Green Label ATMs- Used for agricultural purposes Orange Label ATMs- Used for share transactions.Pink Label ATMs- Specifically for females to help avoid the long queues and waiting time [4].

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)Automated Teller Machines provide 24×7 access anywhere [5]. 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. The notion that something could go wrong never crosses their minds.

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.

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. 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[5].

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

II. LITERATURE REVIEW

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 Open CV 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 [6]A 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.

[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, cashwill 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)[8] 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 finger print 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 finger print 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) chipcards 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 [9]. 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

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

frauds [10]. 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 during authentication.[11] 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.

III. MATERIALS AND METHODS

ATM Simulator is a Next Generation testing application for XFS-based ATMs (also known as Advanced Function or Open-Architecture ATMs). ATM Simulator is a web technology to allow ATM testing with a virtualized version of any ATM.ATM Simulator uses virtualization to provide with realistic ATM simulation, coupled with automation for faster, more efficient testing for face authentication and unknown Face Forwarder Technique[12].

High-Level Model of the Proposed System

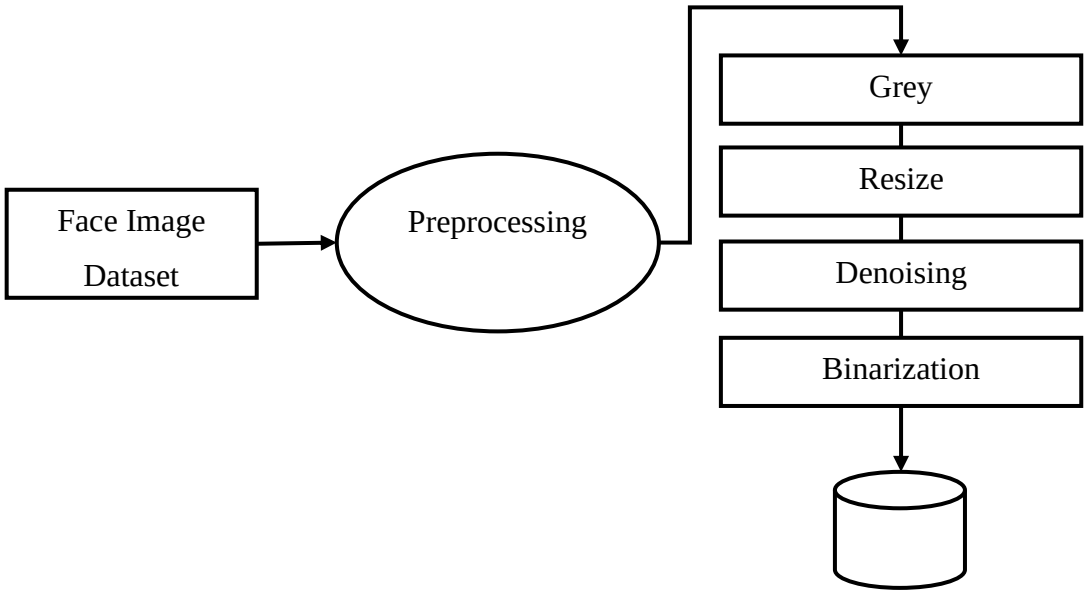

Figure 1: Preprocessing

IV. METHODOLOGY

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windowson the feature map through anchors with different scales and different aspect ratios.Face detection and segmentation method based on improved RPN. RPN is used to generate RoIs, and RoIAlign faithfully preserves the exact spatial locations.These are responsible for providing a predefined set of bounding boxes of different sizes and ratios that are going to be used for reference when first predicting object locations for the RPN.

A. Specification and Justification for the Selected Methodology

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

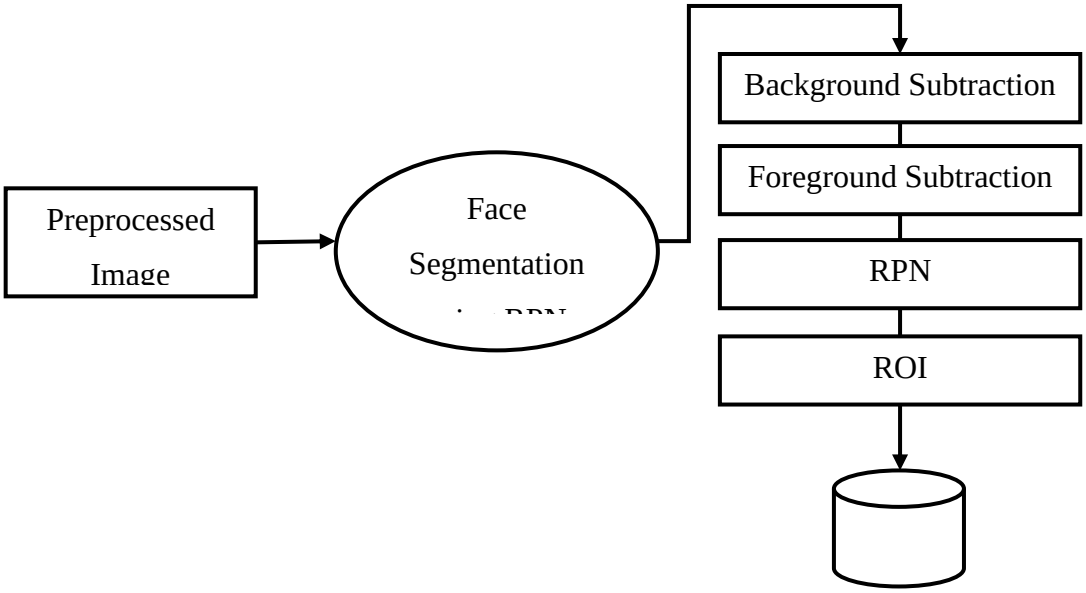

Figure 2: Face Detections

Business Understanding: In this phase of this research work, we understand the merits of intelligent systems to automate the process of procuring cryptocurrency using influencer's tweets. Figure 3 depicts an overview of CRISP-DM tasks and their outputs.

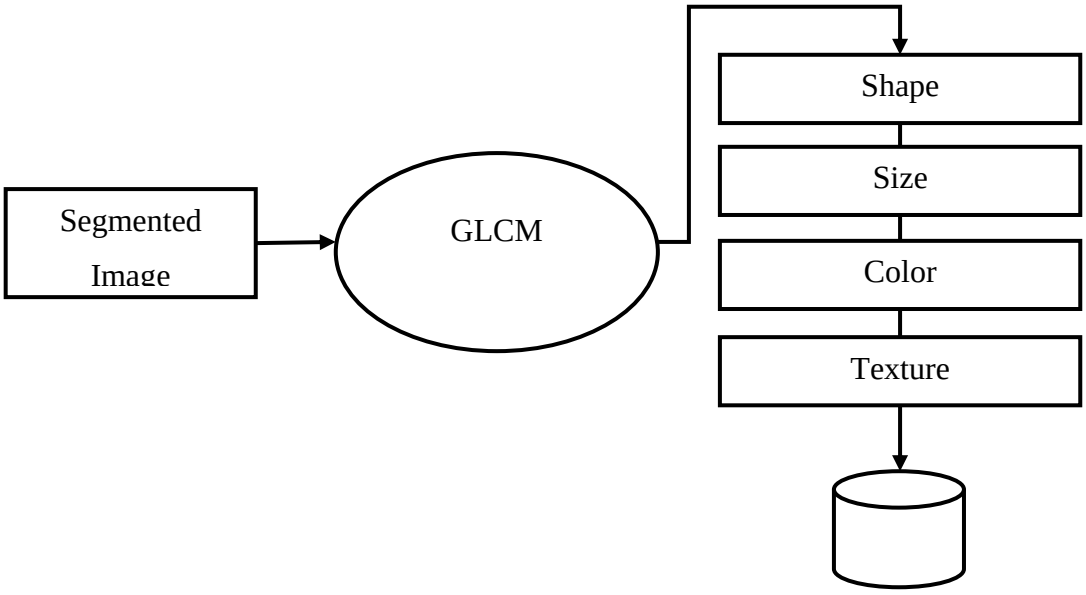

Figure 3: Feature Extraction

Prediction

In this module the matching process is done with trained classified result and test Live Camera Captured Classified file. Hamming Distance is used to calculate the difference according to the result the prediction accuracy will be displayed.

Unknow Face Forwarder

Unknown Face Verification Link will be generated and sent to card holder 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.

Modeling: In this section, you have to enter your withdrawal amount and press enter.
But make sure your withdrawal amount does not exceed your balance in the account otherwise transaction will fail.

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

Evaluation: The important points involved with the performance metrics are discussed based on the context of this project**.**

Deployment: It is also known as balanced F-score or F-measure. F1 score is a measure of accuracy of a model combining precision and recall. In the context of this thesis, a good F1 score shows that there are less false positives and false negatives. This shows that the model is correctly identifying Face in ATM environment.

C. Implementation

I]. Input design:

This Deep learning is a machine learning technique used to build artificial intelligence (AI) systems.Deep convolutional neural networks are mainly focused on applications like object detection, image classification, recommendation systems, and are also sometimes used for natural language processing. Deep Convolutional Neural Networks (DCNN) is a Deep Learning (DL) Method which is different from normal Convolutional Neural Network (CNN) in terms of number of hidden layers usually more than 5 which are used to extract more features and increase the accuracy of the prediction.

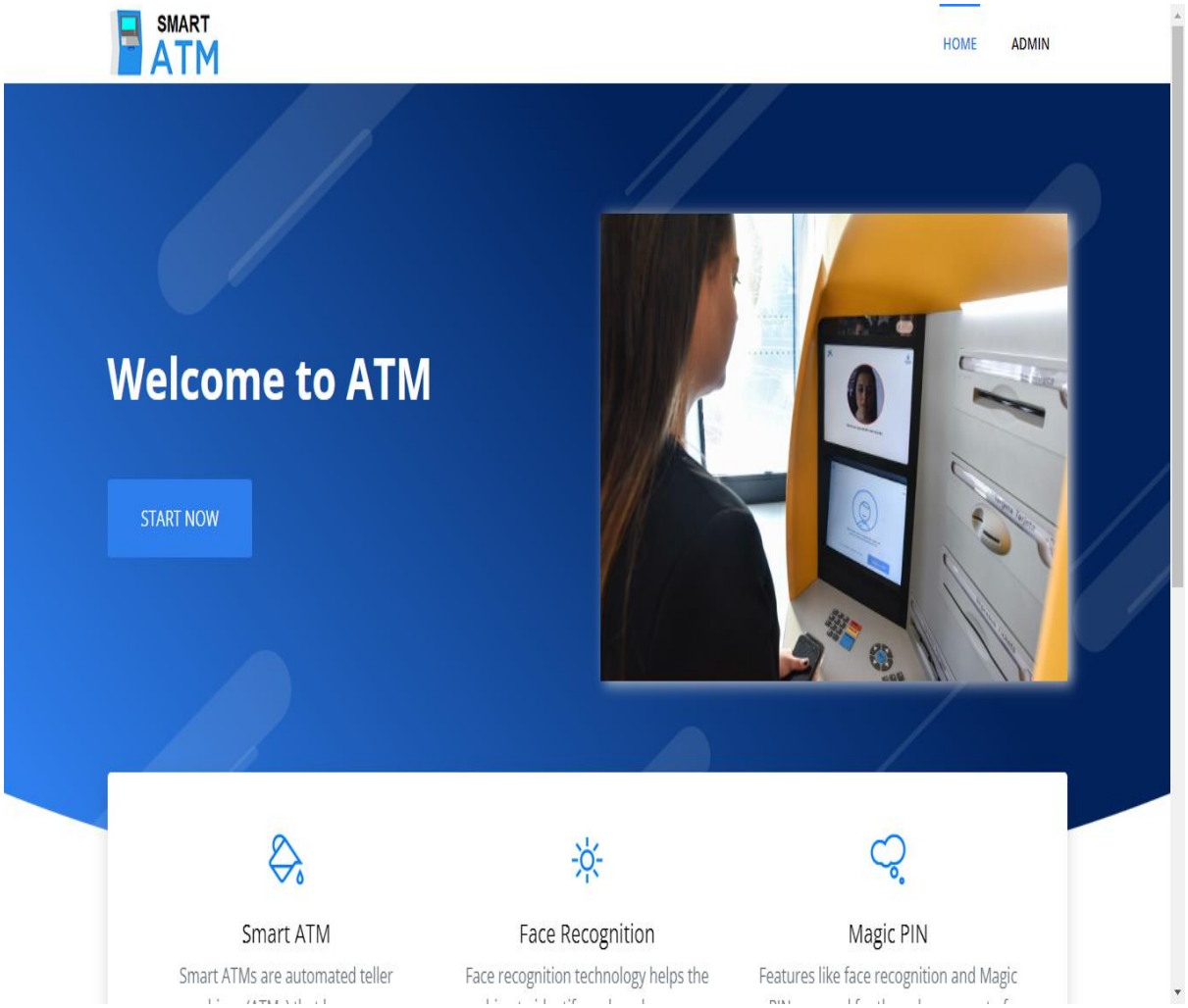

Figure 4: ATM Home page

Figure 5 is a snippet of python code to generate tweets in real time. . Deep convolutional neural networks receive images as an input and use them to train a classifier. The network employs a special mathematical operation called a "convolution" instead of matrix multiplication.

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

```
Testing Phase

from flask import Flask

from flask import Flask, render_template, Response, redirect, request, session, abort, url_for

from camera import VideoCamera

@app.route('/verify_face2',methods=['POST','GET'])

def verify_face2():

msg=""

ss=""

uname=""

  act=""

ifrequest.method=='GET':

act = request.args.get('act')


  #if 'username' in session:

  #   uname = session['username']
```

Figure 5: Input to ATM Home Page

II]. Output:

Face based card holder authentication can be used as primary or as a secondary authentication measure along with ATM PIN. Face based authentication prevents ATM fraud by the use of fake card and stolen PIN or stolen card itself. Face verification is embedded with security features to prevent fraud, including liveness-detection technology that detects and blocks the use of photographs, videos or masks during the verification process.

```
* Serving Flask app 'main' (lazy loading)
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: on
* Running on all addresses (0.0.0.0)
  WARNING: This is a development server. Do not use it in a production deployment.
* Running on http://127.0.0.1:5000
* Running on http://192.169.169.185:5000 (Press CTRL+C to quit)
* Restarting with stat
* Debugger is active!
* Debugger PIN: 120-925-195
```

Figure 6: Output ATM Home page

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

V. RESULTS

A. Pseudo Code/Sequence

Testing Phase

```
from flask import Flask
from flask import Flask, render_template, Response, redirect, request, session, abort, url_for
from camera import VideoCamera
@app.route('/verify_face2',methods=['POST','GET'])
def verify_face2():
msg=""
ss=""
uname=""
   act=""
ifrequest.method=='GET':
act = request.args.get('act')

   #if 'username' in session:
   #    uname = session['username']
   ff2=open("un.txt","r")
uname=ff2.read()
ff2.close()

cursor = mydb.cursor()
cursor.execute('SELECT * FROM register WHERE card = %s', (uname, ))
account = cursor.fetchone()
name=account[1]
mobile=account[3]
print(mobile)
email=account[4]
vid=account[0]
```

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

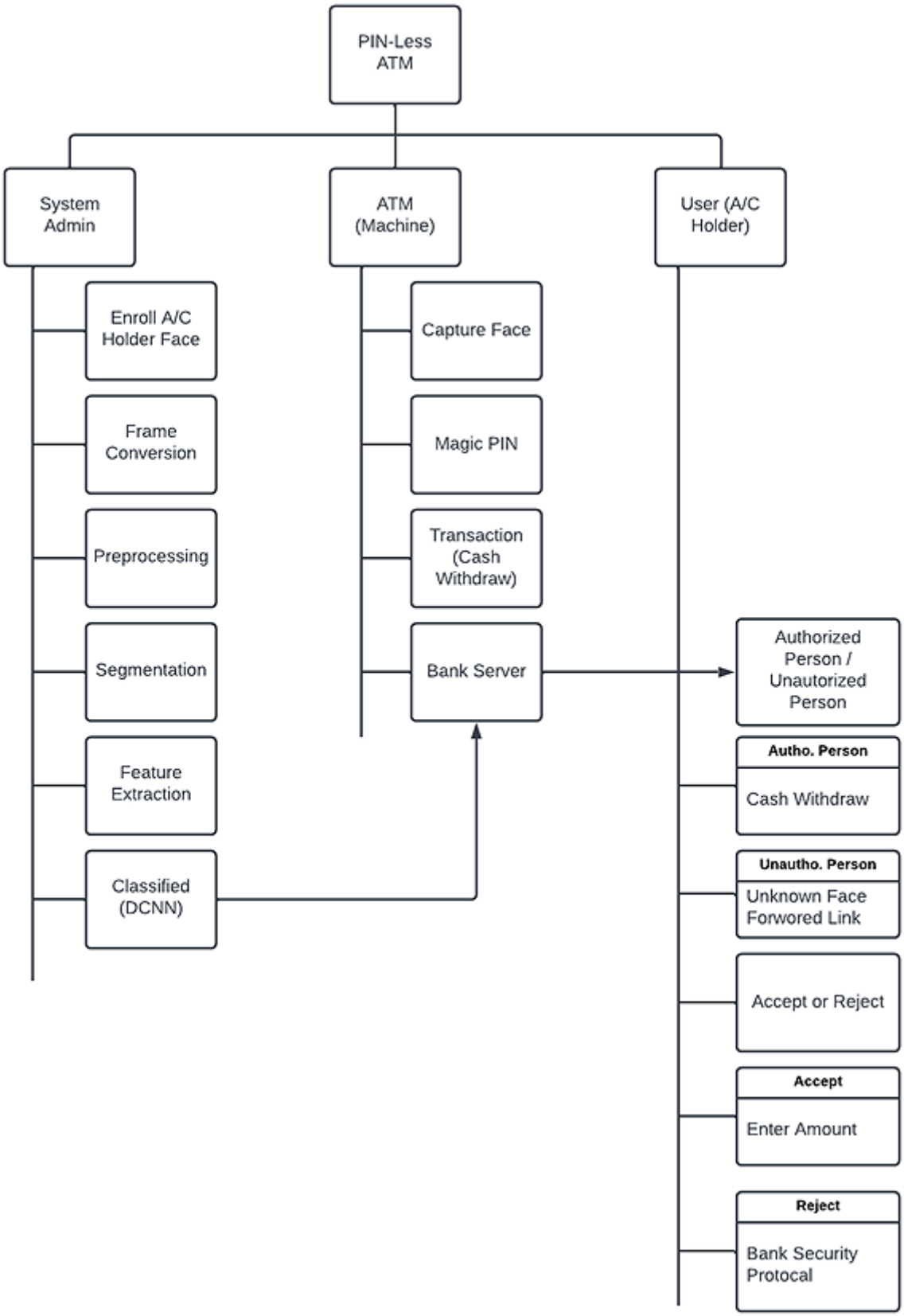

Figure 7: Flow Chart

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 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115140

Data Understanding: Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

B. Development Process for the Procurement System

The development process of Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain.

VI 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 basedon deep residualnetwork," 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 usingautomated face recognition: Based on the PCA & LDA algorithms," inProc. 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 basedon 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, ``RaspberryPi 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 raspberryPI3 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-poseface 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 withsubject 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 surgicallyaltered face images using multiobjective evolutionary algorithm," IEEETrans. Inf. Forensics Security, vol. 8, no. 1, pp. 89-100, Jan. 2013.
[10] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring systemusing RFID and IOT Proc.Conf.Eng.Technol. (IC-GET), Nov. 2016, pp. 1-4