International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

Automated POS System based on Face Recognition and Password

Arnab Dey[1], Sudhanshu Jain[2]

[1]*Dept. of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, Kolkata, India*
[2]*Dept. of Master of Computer Applications, Chitkara Institute of Engineering and Technology, Punjab, India*

Abstract - *Point of Sale systems have seen growth from the time it was first implemented. It is a system that includes both hardware and software. As of today, we can see credit card, debit card enabled POS apart from traditional cash POS with manual entry. POS have evolved with Bar code readers. But now with new age technology we suggest 'AI subset based POS' which is a new method. You will find POS with face recognition and Credit card swipe system at some places. We in this paper propose face recognition along with password as a method of payment making it cards free as well.*

Key Words: **POS, Automated POS, AI subset based POS, Cashless, Card less, Face Recognition POS, New Method to POS**

1. INTRODUCTION

Today, there are many methods of payment solution at point of sale. Some include credit card, cash, debit card etc. Here in this paper we suggest 'A New Method to POS (AI subset based POS)'. We call it Artificial Intelligence (AI) subset based POS as Face Recognition alone is not entirely Artificial Intelligence. AI system in entirety would be something that can pass Alan Turing test. The test stated by Alan Turing in the year 1950 was "when a machine has ability to have intelligent behavior equivalent to or indistinguishable from, that of a human then we can call it AI". Before we proceed to integrities of method, let's see the security problem definition as well. The security problem definition consists of three subsections organizational security policies, threats and assumptions. We also found face recognition is available in unconstrained environment to hackers as well.

The reason to explore this new method of POS is that theft and usage of debit and credit cards are on rise that makes me look into solution that is secure and convenient method of making payment at Point of Sale or Over the Counter. Of total frauds 20% account to credit card frauds, we look forward to bringing that percentage to nil as issuing of credit card would not be required instead just having credit card account with password and face recognition authentication system along with regular transaction amount processing will suffice the system. Even if miscreants bypass face authentication we can say system is secure through password entry by purchaser.

The method that we propose here can be effective by adding two authentication layers that is password in addition to face recognition. It neither uses cash, mobile nor cards.

2. LITERATURE SURVEY

AMSR is a small hardware dongle that reads magnetic stripes on payment cards, encrypts the sensitive card data, and transmits the outcome to the application. The main technical outcome show how an arbitrary application running on the phone can permanently disable the AMSR, extract the cryptographic keys it uses to protect cardholder data, or gain the privileged access needed to upload new firmware to it. The move to use mobile phones as a platform for hosting special-purpose embedded devices will arise in other settings, and there may be overarching security engineering principles that will apply equally well to POS systems and beyond. It can be stated that Smartphone as POS has issues too [1].

Point of Sale system basically fetches the data of the sale instantly at the moment and location of purchase. It gives a primary interface for the credit card transaction to take place. At present, there is no Point of Sale System that provides total security, which makes POS systems hack prone. One of the ways to make the system more secure is to combine POS system with Cloud Computing (CC) that can be utilized as a reference for the evaluation of security. Cloud Computing gives a special construct known as the Protection Profile (PP). Previously, the police identified an international hacker gang which hacked various POS systems for a credit card, which are widely used in various places such as petrol pumps, restaurants, and revealed customers credit card information abroad and thus were spread across 49 different countries and were utilized to make duplicate cards with using that hacked information.

It is also seen that the card information gets stored in POS systems that makes hackers to easily get the card data by hacking the system. The outlook of data leak is simply the direct drain of database having credit card information which is now modified with real- time leakage just by an email at the point of the payment. On making a Protection Profile (PP) for Point of Sales system is just restricted to a POS terminal, which is just a part of the whole POS system. This system will reduce the crime rates occurring in large scale. [2]

Stealing information and data has become common practice among miscreants. After stealing data it is sold at underground marketplaces. There are many ways proposed to prevent it from basic firewall settings to card and password combination.

The best way to say is "more secure" using new technology. This again does not imply that system is 100% secured. Some of improvisations are: Two factor authentication method along with restricted access to system. White listing and monitoring of application is also in support to prevent such data leak and theft is proposed. [3]

There are many ways to implement Biometric Recognition with many advantages and disadvantages. Some of Biometric Recognition technique is to use Eyes, Face, finger prints, voice etc.

Long password are a ways to make it difficult for hackers to hack but then remembering it and typing long password is tough for users itself as well. Biometric recognition with certain technique has false alarm as result. There is limitation that it has, that is, it cannot to be used effectively in government service. [4]

Texture analysis is another technique proposed in this paper as a way of Face Recognition. It is learnt that this method less expensive and has an accuracy rate of 96.75%. It has to be noted there is still mismatch possibility. Certain figures from tests show that match is not found at times and there is also a chance of mismatch in this approach but it helps in achieving better accuracy. [5]

Facial Recognition Cash register such as TPS650 is face authentication in the self payment service, access control, hotel check-in etc. It has pay with your face and method of high precision. It is said to be secure enough to encompass 3D masks or printed photos that can lead to stealing of data and bypass security as authentication. The system has robust method and technology to use Face authentication. It also has numeric keypad touch screen interface to enter amount. [6]

3. SYSTEM MODEL

The system model of our research can be illustrated as we see in the Fig-1, with the following systems and POS terminal as mentioned below:

System 1: It is a system that can work independently to give faces trained model as output. So, images and training algorithm can be on different system.

System 2: It would have trained model to authenticate face. Once Face Authentication happens then password entry is authenticated with database such that transaction can proceed.

POS terminal: It would have amount numeric value, face and password as input. Pass it on to system 2 and show result as Success of Fail on screen.

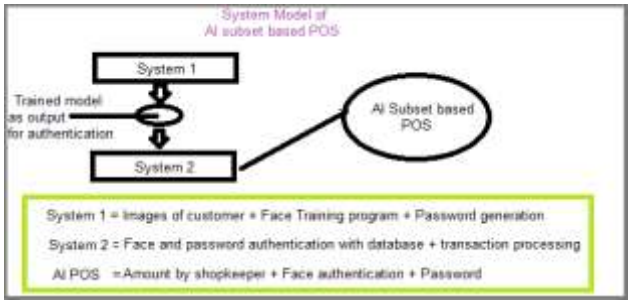

Fig-1: AI based POS System

4. PROBLEM STATEMENT:

What if person sitting in other location takes photo from Facebook tries to hack system? If we restrict upto 3 invalid passwords entries before blocking of account of that person. Then, hackers might block the account due to his invalid guesses. Hacker in this scenario will be able to block anyone's account. The problem is derived from real report on an online news website. [11]

4.1 Problem analysis and comparison to existing system:

Yes this is possible just like accounts get locked when hackers make invalid password attempts in net banking. We propose to restrict password entry to 3 times and conclude to say that system proposed do not do anything better to existing system in this aspect particularly. The blocked account can be opened by real user of the account only.

5. PROCEDURE:

To match face recognition one will have to match it with credit card account of the bank, once link is established then password is only thing required to be entered in to the system. Credit Card organization must have few pictures of account holder to train the Sub AI to recognize that person face. Credit card holder images can be taken once at time of issuance or as part of application process. Password can be sent to users of credit card account holder through existing system of issuance of password.

5.1. Steps to be performed at 'Sub AI based POS' are as follow:

1. Amount to be entered by shopkeeper.

2. Customer needs to be in front of camera and enter password.

3. Success message would be shown on approval.

5.2. FaceNet:

At the time of giving a set of images of same person, FaceNet basically makes a model which is known as facenet model then finds the embeddings and then finds the Euclidean distance between two images. Embeddings are nothing but feature vectors. Invented harmonic embeddings, and a harmonic triplet loss is used followed by matching of two embeddings.

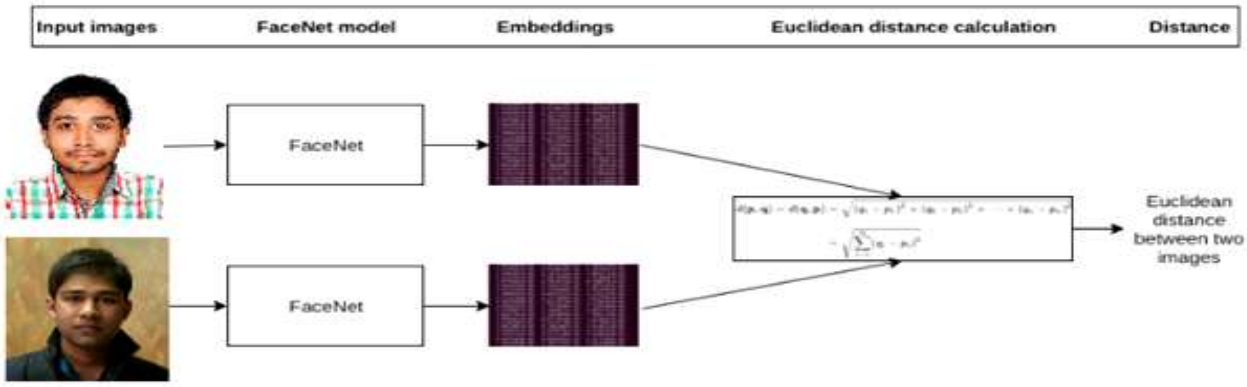

Fig-2: FaceNet Model Illustration

Matching or non matching embeddings give the resulting output.

FaceNet is Google's work on Face Recognition and clustering that has accuracy of 99.63%. It serves the purpose of doing Face Authentication with high precision that is required by this proposed paper. FaceNet uses deep neural network architecture**.** It acquires a mapping from a Euclidean space to a face image in which the distances match directly to a estimate of the similarity of the face. As soon as the space is being created, various tasks can be achieved easily viz. Face verification, recognition and clustering using standard methods with FaceNet embeddings as the feature vectors. For training the system, triplets are used. Triplets are a gathering of one anchor image, one anchor image to non-matching image and one anchor image to matching image. The triplet loss also reduces the distance between a positive and anchor, both of which have the same identity, but expands the distance between a negative and the anchor of a different identity.

A large amount of pre-trained FaceNet models are available that are trained on various deep learning frameworks. Let's see the steps for our pre- trained model:

1. Capture or gather at least 4 pictures of all customers to train system one step ahead.

2. Align the faces utilizing Multi-task Cascaded Convolution Neural Networks (MTCNN), OpenCV or dlib. These methods identify, detect and align the faces by making eyes and bottom lip appear in the same location on each image.

3. Use the pre-trained FaceNet model for representing or embedding the faces of all employees on a 128-dimensional unit hyper sphere.

4. Store the embeddings with respective customer names on disc.

The architecture of FaceNet model is showed in Fig-3.

Fig-3: FaceNet Architecture

Now, it is time to look on how to recognize faces keeping note of above mentioned knowledge. Once Embeddings are available, we are ready to do face match with real time images.

Comparing 128 dimensional embeddings using Euclidean distance measure would give results such that lowest distance is found to be less than value of threshold then person is recognized by the system to lowest distance embedding corresponding to it.

6. SIMULATION ANALYSIS, RESULT AND DISCUSSION

6.1. Algorithm:

Here we have showed both the algorithms one with FaceNet and other one is OpenCV for face recognition part in the POS system.

But later, we will see FaceNet gives better accuracy and optimal outcome.

6.1. A. FaceNet Algorithm:

Step 0: Start

Step 1: Import FaceNet

Step 2: Initialize variable to video capture variable, face detection and recognition

Step 3: Identify, crop and align face (training)

Step 4: Generate embeddings and store it

Step 5: Capture images as frames through camera

Step 6: Convert frames images into embeddings.

Step 7: Compare embeddings.

Step 8: Redirect to payment gateway that accepts Password to make transaction.

Step 9: On receiving "success" from payment gateway close transaction

Step 10: Show "Success" on screen.

Step 11: Stop

6.1. B. OpenCV Algorithm:

Step 1: Start

Step 2: Enter amount that is to be accepted in system.

Step 3: Press 'Activate' to instantiate Face Recognition + Password system.

Step 4: import numpy as np and then import cv2, import pickle # activated system.

Step 5: Initialize

face_cascade = cv2.CascadeClassifier('cascades/data/haarcascade_frontalface_alt2.xml')

#specifies part of face to be recognized. In case of frontal face

recognizer = cv2.face.LBPHFaceRecognizer_create()

recognizer.read("./recognizers/face-trainner.yml")

#read from existing trained binary.

labels = pickels

database of people names.

#camera is to be initialized

Step 6: Read input from camera using cap variable into frame through frame by frame when true.

Step 7: Convert input image into gray scale image so that there is common ground to match faces in image.

Step 8: Then utilize predict() method available in cv2. Pass gray converted input as parameter to predict. Predict is to be used with object recognizer that has trainer binaries.

Step 9: Capture result into conf variable. # conf means confidence of match

Step 10: If conf>45 or 75 then

Redirect to payment gateway that accepts Password to make transaction.

Step 11: On receiving "success" from payment gateway close transaction

Step 12: show "Success" on screen.

6.2. Result:

The simulated result of POS face recognition system after running it in our Windows 10 system is shown in Illustration-1.

Illustration-1: Output of Face recognition system of POS

When compared with other methods of POS system with credit card, debit card, cash etc it is to be noted that Face Recognition (Sub AI) and Password method is more secure. It conforms to suggested solution of two factor authentication in other paper as well.

It is comparatively more convenient to society as no cards, mobile, cash is to be carried along to make transaction. It is secure as well from theft that is subjected with credit, debit, and cash stealing.

6.3. Analysis:

The pie chart as given in Chart 1 shows Credit card related frauds amounting to 20% of 100% fraud activities. With proposed method this 20% can be reduced as no credit card issuing would be required because transactions would be possible without it through proposed method.

It must be noted that Credit Card account would still be required but not issuance of it.

Fig-4: Stealing card

From the above Fig. 4, show that such acts is possible with existing POS that could lead to final transaction. But with Face Recognition (Sub AI) and Password at POS it is not likely to make final transaction unless revealed by user itself.

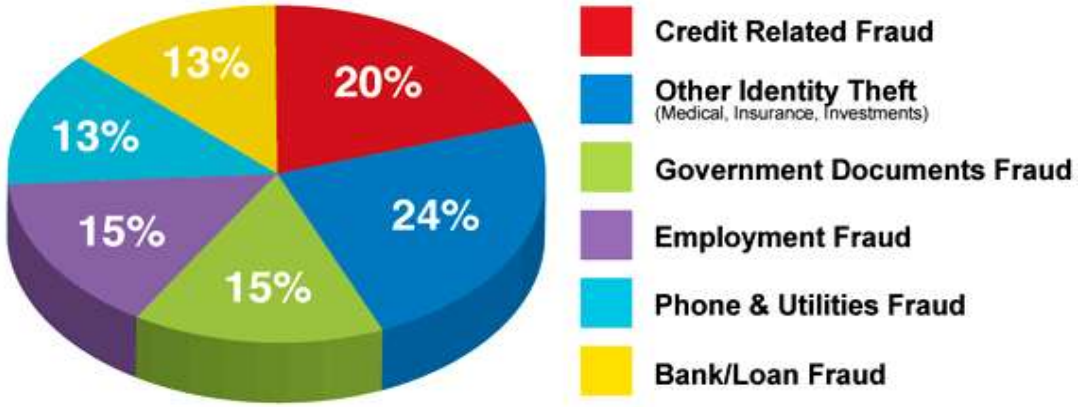

Chart-1: Pie chart showing credit card frauds

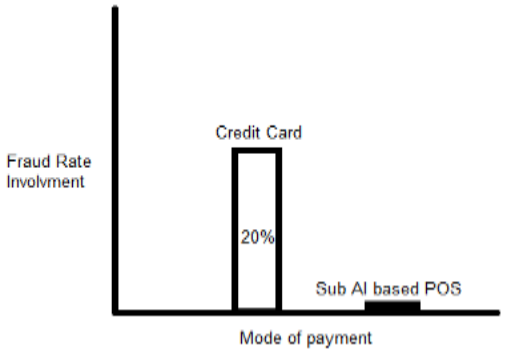

Fig-5: Bar chart analysis

The Bar Chart as we see from Fig-5, we assume that Sub AI POS would bring down to 1% of fraud activity linked to credit cards.

6.4. Graph:

Below stats are based on few people database. Input size of image may vary as not all pictures or camera would be of same resolution.

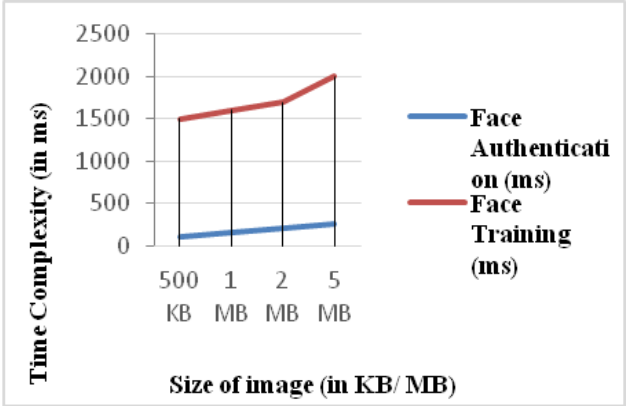

Chart-2: Graph showing Time Complexity

6.5. Time Complexity Analysis:

Above assumption based graph showed in Chart-2, shows that the time complexity of the algorithm we used for face authentication is almost linear in nature that is O (1) i.e. constant time, and the time complexity for face training is linear upto 2 MB sized images but if image size is larger than 2 MB the graph breaks linearity and becomes O (n).

It is an assumption based as time complexity could change based on system configuration and performance.

7. CONCLUSION

In this research paper, we have revealed that a New Method to POS (AI subset based POS) when implemented can at large bring down unwanted transactions that are without permit of the customer or client. From reduced transaction cost to convenience it is effective to society at large. Face recognition using OpenCV only gives 70% accuracy whereas Face Recognition using FaceNet provides 99.67% accuracy. It has to be noted that both OpenCV and FaceNet would bypass authentication even through photo. Thus, in our system we used FaceNet to achieve high accuracy and high security as well by means of adding password matching after face recognition. Even if miscreants bypass face authentication we can say system is secure through password entry by purchaser.

8. ACKNOWLEDGEMENT

We would like to acknowledge the department of Computer Science and Engineering and MCA of our respective colleges for giving their constant support and motivation.

9. REFERENCES

[1] WesLee Frisby, Benjamin Moench, Benjamin Recht, and Thomas Ristenpart, "Security Analysis of Smartphone Point-of-Sale Systems", Thesis of University of Wisconsin–Madison.

[2] Hyun-Jung Lee, Youngsook Lee, and Dongho Won, "Protection Profile for PoS (Point of Sale) System", Springer Publication, 2014, pp 495-500, DOI 10.1007/978-3-642-40675-1_74, Print ISBN 978-3-642-40674-4.

[3] Symantec Corporation, "Security Response- Attacks on point-of-sales systems", A Special Report, pp. 1-14, Version 2.0 – November 20, 2014.

[4] Anil K. Jain, Fellow IEEE, Arun Ross, Member IEEE, and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions On Circuits And Systems For Video Technology (IEEE CAS), IEEE Invited, VOL. 14, NO. 1, January 2004.

[5] J. V. Gorabal, Manjaiah D. H., "Texture Analysis for Face Recognition", International Journal of Graphics And Multimedia (IJGM), ISSN 0976 - 6448 (Print), Vol. 4, Issue 2, December 2013, pp. 20-30.

[6] Telepower Communication Corporation Ltd., "System with Cash Register through Face Recognition only", TPS650-FACE.

[7] Florian Schroff Google Inc., Dmitry Kalenichenko Google Inc., James Philbin Google Inc, "FaceNet: A Unified Embedding for Face Recognition and Clustering", Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, 12 Mar 2015.

[8] Lochan basyal, Bishal karki, Gaurav Adhikari, Jagdeep Singh, "Efficient human identification through Face Detection using RASPBERRY PI based on Python-OpenCV", Proceedings of WRFER International Conference, 24th June, 2018.

[9] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, Lior Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification", Thesis of Department of Computer Science, University of Toronto.

[10] Narayan T. Deshpande, Dr. S. Ravishankar, "Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN", Advances in Computational Sciences and Technology (ACST), ISSN 0973-6107, Volume 10, Number 5 (2017) pp. 1173-1189 , http://www.ripublication.com.

[11] Network18 Digital Organization, "Indian banks lost Rs 109.75 crore to theft and online fraud in FY18", Source-Money Control, Current Affairs, Report, Aug 25, 2018.

10. BIOGRAPHIES

Arnab Dey is a final year student of Bachelor of Technology (B.Tech.) in Computer Science and Engineering (CSE) from Maulana Abul Kalam Azad University of Technology, Kolkata. He was associated with the Entrepreneurship Cell of Indian Institute of Technology, Kanpur for one year. His current research interests include Image Processing, Algorithms, IoT, Machine Learning, Cloud Computing and Wireless Communication and Systems. He also prepares project for various companies.

Sudhanshu Jain has completed Master of Computer Applications (MCA) from Chitkara Institute of Engineering and Technology affiliated to Punjab Technical University (PTU) in 2010. His current interest is to research on innovative solution along with implementation. He has also worked at MNC companies like Infosys Technology Ltd. During training cum internship his team and he was awarded for 'Best Project Execution' at Mysore.