International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 01 | Jan - 2021 ISSN: 2582-3930

ENHANCEMENT OF ATM SECURITY USING DEEP LEARNING

Utkarsh Shukla
Dept. of Computer Science & Engineering SRM Institute of Science and Technology

Abstract

*A*TM transactions are found safe, reliable and inevitable these days for fulfilling our financial commitment. The traditional approach for using ATM mandates the involvement of ATM cards. However, people do experience times when either their account lacks balance amount or they forget to carry the card and thus they struggle to complete a transaction. This system is likely to be harmed by many security issues such as theft of ATM Card, Skimming, Lebanese Loop, etc. So in this paper, we'd like to propose a system that uses Facial Recognition Authentication along with an alphanumeric PIN that allows a user to access their account which is a more secure and reliable process than the existing system. Here we will be using the concept of transfer learning by implementing the OpenFace (Open-*source face recognition with deep neural networks) alongside the* Cascade Classifier which uses digital image features for recognition and Local Binary Pattern Histograms (LBPH) classifier is used for efficient texture operator which labels the pixels of image by thresholding the neighbourhood of each pixel.

Keywords

Facial Recognition, Alphanumeric PIN, Cascade Classifier, Deep Learning, ATM Transactions ***Introduction***

ATM is generally used for the withdrawal of money from a bank account without going to the Bank. Traditionally, ATM transactions are all card-based and security is handled by requiring the combination of a physical access card and a four-digit PIN to access a user's account. In the currently implemented ATM technology, there is always a chance of stealing someone's money. The money can be easily stolen if one gets access to the ATM card and security PIN. The ATM card can be stolen or simply misplaced by the user.

Our paper proposes an automated teller machine security model that would combine an alphanumeric PIN and electronic facial recognition. We'd like to propose this model as the FRAP Model. This is implemented by taking a live clip of the user at the ATM and asking the user to enter an alphanumeric PIN. Only when the alphanumeric PIN matches with the account and the live-captured image and the stored image of the user give a match, that the user will be considered fully verified. This system also has an alphanumeric PIN which will sort the problem for the user who has multiple accounts. Credit cards are generally issued by the institution or by an organization, in that case, a message notification will be sent to the account holder along with the captured image to authenticate the person to use the account.

Consider a situation that if an alphanumeric PIN matches and images fail to identify the person then the account holder has to authorize that person to use his/her account via their Mobilephone through a secured connection. The last consideration is that consumers may be wary of the privacy concerns raised by maintaining

images of customers in a bank database, so the data will be encrypted to avoid possible breaking attempts or the misuse of user images by the bank employees.

Materials and Methods

The proposed FRAP model includes an ATM that will be equipped with face recognition and alphanumeric PIN mechanism to enhance the level of security of the ATM transactions. Facial recognition is built using the concept of transfer learning by implementing the OpenFace (Open source face recognition with deep neural networks) alongside the Cascade Classifier which uses digital image features for recognition. A camera with the capability of thermal imaging is to be installed at the ATM which captures the image as the input when the user faces it and validates that image with the database available in the bank using the face recognition deep-learning technique and thermal face recognition to establish a successful bank account match. A unique alphanumeric PIN is assigned to each user containing the bank code as the first two characters and next to characters for the identification of different cards, which will help in determining the payment network and service facilities of the customer (gold, silver or platinum) and last four spaces will be a unique alphanumeric combination. The entered alphanumeric PIN leads to mapping with the account number and hence by which the account details of the user will be fetched. By the card type designated in the PIN, the database will get strained accordingly and will the user's database be fetched from the bank's server. Data of the user will be updated each time the user visits the ATM by adding their image to improve the recognition model. In case, if the ATM user is not the owner of the account then an alert message will be sent to the registered mobile device of the cardholder using a secure application. If the account holder grants access to the ATM user then only the user will have the authority to use an account for that instance of time. Once payment is done successfully then a notification will be will send to the account holder about the transaction as well as the captured image of the person who'll be present at the ATM for the transition. This will reduce the use of Physical ATM Cards, instead, a virtual card will be given to the user for online transactions.

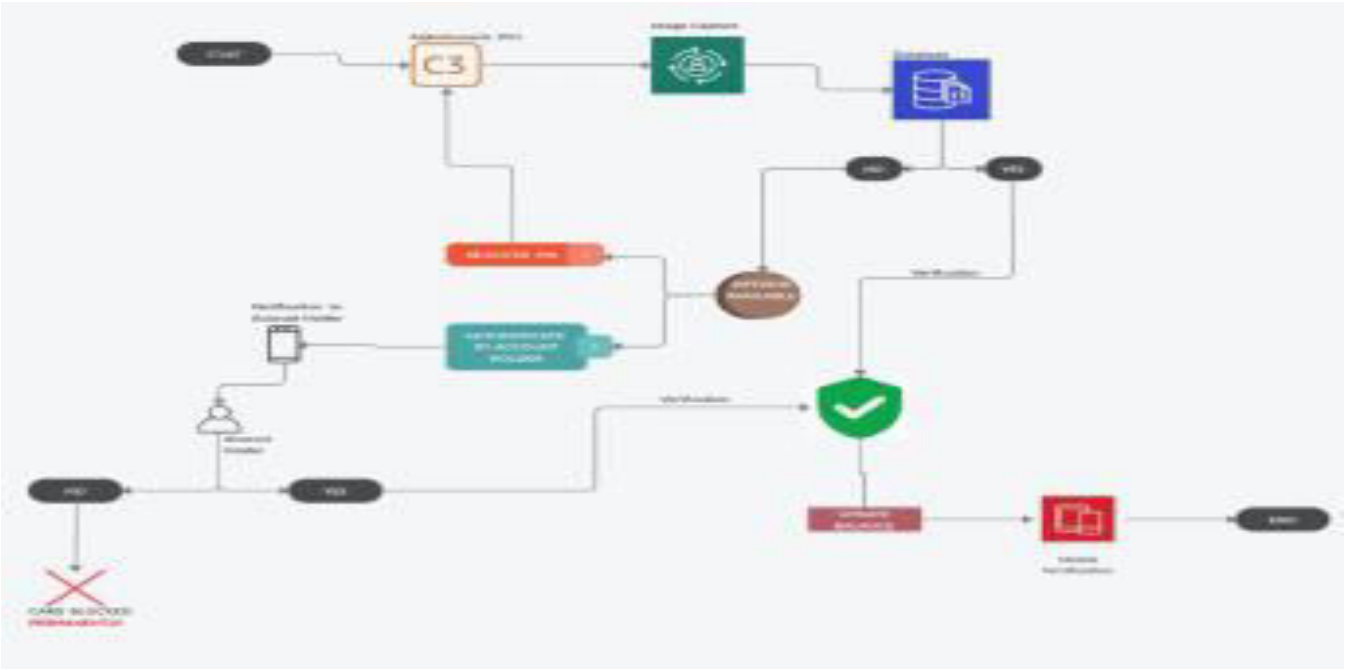

Fig 1. Workflow of the FRAP Model

Facial Recognition -

- Face Capturing Technology:

  Face Detection Technology will capture all the faces in the front of the camera, then all the captured images will be temporarily stored along with time and date stamp. These will then be passed to the Face Recognition Model.

- Face Match and Authentication:

  This will be implemented by combing the deep-learning Face recognition technology along with the thermal infrared face recognition for a secure match. This approach will follow the basic concept *of your face is your key*.

Results

The proposed model includes both Facial Recognition and an alphanumeric PIN system which paves a secure access path for the user and reduces the probability of forgery in any form.

Advantages of the FRAP Model:

1. The use of an Alphanumeric PIN will increase the security of ATM transactions. 2. Facial Recognition will provide card-less access to the account and also enhances the level of the security, hence prevents all the kind of forgery that can be incorporated through it.
3. It'll deliver a practical and workable solution that addresses the requirements of the regulatory authorities.
4. It'll fulfill social responsibility by reducing the rising levels of crime that are associated with cash-card transactions such as ATM Frauds.
5. It'll increase customer satisfaction

by eliminating the need to carry physical cards to ATM.

6. It'll also bring about a positive environmental change by reducing the need to manufacture physical cards.
7. Remote on Us (ROU) transactions will be possible by using this model. 8. The method can be implemented at a low installation cost.

Disadvantages of the FRAP Model:

1. Biometric Authentication will require a large storage medium to store the images for authentication.
2. Biometric Information such as facial features can change temporarily or permanently due to physical incident or sickness.
3. Image Recognition will require more

computing power than the traditional approach.

Discussion

A cardless ATM was proposed by the name of the A.M. Iyabode Model which uses biometric information and alphanumeric PIN to authenticate a user for transaction aiming for a cardless transaction. But this model fails if a customer of a particular bank wants to do a transaction using another bank's ATM which is been rectified in this proposed model by using a universal alphanumeric PIN containing the name of the bank as the first two characters. Hence, the authentication to the account can be done from any bank's ATM.

Iyabode model and a few other models haven't included the details for different electronic fund transfer brands, like VISA, MasterCard, American Express who offers different categories like Silver, Gold, and Platinum and hence their facilities are different for the recognition of the card type. In this proposed model, the alphanumeric PIN includes the next two characters of the PIN
as the card type like VI for VISA, MA for MasterCard which enables easy concurrence to facilities of the card for the cardholder.

The concept used also cut shorts the computation as by knowing card type the server rather for looking into the whole database of the bank the search is aimed only in the database of particular card type.

The biometric face authentication process is more secure as biometric information can't be altered forcefully.
In the proposed model facial recognition is also used for secure authentication of the user. The deep-learning algorithm is used for cross-validating the image captured before the transaction in the ATM with the database present in the bank. The database of the facial features of a particular user will keep on updating each time the person goes for a transaction to any ATM and thus keeps the user facial data up to date for a more reliable and faster authentication.

Conclusions

We thus developed a model that could replace the classical ATM approach with a more reliable, secure and easier process and will also eliminate the need for carrying an ATM card. The faceprint of an individual is a form of biometrics used to identify an individual. It does so by allowing the recognition of a registered person through quantifiable physiological characteristics

that verify the identity of an individual. It is a user-friendly inexpensive experience incorporating the security aspects of the proposed FRAP model for ATM, thus preventing the cases of illegal transactions without the knowledge of the authentic owner. Our proposed FRAP Model, therefore, eliminates all the drawbacks of the classical model with a more secure and user friendly approach.

References

1. Card-Less Electronic Automated Teller Machine (EATM) With Biometric Authentication (http://www.ijettjournal.org/2015/volume-30/number-2/IJETT-V30P219.pdf)

2. OTP Based Cardless Transction using ATM (https://www.researchgate.net/publication/331563962_OTP_Based_Cardless_Transction_using_ATM)

3. An Overview of Thermal Face Recognition Methods (https://bib.irb.hr/datoteka/941518.5074-An-Overview-of-Thermal-Face-Recognition Methods-v2.pdf)

4. OpenFace, Free and open source face recognition with deep neural networks (https://cmusatyalab.github.io/openface/)

5. FaceNet: A Unified Embedding for Face Recognition and Clustering (https://arxiv.org/pdf/1503.03832.pdf)