Face PIN: Face Biometric Authentication System for ATM using Deep Learning

[1]Sanchana. R, [2]Purundaranarayanan, [3]Kevin Richard, [4]Balavinayagam. S

[1]Assistant Professor, [1,2,3,4]Department of Information Technology, Sri Sairam Institute of Technology, India. [1]sanchana.it@sairamit.edu.in

Abstract— Automated Teller Machines also known as ATM'sare widely used nowadays by each and every one. 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 systems today use no more than an access card and PIN for identityverification. 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 an automatic teller machine security model that would combine a physical access card and electronic facial recognition using Deep Convolution 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 – Face, PIN, Deep Learming.

I. INTRODUCTION

Due to rapid development in technology, many innovations are built-up with enhanced security features. On the other side to destroy the security walls many threats are arising. Enhancement in security level much automation has made a positive impact in the society, but many institutions like banks application like ATM are still subjected to thefts. The existing model uses cards and PIN which give rise in attacks. The attacks are in the form of card theft or duplicity of cards. In order to overcome this drawbacks hybrid models where introduced. The hybrid model consists of various conventional features. The conventional features include facial recognition and one-time password. The password and the facial recognition information are been stored in the database. The database holds the information about the account details, mobile number and finally facial recognition technique is added. The account details in addition to the OTP and facial recognition will enhance the security to a larger extent.

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. The use of facial recognition enables to deliver more advanced transactions at its ATMs because facial recognition provides an extra layer of security for both the cardholder and the bank. Bank customers can use their Debit/Credit card at the ATM to access their accounts, rather than being limited to only those accounts associated with their ATM card. With facial recognition, Bank can now guarantee its customers the most rigorous security along with the convenience of open banking.

The major advantage of using this model is integrating of the ATM is very much improved. The integrated model is implemented of biometric devices such as facial recognition and fingerprint. The validation of the system is increased which in turns increases the integrity of the system. Since these factors are implemented on the ATM machine which in turns result in the improvise the user search? The search concentrates on determine the correct user which in turns maintains the credibility of the system. The model provides increase in data confidentiality of the ATM machine and improves the authentication system. The third major advantage is the model provides advanced verification stages to access the bank account through ATM machine. The major challenges in developing the model is each and every user have their own fingerprint and facial recognition. In order to read or scan the fingerprint or facial a proper algorithm has to be implemented. Then the data that is being scanned or read need to be stored in the database. The next major challenge is which database is suitable for storing such data.

The process of cash withdrawal seems to be a simple task. The process is a combination of certain computer

 DOI : 10.35291/2454-9150.2022.0392

operations and research made on the particular domain has been done on a constant basis which has improved to offer the customers a flawless experience. The first step in withdrawal of money is to identify the person at the ATM. The process is carried out in a traditional way. The initial step is inserting the pin but now a days the identification of the user id identified using a new method such as biometric method. The facial recognition technique at the initial stage the user has to look into the camera installed on the ATM.The camera captures the user and sends the image of the user to theregistered mobile number. If the face matches with either one of the faces, the user identification gets confirmed and further the transactions are allowed. Lot of people faces security issues after they lose their cards. There are many numbers of cases where two factor authentications is very secure and reliable for credit card authentication. In addition to that multi-factor authentication can be used. Multifactor authentication includes SMS services. Multifactor authentication do not provides more security and human error plays a vital role in part of this authentication. This is the point where the point of authentication becomes very risky. The major drawback of the two factor authentication is inadequate in terms of registered cell phone provider breaches methods and its lacks security. The lack of security deals with not providing strong passwords to the user. Phishing is the easiest and the direct way to fake login page. The user gives his or her credentials to the hacker. The hacker in turns forwards the values to the login page separately. The hackers trigger the authentication procedure which leads to the target numerical code. The target is still using and now has completed the authentication procedure. The limitations are generating the code. The hacker need to generate the code as fast as possible. Once the code is generated and successfully logged in the hacker can easily manipulate the phone number of the user and email id. The hacker can easily access their Net Banking Account, where they can easily bypass 2FA of credit card transactions.

II. LITERATURE SURVEY

Impact of video surveillance system on ATM pin security was proposed by Piyumi Seneviratne et al., (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. .

Secure card-less ATM Transaction was proposed by Khushboo Yadav et.al.,(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.

Effective cash Withdrawal from ATM machine using QRcode Technology was proposed by Rahul Patil et.al. (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 QR code. 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 QR code 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.

Design of embedded based dual identification ATM card security system was proposed by Priyanka Hemant kale et.al. (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 transactions

 DOI : 10.35291/2454-9150.2022.0392

cannot be retrieved easily. To overcome such crimes the new authentication features of finger print and OTPmust be added to the ATM. Whenever the ATM transaction has been processed the ATM ask to enter PIN. After entering PIN, the OTP is sent to the number to which your bank account is linked andthe transaction can be possible. But in this system, only entering PIN is not enough ,after entering a PIN the user needs to choose anyone option to make the whole transaction successful that option is fingerprint or OTP.

Security Enhancement through IRIS and Biometric Recognition in ATM was proposed by Abhishek Tyagi et.al, (2019). Nowadays irisrecognition 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.

Secure Authentication for ATM transaction using NFC technology was proposed by Divyans Mahansaria et.al, (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. ATM card security using Bio-Metric and message authentication technology was proposed by Uttam Kumar Roy et.al, (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.

A novel ATM Security system using a user defined personal identification number with the aid of GSM technology was proposed by Swathi et.al, (2018). Presently, ATM systems use no more than an access card which usually has a magnetic stripe (magistrate) 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, simpleas 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 alsoeliminated.

Enhanced security for ATM machine with OTP and facial recognition features was proposed by Mohsin Karovaliya et.al. Thepaper mainly focuses on a new mechanism which enhances the usability, convenience of transaction at ATM. The facial recognition is introduced in order to enhance the privacy and security of the user. Facial recognition technique is mainly used to uniquely identify each and every person. This system reduces the possibility of fraud in the ATM machine. The system increases the usefulness of the system and there is no need for the user toremember the pin.

Facial verification technology for use in ATM transactions was proposed Aru. This paper mainly focuses on integrated facial recognition model. This system combines the pin and electronic facial recognition model with the physical access card. The major advantage of the model is to increase the security in user identification.

III. ARCHITECTURE

Existing ATM authentication method is the use of password-PINs and OTP. 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. QR cash withdrawals were enabled so customers could ditch their ATM cardsand simply scan a QR-code on ATMs using the QR app to withdraw cash. A QR code scanner is required to detect code and decrypt

 DOI : 10.35291/2454-9150.2022.0392

information in stored in QR code. 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 QR code 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. The algorithms used 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). LDA, PCA.

The proposed system consists of face recognition module. The module is subdivided into face enrollment module and face authentication module and unknown verification link. The face enrollment module registers the new user face with the bank beneficiary templates. The face authentication module captures the face image and send the information to the face authentication module. 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.

The proposed system works as follows – the initial step is user approaches the ATM Machine. The system asks the user to show his face on the camera. The system captures the face and sends the captured face to the particular account holder. The captured face is received by the account holder that is to the registered mobile number. The user has to either accept or decline. Once the accept button is pressed the user is allowed to withdraw the cash. Once the cash is withdrawn the user receives a message containing the information about how much amount is withdrawer. Once the decline button is pressed the user will not be allowed to withdraw the cash. The following figure 3.1 represents the system architecture of the facial recognition model.

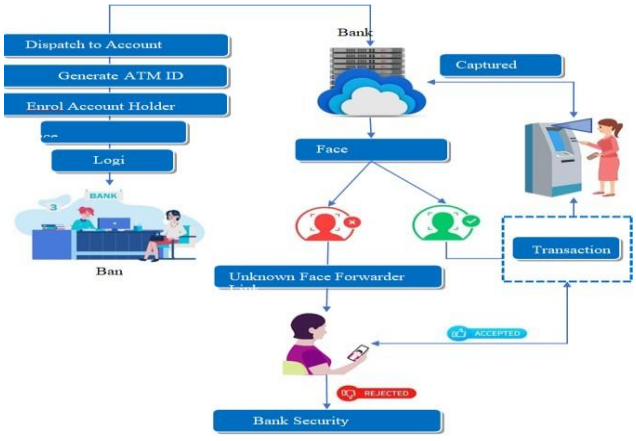

Figure 3.1 System Architecture

IV. MODULE DESCRIPTION

4.1 ATM SIMULATOR

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.

4. 2. FACE RECOGNSATION MODULE

Face enrollment module begins by registering a few frontal faces of Bank Beneficiary templates. These templates then become the reference for evaluating and registering the templates for the other poses: tilting up/down, moving closer/further, and turning left/right.

Face authentication is done by capturing the face image from the ATM camera, the image is given to face detection module. This module detects the image regions which are likely to be human. After the face detection using Region Proposal Network (RPN), face image is given as input to the feature extraction module to find the key features that will be used for classification. The module composes a very short feature vector that is well enough to represent the face image. Here it is done with DCNN with the help of a pattern classifier, the extracted features of face image are compared with the ones stored in the face database. The face image is then classified as either known or unknown. If the image face is known, corresponding Card Holder is identified and proceeds further. The following figure 4.1 represents the facial recognition methods.

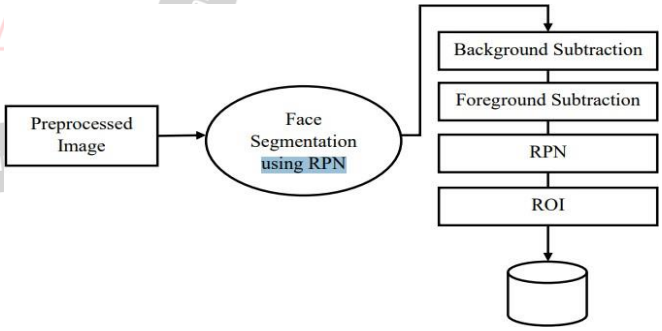

Figure 4.1 Facial Recognition

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.

4.3 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

 DOI : 10.35291/2454-9150.2022.0392

displayed.

4.4 TRANSACTION MODULE

Enter the withdrawal amount and press enter. But make sure your withdrawal amount does not exceed your balance in the account otherwise transaction will fail. The money can be collected from the lower slot of the ATM machine.

4.5 ALGORITHM

DCNN is a machine learning techniques. DCNN model is used to build an artificial intelligence system. The model is developed based on the idea of artificial neural network. The model is mainly designed to perform complex analysis on huge amount of data by passing the input to the multiple layers of neurons. DCNN is mainly used to identify the pattern in images and videos. The algorithm mainly focuses on application such as object detection, image classification and recommendation system. There are two kinds of DCNN one is increasing the number of hidden layers. The other kind is increasing the number of nodes in the hidden layer. The main advantage of using DCNN is layering. The model uses three dimensional neural networks to process the red, green and blue elements of the image at the same time. The model in turns reduces the number of artificial neurons required to process an image. The model takes the input as images and uses these data to train the classifier model. Once the model is classified it employs certain mathematical operation of the input images. The mathematical operation is called convolution instead of matrix multiplication. The convolution layer is the first layer that is used to extract the various features from the input images. The mathematical operation is performed in between the input images and the filter. The dot product is performed between the filter and the parts of the input image. The output obtained after the dot operation is termed as feature map. The feature map gives the information about the images such as corners and edges. The second layer is the pooling layer. The main aim of this layer is to decrease the size of the convolution feature map to reduce the computational cost. The computational cost is reduced by decreasing the connections between the layers and independently operates on the feature map. The third layer is fully connected layer which consist of weights and bias along with the neurons. The fully connected layer is placed before the output layer and from the last few layers of the CNN architecture. The input obtained from the previous layer is flattened and fed to the fully connected layer. The last layer is the dropout layer. The layer is mainly introduced when all the features are connected to fully connected layer it can cause over fitting of the data. In order to overcome this problem a dropout layer is introduced. The dropout layer is utilized when few neurons are dropped from the neural network. The neurons are dropped from the network which in turn results in reducing the size of the model. The final is activation function which is used to learn the continuous and complex relationship between the variables. There are several activation function used they are ReLU, Softmax and sigmoid functions. In DCNN model the sigmoid and the Softmax function are used for binary classification. For multiclass classification generally Softmax activation function is used. The working of facial recognition is numerical representation of the face is termed as feature vector. The various attributes are taken for detecting the faces are height and width of the face, color of the face, height and width of parts of the face and finally the ratio obtained is feature vector after the rescaling. The feature vector obtained after the rescaling can be organized. These attributes are organized into a table. The machine learning model can be used in tow things they are deriving the feature vector and matching algorithms. In the process of deriving the feature vector we convert the entire feature vector into names. The machine learning algorithm can label out these features. In matching algorithms it matches the new image with the set of features vectors present in the corpus.

4.6 PROGRAMMING LANGUAGES

The database chosen is MySQL for storing and retrieving the facial recognition related information in the database. The data is being stored in the form of images such as BLOB format. MySQL can be integrated with the python programming and allows storage of data to be stored. The programming languages used is python.

V. RESULT AND DISCUSSION

5.1 HOME PAGE

The following figure 5.1 represents the home page of the ATM machine. The home page contains information about the admin login.

Figure 5.1 Home page of ATM machine

5.2 ADMIN PAGE

The following figure 5.2 represents the admin page. The admin page contains the information about the admin username and password. Once the username and password is entered press the login button.

 DOI : 10.35291/2454-9150.2022.0392

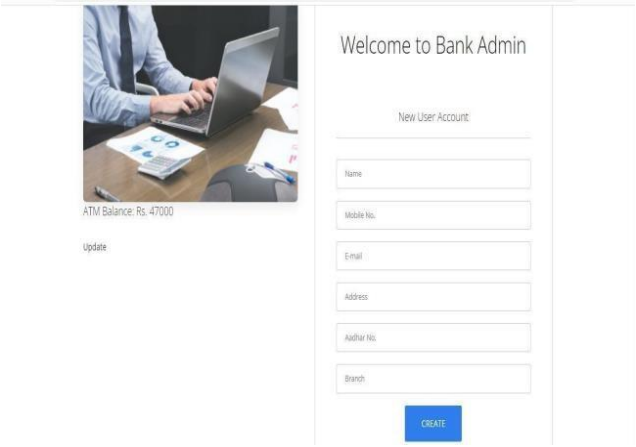

Figure 5.2 Admin page

5.3 CREATION OF USER ACCOUNT

The following figure 5.3 represents the creation of user account. The account page asks the user to enter the name, mobile number, email id, address, aadhaar number and branch details. Once the details are entered press the create button. The create button creates and stores the user related information in the database for future reference. Once the account is created the user can enter the admin page. In the admin page the user is asked to enter the username and the password details.

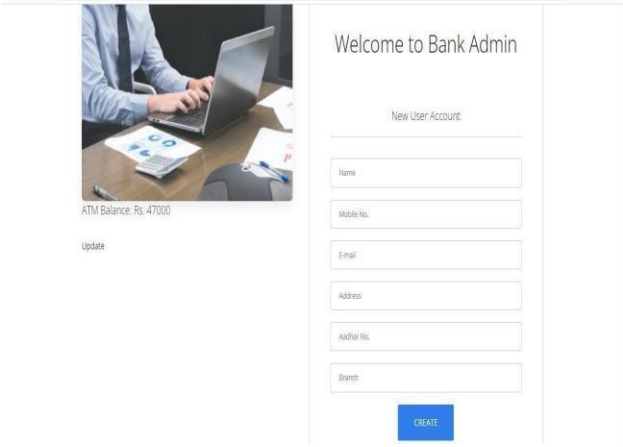

Figure 5.3 Creation of User Account

5.4 VERIFICATION PAGE

The following figure 5.4 represents the verification page. When the card is inserted the verification message is send to the particular account holder. The user has to wait for certain amount of time until the card holders accept the approval.

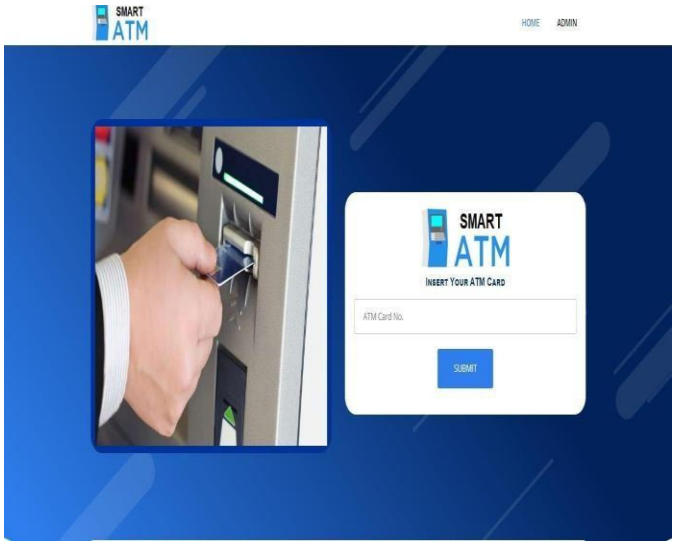

Figure 5.4 Verification page

The following figure 5.5 represents the approval page from the user. Once the ATM Card is inserted the verification message is send to the user along with the face verification. The message is send to the account holder. Once the account holder accepts it allows the particular user to withdraw the money else the user is not allowed to withdraw the money once the decline button is pressed.

Figure 5.5 Approval page from the user

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

 DOI : 10.35291/2454-9150.2022.0392

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] 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.

[2] 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.

[3] A. Li, S. Shan, and W. Gao, ``Coupled bias-variance tradeoff for cross-poseface recognition,'' IEEE Trans. Image Process., vol. 21, no. 1, pp. 305-315,Jan. 2012.

[4] 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.

[5] 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.

[6] 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, p5.

[7] T. Sharma and S. L. Aarthy, ``An automatic attendance monitoring systemusing RFID and IOT using cloud,'' in Proc. Online Int. Conf. Green Eng.Technol. (IC-GET), Nov. 2016, pp. 1-4.

[8] 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.

 DOI : 10.35291/2454-9150.2022.0392