A Survey on Secure Access in Online Transaction with Multi Party Face Identification

V. Jeeva[1], Dr. R. Ravi[2]

[1]*M.E., Student,* [2]*Associate Professor,*

Department of Computer Science and Engineering, JJ College of Engineering and Technology, Trichy, Tamil Nadu, India

***Abstract:-*Internet banking services must be more responsive towards security for clients. Now a day in this network world, the way for cybercrime becomes so easier for hacking purpose. For this reason, network security has become one of the biggest challenges in today's IT department's security. Internet banking transaction should be layered protection against security threats; the providers should give security considerations as part of their service offerings. And by hearing a lot about hackers and crackers ways to steal any logical password or pincode number character, crimes of ID cards or credit cards fraud or security breaches. In existing framework, Identification can be equated to a username and is used to authorize access to a system. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he or she claims to be – the authentication process. Authentication based on biometric and identification systems are the new solutions to address the issues of security and privacy. The Face Recognition is the study of physical or behavioral characteristics of human bio structure used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. So implement real time authentication system using face biometrics for authorized the person for online banking system. The general objective of our project is to develop fully functional face recognition, verification system provide and understand the key aspects of these major technologies, namely those relating to the technological, application entity domain, social environmental system and performance aspects. And also provide multiparty access system to allow the multiple persons to access the same accounts by providing access privileges to original account holders. Experimental results show that the proposed system provide high level security in online transaction system than the existing traditional cryptography approach.**

Keywords: **ATM, Security, Face recognition, verification, Fraud, PIN, KNN Classification**

I. INTRODUCTION

ATM is an electronic telecommunication tool to facilitate the clients of an economic organization to carry out monetary deal, mainly currency extraction, lacking the need for a being cashier, clerk or banker. On the accumulation contemporary ATMs, the client is recognized by inserting a plastic ATM card with a attractive strip or a plastic smart card with a chip that contains a limited card number and a few safety information such as an end date. Confirmation is provided by the client entering a personal identification number (PIN). With an ATM, client can way in their bank deposit or credit accounts in arrange to make a variety of transactions such as cash withdrawals, check balances, or credit mobile phones.

To use an ATM with facial recognition system it needs digital camera. In a day, computer will automatically initiate a face recognition procedure, whenever the computer detects a face in camera that obtains a picture of your face, then the computer will compares the image of the face to the images of registered customers in its database .If the face (as seen by the ATMs camera) matches the picture in the data base, it automatically authenticate. The machine will then play a recording that will be heard through a loudspeaker, which says" your face is recognized". ATM is a device that made currency dealings simple for clients. This paper proposes an automatic teller machine security model that would combine a physical access card, a PIN, and electronic face recognition.

II. RELATED WORK

Roger A. Leite [1] this paper one of the main concerns of monetary institutions is to assurance safety and authority in their services. The reliability of these notice and evade fake schemes institutions also improved. Now, still require Visual Analytics techniques still lacks the fraud discovery approaches. This manuscript planned a Visual Analytics process that tackles the main challenges in the area of fraud detection. Financial pitch becomes the major challenges of fraud discovery. Though active approaches utilize still data displays a VA approach, focusing on fraud detection, and customer monitoring. The require of the pipeline combines well-organized fraud detection techniques (i.e., AI techniques and fraud detection metrics) with VA methods.

Roger Almeida Leite [2] paper monetary institutions are constantly attracted in ensuring safety and superiority for their clients. Banks require to recognize and avoid insecure transactions. To detect fraudulent operations, data mining techniques based on verification and customer profile generation are commonly used. Still Visual Analytics technique approaches are not supported. The proposed a Visual Analytics approach for supporting and fine-tuning profile analysis and reducing false positive alarms. Based on these challenges we propose a VA approach for profile analysis to support fraud detection and user monitoring. An integrate this VA approach into the fraud detection process to

efficiently combine AI techniques with interactive visual means.

William N. Dilla a [3] interactive data visualization is potentially useful for detecting fraudulent transactions. Analyze factors influencing the efficiency and effectiveness of this technology. This analysis includes a set of testable research propositions. To detect transaction anomalies is an important fraud detection procedure the data are analyzed. To change the representation of data from text to graphics and filter out subsets of transactions for further investigation have ability to make the detection of fraudulent transactions more efficient the investigators allows the Interactive data visualization tools. This framework will developed research questions and testable propositions related to this topic. The paper concludes that how academic research might proceed in investigating the efficacy of interactive data visualization tools for fraud detection.

Johnatan S. Oliveira [4] the security of transactions is currently one of the major challenges facing banking systems. The biometric authentication using the face becomes the adopted technique due its convenience and acceptability. Nowadays, almost all mobile and computers devices have built-in cameras. User authentication approach is attracted by the large investments in banking and financial institutions, especially in cross-domain scenarios, where the facial images from ID documents that are compared with digital self-portraits (selfies) taken with the mobile devices, for the immediate opening of new checking accounts or financial transactions authorization.

T. Suganya [5] ATM though banking becomes easier, it also became feeble. There has been infinite gear of abuse in banking transactions. It is essential to provide high security. In this paper the amalgamation of Face Recognition System identifying verification process engaged in ATMs to enhance the security system is been proposed. Facial verification software at present have the task of provided that important match rates for use in ATM transactions. By adding the facial recognition systems to the identity confirmation process used in ATMs will reduce transactions to a great extent.

Face recognition is an attractive area of research for both computer vision scientists and neuroscientists. Human beings are having the ability to identify, with high rate of reliability. A large number of faces recognition researches illuminate computer vision. In this research, an ATM model will be more reliable in giving more security by using facial recognition approach that is presented with conceptual framework for use of face- based access control in ATMs. The research has listed that ATM users have been encountered many problems in the past, which the research work has offered solutions. While the scope of this research, further works could be considered in the area of integrating virtually in all the biometric measures into a unique system. This will strongly ensure maximum security in all ATM-related transactions and also reduce frauds and to reduce all the aforementioned problem that are advisable that government partner with banking sector to use biometric techniques “face-based access control” in ATMs as it will reduce the problems associated with smartcard access control.

Olutola Fagbolu [6] in this paper face recognition has been an attractive area of research for both neuroscientists and computer vision scientists. In this ATM model there is more reliable in providing security by using facial recognition approach which are with conceptual framework for face-based access control in ATMs. This will totally ensure high security in all ATM-related transactions and drastically reduce frauds and to overcome all the aforementioned problem it is advisable that government partner with banking sector to use biometric techniques “face-based access control” in ATMs as it will eradicate the problems associated with smartcard access control.

Sandeep V, Guruprasad Hegde [7] recently, bank and locker robberies are frequently happening. This means the locker is vulnerable to theft since it has less protection rather than a lock and key. Latently, many banks use two keys to open the lockers. Introducing Locker Security Sys-tem based on Face Recognition and GSM (Global System for Mobile) technology, which can be used in Banks, Security Offices and Homes for giving protection to expensive things. In this system, the authorized person can only access the valuable like money, licenses and jewels from locker. Face Recognition is done by active appearance model algorithm with Bayesian classifier that is used to identify the persons and verify their identity with the Raspberry Pi processor. RFID (Radio-frequency identification) and GSM technology are combined together for accessing the locker securely. When an authorized person tries to access the locker, the system will generate a one-time password and send to the registered mobile number of that person. If the password entered by him is correct, then only he will be allowed to access the locker. If he does any offensive acts on the locker, it will be sensed by the vibration sensor and the sensor will send the control signal to Raspberry pi processor and it will generate alarm sound.

III. EXISTING METHODOLOGY

Existing approach exploits the discriminate information of the generic set for the face synthesis process. The new algorithm called domain-specific face synthesis (DSFS) maps representative variation information from the generic set in the OD to the original reference stills. In this way, a compact set of synthetic faces is generated that represent reference still images and probe video frames under a common capture condition. The DSFS technique involves two main steps: (1) characterizing capture condition information from the OD, (2) generating synthetic face images based on the information obtained in the first step. Prior to operation (during camera calibration process), a generic set is collected from video captured in the OD. A compact and representative subset of face images is selected by clustering

this generic set in a capture condition space defined by pose, illumination, blur. The 3D model of each reference still image is reconstructed via a 3D morphable model and rendered based on pose representatives. Finally, the illumination-dependent layers of the lighting representatives are extracted and projected on the rendered reference images with the same pose. In this manner, domain-specific variations are effectively transferred onto the reference still images.

IV. COMPARISON & DISCUSSION

Author	Title	***Purpose***	***Techniques***	Disadvantages
Roger A. Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein, and Johannes Kuntner	Visual Analytics for Fraud Detection and Monitoring	A Visual analytic process that deals the main challenge in the area of fault deduction. This is done by Pipeline combines efficient fraud deduction technique.	Visual Knowledge Discovery, Time Series Data, Business.	• The modification of analytic method will be problem.
Roger Almeida Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein & Johannes Kuntner	Visual Analytics for Fraud Detection: Focusing on Profile Analysis	A Visual Analytics approach for supporting and fine-tuning profiles analysis and reducing false position alarms.	Visual Knowledge Discovery, Time Series Data, Business and Finance Visualization, Financial Fraud Detection.	• Repeating the process will have the time consumption.
Johnatan S. Oliveira Gustavo B. Souza, Anderson R. Rocha, Flavio E. Deus and Aparecido N. Marana	Cross-Domain Deep Face Matching for Real Banking Security Systems	Login the account using the cross domine image (selfi) using mobile.	Normalization	• The camera quality in customer mobile should have the high pixel.
T. Suganya, t. Nithya C. Sunitha , b. Meena preethi	Securing ATM by image processing – facial Recognition authentication	Deducting the face recognition using the structure of the face using graphical scale with accuracy.	ATM System, Face Recognition Software (FRS), Security.	• Become complex when the client facial structure change.
Olutola Fagbolu, Olumide Adewale Boniface Aleseand Osuolale Festus	Secured Banking operations with face-based Automated Teller Machine	Capturing the various face by the dimension to produce the optimal linear squares decomposition of a training set and Eigen face.	Personal Identification Number (PIN), biometrics, security, eigen faces, fraud.	• Storing all related data in a single system will reduce the process.
Prof. Sandeep V, Guruprasad Hegde , Chetan N, Girish P Patil, Lad Bhavesh	Face Detection based Locker Security System using Raspberry Pi	Using the model algorithm with Bayesian Classification, identification and verification of data using Raspberry Pi Processor.	Appearance model algorithm with Bayesian classifier	• No Co applicant can access the account at any cost.

V. PROPOSED FRAMEWORK

The first step of this paper is to locate a powerful open-source facial recognition program that uses the local feature analysis and which is targeted at face verification. This program should be compliable on multiple systems Windows variants, and should be customizable to the extent of allowing for variations in processing power of the machines onto which it would be deployed. Need to familiarize ourselves with the internal workings of the program so that we can learn its strengths and limitations. Simple testing of this program will also need to occur so that we could evaluate its effectiveness. Several sample images will be taken of several individuals to be used as test cases – one each for "account" images, and several each for "live" images, each of which would vary pose, lighting conditions, and expressions. Once a final program is chosen, we will develop a simple ATM black box program. This program will serve as the theoretical ATM with which the facial recognition software will interact. It will take in a name and password, and then look in a folder for an image that is associated. Eradicate Fraud costs for the bank deliver a practical and workable solution that addresses the requirements of the regulatory authorities.

Proposed System Architecture

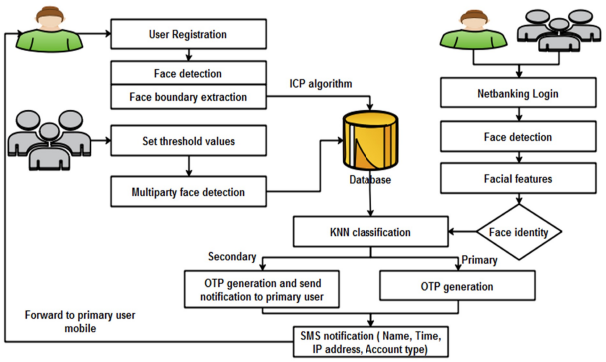

Figure: Proposed System

Limit the financial risks given that they were forced to take responsibility for financial loss [rather than being allowed to pass this on to the account-holder Provide a framework that still allowed for high withdrawal limits to cater for the demands of a cash-focused customer base Take societal responsibility to reduce rising levels of crime that

were associated with cash-card transactions Increase customer satisfaction.

V. CONCLUSION

The survey paper develops an ATM model that is more confidential in providing security by using face recognition software for authentication. By keeping the time beyond the verification process to an insignificant amount we even try to maintain the efficiency of this ATM system to a greater degree. Identifying and authenticating account holder and the co-applicant at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this paper issue of fraudulent transactions through Automated Teller Machine by biometrics that can be made possible only when the account holder is physically present. This survey paper online transaction ATM face detection various techniques & method process.

REFERENCES

[1]. Visual Analytics for Fraud Detection and Monitoring Author: Roger A. Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein, and Johannes Kuntner Year: 2013 Vol 24 pp.201-202

[2]. Visual Analytics for Fraud Detection: Focusing on Profile Analysis Author: Roger Almeida Leite, Theresia Gschwandtner, Silvia Miksch, Erich Gstrein & Johannes Kuntner Vol 323 Year: 2016 pp.1-3

[3]. Data visualization for fraud detection: Practice implications and a call for future research Author: William N. Dilla a, Robyn L. Raschke b Year: 2015 Vol 16 pp.1-22

[4]. Cross-Domain Deep Face Matching for Real Banking Security Systems Authors:Johnatan S. Oliveira, Gustavo B. Souza, Anderson R. Rocha, Flavio E. Deus and Aparecido N. Marana Year: 2018 Vol 22pp.

[5]. Securing ATM by Image Processing – Facial Recognition Authentication Authors:T. Suganya, T. Nithya C. Sunitha, B. Meena Preethi .vol:4 pp.913-916.Year:2014

[6]. Secured Banking operations with face-based Automated Teller Machine Authors: Olutola Fagbolu1, Olumide Adewale2 Boniface Alese2and Osuolale Festus2. vol-10. pp.584-592.Year:2014

[7]. Face Detection based Locker Security System using Raspberry Pi Authors:Sandeep V, Guruprasad Hegde , Chetan N, Girish P Patil, Lad Bhavesh .vol-7. pp.73-77.Year:2016