Biometric based ATM System: A Survey

Subhrajit Roy
MCA
Jain University, Jayanagar 9th Block, Bengaluru.

Dr. Pawan Kumar
Assistant Professor
Jain University, School of CS & IT

ABSTRACT:- **Biometrics-based authentication is a potential alternative to password-based authentication. Of all biometric methods, face-based identification is one of the most convenient one. In ATM systems, facial images are captured using a high resolution camera. Bank security measures can play an important role in preventing customer attacks. These measures are of paramount importance in addressing the weaknesses of civil lawsuits. Banks must meet the criteria to provide their customers with a secure banking environment. This white paper focuses on the increased vulnerability and criminal activity of automated teller machines (ATMs), not the banks themselves. Both customers and bankers.**

Keywords: **Automated Teller Machine(ATM), Camera, Verification, Crime, E-Banking.**

INTRODUCTION

The ATM is an automatic teller machine that could be a computerised telecommunications device that gives clients of a establishment with access to monetary transactions in an exceedingly public area while not the requirement for somebody's clerk or bank teller. In ATMs the customer is known by inserting a plastic ATM card with a magnetic tape or a plastic smartcard with a chip that contains a novel card variety and a few security information. the primary ATM was put in in Enfield city in London on June 27, 1967 by Barclays Bank. The ATMs are acknowledged by numerous alternative names as automatic Transaction Machine, automatic Banking Machine, money purpose (at Britain), Hole within the wall, Ban extraterrestrial object (in Europe and Russia) and Any Time cash (in India).

With automated teller machines (ATMs), customers can make bank transactions anytime, anywhere without the need for a human teller. By using a debit or ATM card at a ATM, an individual can withdraw cash from one account, deposit or transfer money from one account to another, and perform other .The number of financial crimes has increased significantly over the past few years, primarily centered on ATM cards. All parties, including bankers and customers, are faced with crime and security threats to the card scheme. Many criminals are researching various illegal ways to manipulate and steal customer data on ATM cards. If a user's ATM card or PIN is lost or stolen, the user's account becomes vulnerable to attack. Fraudsters are now adopting different means to look for a user's personal identification number (PIN) in order to scam an unsuspecting customer. The traditional method of authenticating a user using a password and user ID or ID card and PIN has some limitations. Passwords or PINs can be hacked by cybercriminals or obtained through surveillance. If an ATM card is lost or stolen, an unauthorized person can attempt to manage the bank account of an authorized customer. Many customers use their phone number and date of birth as their password. This can be easily guessed by

a barbaric attacker. Because biological information is unique, cannot be transferred to the owner, and cannot be replicated by anyone, biometric technology has the potential to solve these problems in existing systems. This paper proposes a system to replace the existing card system of ATM transaction with biometric face recognition used in the ATM system.

The main goal of this research system is to create a Face Recognition-based ATM system that uses the user's face as authentication. You don't have to worry about losing your ATM card, and you don't have to carry your ATM card in your wallet. To do banking, just use your face. Users must sign in with their own face. Users can withdraw money from their account. To withdraw funds, the user must enter the amount they want to withdraw and specify the account they want to withdraw (savings account, checking account, etc.).

Related Work:

Mr. Aru, et al., suggested Today's ATM systems suggest using PINs and access cards for identity verification. Recent advances in biometric technology, retinal scans including fingerprints, and facial recognition have made great efforts to save unstable ATM situations.

In this study, we considered developing a scheme to integrate facial recognition technology into the validation process used in ATMs. ATM systems have been proposed that reliably provide higher security by using face recognition. By developing such a system, customers and financial institutions can be protected from intruders and identity thefts as well.

The main aim his paper is to concentrates on an ATM security system which would combine a Personal Identification Number, a physical access card, & electronic facial recognition that will go as far as withholding the fraudster`s card. Nevertheless, it`s apparent that person`s biometric capabilities can not be replicated, this suggestion will cross a protracted manner to resolve the trouble of Account protection making it feasible for the real account proprietor on my own have get entry to to his accounts. The blended biometric capabilities method is to serve the cause each the identity and authentication that card and PIN do. [9]

Moshin Karovaliya, et al.[1] suggested Features such as facial recognition and one - time passwords are used to improve account security and user privacy. Face recognition technology helps the machine uniquely identify individual users. This allows the to use

the face as a key. This eliminates the possibility of fraud due to theft or duplication of the ATM card. In addition, the randomly generated OTP acts as the PIN itself, eliminating the need for the user to remember the PIN .

Face recognition and PIN number-based user authentication. He preferred to use Face recognition-based user authentication system with PIN due to technological advances in financial infrastructure, most bank customers have automated ATMs (automated teller machines) and internet websites to carry out banking transactions. The goal of our work is to run face recognition using the new computer vision framework with a built-in ATM camera. Customer authentication on automated teller machines (ATMs) usually relies on full PIN-based verification. So far, several factors have been investigated to improve the security of customer authentication at the ATM. In the first scenario, If the pin number and face recognition match, Then the User will be given access to their account. In the second scenario, if the pin and face recognition do not match, the User will not be given access.

The paper [3] proposes a vibration sensor that detects delivered from ATM machines at whatever factor robbery happens. His framework makes use of

an ARM regulator-primarily based totally inserted framework to handle ongoing data amassed utilising the vibration sensor. When the vibration is detected the sign sound will show up from the bell. DC Motor is applied for shutting the entryway of an ATM. Some different more protection efforts are applied. This will prevent the burglary and the individual including in robbery can be effects gotten. Programming execution is despatched utilising programming bundles, the initial one is the Keil Vision 3.0. The second one is the Flash sorcery test system . Keil Vision 10 Debugger precisely recreates on-chip peripherals. This framework helpsin quick response and minimization of misfortune with the aid of using distinguishing the ATM machine at a consistent whilst it's been taken may be determined thru GSM technology. In paper [4], the unique mark acknowledgment is completed with curvelet alternate by tracking down the Euclidean distance between the relating finger codes. The test finger code is contrasted and the entire finger codes within side the data base. In the case of its matches, an OTP will be despatched to the corresponding registered mobile number. Pre-processing is done with the aid of using using built-in math lab functions read. Histogram equalization method helps in working on the international difference

of a picture with the aid of using moving marginally the depth distribution on a histogram. This permits areas of lower nearby evaluation to benefit a better differentiation with out influencing the international difference. Histogram adjustment satisfies this with the aid of using viably fanning out the most successive power esteems. The component extraction should be possible utilising curvelet alternate and by using FFT. The ATM protection is upgraded with the aid of using including a GSM module to provide OTP in paper [5]. When there's an corporation difficulty in GSM innovation, instead of GSM right here executes Bluetooth affiliation with ATM, which produces OTP reference thru patron portable. GSM modems can be a quick and compelling manner to get commenced with SMS due to the fact a unique subscription to an SMS provider issuer isn't always required. The paper [6] recommends fisher faces calculation for face acknowledgment. Contrasted with global primarily based totally administered dimensionality decrease techniques like Fisher discriminant analysis (FDA), locality-primarily based totally ones including Local Fisher Discriminant Analysis (LFDA) have drawn in increasing interests since they expect to pre-serve the intrinsic records structures and are able to handle

multimodally disbursed data. In any case, both FDA and LFDA are typically tackled thru a proportion follow structure to inexact the following proportion, which is Fisher's unique goal criterion. In the paper, [7] Deep Learning method is offered as a piece of learning-primarily based totally methodology to give a general research approximately the face checks gift within side the framework. The obvious preferred problems in face acknowledgment are fake faces and the components influencing acknowledgment exactness like commotion, redirections in the factor, postures, and appearance. These problems are the fundamental driver for a framework to lose its perfection, right here it improves the accuracy of recognition with the aid of using keeping the track of historical data approximately the faces arriving as an input. The experimental consequences obtained on YALE and ORL records set show that this is an green method. One-Touch Multi-banking Transaction ATM System utilising Biometric and GSM Authentication is implemented in paper [8] the account details of the user are saved on cloud in a unified manner. The file subtleties of all of the financial institution money owed of account holders are shown. The patron wishes to choose one of the financial balances for the trade. Assuming the patron wishes

to transport the coins or price the coins from ac-take a look at he'll get OTP at the enrolled flexible number. The GSM module produces OTP for enforce legitimate trade from the financial institution side.

CONCLUSION:

Facial recognition has evidenced to be one in all the foremost secure strategies of all biometric systems to realize a high level of security, forestall ATM robbery, and supply ATM security. It replaces the standard ATM system. it's benefits love savings in card producing prices and overcomes the shortcomings of traditional systems such as carrying ATM cards, losing cards, and ATM card-related deceitful calls. you'll be able to improve system efficiency.

REFERENCES:

1. "J.J.Patoliya et al. , "Face Detection based ATM Security System utilizing Embedded Linux Platform ", second International Conference for Convergence in Technology (I2CT), (2017)."

2. "M.Karovaliyaa et al., "Improved security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Technologies and Applications (ICACTA), (2015)."

3. "Sivakumar T et al., " Plan and Implementation of Security-Based ATM burglary Monitoring framework", International Journal of Engineering Inventions, Volume 3, Issue 1, (2013). "

4. "C. Bhosale et al., "ATM security utilizing face and unique finger impression acknowledgment", International Journal of Research in Engineering, Technology and Science, vol. 7, Special Issue, Feb. (2017)."

5. "Manoj V et al. MultiAuthentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology (IRJET), 71."

6. "L. Wang et al. " Face acknowledgment utilizing most extreme nearby fisher discriminant investigation", eighteenth IEEE International Conference on Image Processing, (2011)."

7. "K.Shailaja et al. , "Successful Face Recognition utilizing Deep Learning-based Linear Discriminant Classification ", IEEE International Meeting on Computational Intelligence and Computing Research, (2016)."

8. "H. R. Babaei et al. , "Face Recognition Application for Automatic Teller Machines (ATM)", International Conference on Information and Knowledge Management (ICIKM) , (2012)."

9. "Aru et al. "Facial Verification Technology for Use In ATM Transactions" American Journal of Engineering Research (AJER) e-ISSN :2320-0847p-ISSN:2320-0936 Volume02, Issue-05. (2013)."

10. "Archana et al., "Enhance the Security in the ATM System with Multimodal Biometrics and Two-Tier Security", International Journal of Advanced Research in Computer Science and Software Engineering 3(10), pp. 261-266, October (2013)."