International Journal of Interpreting Enigma Engineers (IJIEE)

https://ejournal.svgacademy.org/index.php/ijiee/

OPEN ACCESS

ATM TRANSACTION WITHOUT A CARD VIA BIOMETRIC AND HAND RECOGNITIONMETRIC

IJIEE
INTERNATIONAL JOURNAL OF INTERPRETING ENIGMA ENGINEERS
Published by
Swami Vivekananda Global Academy, India
June 2024 | Vol. - 1 | Issue - 2

Manisha Bandari, Dr GVS RAJU

Original Article

Professor & Department of Computer Science Engineering1.2, Stanly College of Engineering &Technology For Women,India

*Corresponding Author's Email: bandarimanisha40@gmail.com

Abstract

Studying the system that allows for more secure cash withdrawals from ATMs is the main goal of this research. It is an approach, banker will be capture the clients phone number and prints during opening account, and only the consumer will have access to the ATM. When a customer accesses an ATM, the system will begin to function. There is an entrance switch first. Upon entering, the consumer is required to place his finger on the fingerprint module. After that, the system verifies the user's identification and the finger's legitimacy. For all of recorded time, humans have recognized one another based on a variety of traits. We recognize people based on their facial expressions and voices when speaking with them. Computer systems have historically relied on user knowledge (passwords, PINs), or possessions (keys, magnetic or chip cards) for identity verification, or authentication. On the other hand, things like cards and keys frequently get lost or stolen, and passwords are frequently forgotten or revealed.Using a characteristic that accurately describes the individual in question will lead to more trustworthy identification or verification. Based on the concept of observable physiological or behavioral traits, biometrics provide automated techniques for identity verification or authentication.

Keywords: OTP, PIN, two-phase security, and biometric ATMs.

Introduction

Current user authentication techniques using identifying cards and PIN's(personal identification numbers) or passwords and user IDS(identifiers) have several shortcomings .One unlawful method of obtaining passwords and PIN's is by direct covert observation. When a hacker gains network access or a user ID.User identification is also required by a plethora of other ubiquitous applications, which include online banking,e-shopping , and physical control over computer resources.These applications might also benefit from having a password, as it gives an attacker complete access to the user's resources.

Furthermore, there is no means to establish a positive connection between the system or service user and themselves; in other words, the user ID owner cannot be protected from being retracted. As a result, we propose a verification technique that incorporates fingerprint biometrics in addition to cash cards and PINs. This biometric capability is obtained by standard ATM operations, requiring no additional steps. Furthermore, this biometric trait is difficult to falsify since it is a dynamic property that varies over time. While common biometric characteristics like face, iris, and DNA can provide a high level of accuracy, they are not ideal for use in ATM verification. Because they impose physical and psychological strain on ATM users and necessitate the use of a specialized gadget and particular operation from the user. It is also possible to duplicate these static biometric traits [1,2].ATM systems can employ the fingerprint technique more frequently due to its benefits in creating a non-intrusive environment.

Literature Review

The vital for improving ATM deal security is secured in this paper. The ATM has developed less secure due to a critical rise in felonious effort and the volume of villains. Right presently, ATMs fair bear an get to card and Leg to authenticate a stoner's dentification. Not as it were does the specific Distinguishing proof Number(Leg) grant great security. The point is one of a kind and cannot be replicated by another individual. This composition employments a combination of point acknowledgment and leg confirmation innovation for identification. It too diminishes the stoner's dependence on bank officers in exchanging plutocrat to removed cousins at domestic and overseas. Concurring to Mr. Aru and others, Legs and get to cards are suggested by ultramodern ATM frameworks for recognizable proof confirmation. A parcel of work has been done to spare unsteady ATM circumstances with later progressions in biometric advances, retinal audits (counting fingerprints), and facial acknowledgment. In this investigation, we looked into making a arrange to incorporate facial acknowledgment innovation into ATM affirmation methods. proffers have been made for ATMs that utilize confront acknowledgment to continually offer expanded security. visitors and monetary teach can be protected against programmers and personality robbery by making a framework like this. (1). In spite of the fact that confront acknowledgment is by and by developing at a awesome pace, there are various issues to be tended to. in this way, there's a awesome inevitability for confront acknowledgment styles are bettered. easing driving biometrics investigation of distinguishing proof of affirmed existent advance reasons utilizing face focuses, lines, locales. Manish etal.(2), recommended the utilize of fingerprints and confront acknowledgment. within, the confirmation law is latterly exchanged portable client law . However, that people confront is to be saved and posted to assist recognize guilty parties, In the event that somebody enters an erroneous law. Chowdhury etal. in paper (3) have displayed the work grounded on numerous druggies' sentiments. They've moreover utilized the CNN show to apply a acknowledgment approved comes about grounded on interests of Joy still, the comes about weren't precise sufficient, and challenges when product changed within and the delicacy additionally demonstrated to be lacking. Kumar etal. the work in(4) has displayed the Arduino ATM security framework grounded on Haar's calculation to fete the confront of the bank's visitors. Still, they set up that it requested more extension and superior execution to deliver an precise result. In the long run, Mohite etal.(5) upheld point and facial acknowledgment ATM security utilizing demonstrate by giving four chances to authenticate coordinating. In spite of the fact that the framework is grounded on two biometrics, the person's distinguishing proof was lacking, and the comes about were outfitting small to no delicacy. proposed combining three facial acknowledgment styles coordinate discriminant investigation, beat component examination unique twofold designs. styles were connected to colorful components to guaranteed the delicacy of the acknowledgment. With respect to the confront, smart of first twofold pattern which had destitute delicacy stoner's confront. Still, the delicacy influence accomplished way acknowledgment was shallow and inadequate. proposed combining biometrics with a confront and point for stoner distinguishing proof and confirmation employing a scoff pimicro-controller to look within the database. And they recommended coordination manufactured insights for simpler recognizable proof of druggies. Jebaline etal. displayed a biometrics ATM framework blowfish calculation, print of a point, portions the being with the database in an interpreted some time recently exchanging it to the garçon to guaranteed security. developed a point acknowledgment ATM framework model, utilized PIC16F877Amicro-controller and composed the framework utilizing framework empowered recognizable proof of the stoner effectively**.**

Proposed Method

The Biometric Fusion Method Under Consideration

The proposed Biometric fusion technique, as illustrated in Fig. compares images using biometrics determine whether the camera has taken pictures that correspond to the image. To expedite execution process and minimize the number of iterations, the suggested approach first resizes the images to 256 × 256 dimensions. After that, the prewitt edge detection filter is used to define and clean the edges during the edge detection step. The Prewitt filter operates using a gradient-centred mechanism. In order to detect picture edges, it computes and estimates the gradients of image intensity . The corresponding gradient vector or the normal vector of an image pixel is what the Prewitt operator operates on. An improved Cellular Automata Segmentation process would be utilized following the application of a filter.

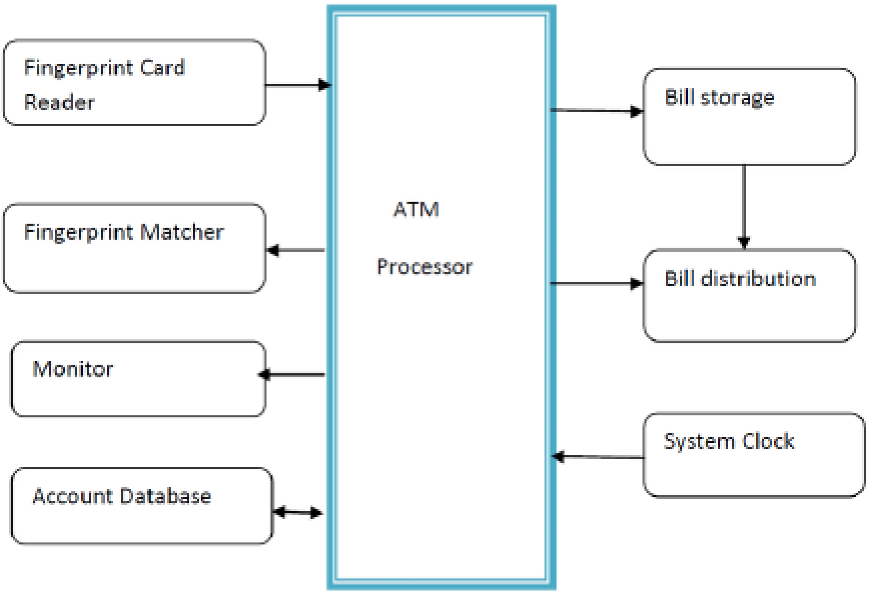

Figure 3.3 The Architecture of ATM Processor

The suggested system is an enhancement of the current one, and it runs without a card and PIN. The suggested system would only use biometric fingerprints; the user would use their fingerprints at the ATM, and if they match correctly, all of the banks they have accounts with would appear. The user would then choose which bank to transact with, choose the type of account they have with that bank, and then decide whether to withdraw money, check their account balance, and everything else. In order to secure ATM transactions using a biometric fingerprint, the customer must now decide which bank he wishes to withdraw* money from and indicate whether the account is a savings or current account.There are several benefits to this suggested technique over the current Card and PIN approach.

ADVANTAGES

1. Banks will spend less money purchasing ATM cards.
2. Patrons won't be carrying as many ATM cards as before.
3. Financial security will increase.
4. Every customer's bank account is connected to one another
5. You can stop worrying about malfunctioning cards, ATM card traps, and card theft.
6. With the new fingerprint PCS, online buying is also feasible.
7. Quicker than with conventional techniques

APPLICATION METHOD

The following is the procedure for the suggested system as described:

1. Obtain a fingerprint image.
2. Does the fingerprint match?
3. If so, go to step 5. Otherwise, GO To 2.
4. Continue with the bank transaction
5. Pick Banks.
6. CHOOSE Current or Savings Account Type.
7. Complete Your Cash Transactions.

Result

Hand geometry is a method that deals with the geometric structure of the hand including palm thickness,palm diameter,finger lenghs size and finger widths at various point.With the use of hand recognition technology, a machine can recognize every user individually, making the hand a crucial tool. This totally removes the possibility of fraud resulting from ATM card theft or fraud.We can protect our accounts from fraudulent attacks thanks to this technology. The banking sector will see far greater dependability from account holders. Additionally, a secure transaction will be accomplished.The use of fraudulent ATM cards to gain unauthorized access will be somewhat prohibited. Since this system relies heavily on hand identification, both bank employees and clients will be protected from all forms of infiltration.

Biometric Modality	**Accuracy**	**Coast**	**Size of templets**	**Long TermStability**
Facial Recognization	high	low	Small	Medium
Iris scan	high	high	Small	Medium
Hand Recognizatiom	**high**	**low**	**Small**	**Medium**
Finger Vein	high	Medium	Medium	high
Voice Recognization	low	Medium	Small	low

Conclusion and Future Work

The present study suggests that biometric systems, which facilitate transactions and do away with the need for swipe cards of any type, are a better and more dependable option for ATMs than traditional ones. One of the various biometrics used to identify people and confirm their identities is the fingerprint. Stability and dependability are derived from the user's fingerprint traits. Fingerprints are measurable physiological traits that confirm an individual's identification and enable the recognition of a registered person. The strong security characteristics needed for this suggested system are provided by the AES 256 encryption technique. The stenography method quadruples the level of security. When low-cost, memory-efficient biometric scanners become available, this system will be able to offer a novel, user-friendly, affordable.An increasing number of users require quick and precise user identification and authentication as a result of the rise in electronic transactions. Pins are often used as access codes for computers, bank accounts, and buildings. They serve as identity and security clearances. identity password or social security number, are not entirely trustworthy. Passwords may be ignored or hacked, cards may be misplaced or stolen, but an individual's biometric is inextricably linked to them. It is not readily forgeried, borrowed. Access is granted with the correct PIN, but the PIN holder is not validated. In the event that ATM and credit cards are misplaced or stolen, an unapproved Fingerprint Reader Power Supply.

References

1. C Kishor Kumar Reddy, Anisha P R, Samiya Khan, Marlia Mohd Hanafiah, Lavanya P, Madana Mohana R, “Sustainability in Industry 5.0: Theory and Applications”, CRC Press, Taylor & Francis, 2024
2. C Kishor Kumar Reddy, Anisha P R, Marlia Mohd Hanafiah, Srinath Doss, kari J Lipert, “Intelligent Systems and Industrial Internet of Things for Sustainable Development”, Sustainability in Industry 5.0: Theory and Applications, CRC Press, Taylor & Francis, 2024.
3. C Kishor Kumar Reddy, Pullisani Satvika, Marlia Mohd Hanafiah, Srinath Doss, “An Efficient early Diagnosis and Healthcare Monitoring System for Mental Disorder using Machine Learning”, Intelligent Engineering Applications and Applied Sciences for Sustainability IGI Global, 2023

4. Nuzhat Yasmeen, Kishor Kumar Reddy C, Srinath Doss, “Intelligent Systems Powered Hourly Attendance Capturing System”, 7th IEEE International Conference on Trends in Electronics and Informatics, Tirunelveli, India, 11-13 April 2023 DOI: 10.1109/ICOEI56765.2023.10125964.
5. Ramana Kadiyala, Madana Mohana, Kishor Kumar Reddy, Tippa Reddy G, “Block Chain Based Data Sharing System for Cloud Based Internet of Things Systems with Efficient Smart Contracts”, IEEE ICC 2023, Rome, Italy. DOI: 10.1109/ICCWorkshops57953.2023.10283747.
6. Leow, H.B. (1999). New Distribution Channels in banking Services. Banker's Journal Malaysia, No.l 10, 48-56.
7. Liu, N. Y. (2013). Bio Privacy: Privacy Regulations and the Challenge of Biometrics.
8. Oko, S. and Orah, J. (2012): Enhanced ATM security system using biometrics. UCSI International Journal of Computer Science Issues, 9(5), 352-357.
9. Ravikumar, S., Vaidyanathan, S., Thamotharan, S. &Ramakrishan, S. (2013), A new business model for ATM.
10. Rosenblatt, S. (2013). Two-factor authentication: What you need to know. Retrieved from: http://www.cnet.com/news/two-factorauthentication-what-you- need-to-know-faq/ last updated on April 14, 2014. Accessed on November 23, 2014.
11. Shoewu, O. and Edeko, F.O. (2011). Outgoing call quality evaluation of GSM network services in Epe, Lagos State. American journal of scientific and industrial research, 2(3), 409-417.
12. Siddique, M.I and Rehman, S. (2011). Impact of Electronic crime in Indian banking sector - An Overview Int. International Journal of Business & Information Technology, 1(2), 159-164.
13. Okokpujie K., Olajide F., John S. and Kennedy C.G., (2016). Implementation of the enhanced fingerprint authentication in the ATM system ssing ATmega128 with GSM feedback mechanism. Conference paper on Â banking in Nigeria.