Original Article

Secure Withdrawal From Atm Using Biometric Fingerprint

Princy Gupta[1*], Somya Garg[2], Dr.Jagbeer Singh[3]

[1*,2,3]Computer Science & Engineering Department, Meerut Institute of Engineering and Technology, Meerut

Corresponding Author: Princy Gupta

*Computer Science & Engineering Department, Meerut Institute of Engineering and Technology, Meerut
DOI: 10.47750/pnr.2022.13.S07.931

Abstract

Automated Teller Machines (ATMs) are a very convenient way to withdraw money wherever you are ATMs are in high demand because users rely heavily on their ATMs. But if someone has access to us, they can easily access our bank accounts. The only solution for ATM security is a 6-digit PIN. There are still many vulnerabilities that criminals can use to fraud customer data. To avoid such thievery and fraud, the actual creator embedded in the smart card A biometric identification system, and a database server are integrated. Under biometrics, we've got iris recognition, face recognition, and fingerprint recognition. By using these techniques, your account will be easily accessible and no one will be able to withdraw your funds illegally. This is designed to provide better security for ATMs. It is hoped that this method will minimize ATM fraud and allow customers to use their ATMs more safely. Based on previous implementations and test results, we are accustomed to improving the efficiency of fingerprint ATM scanner feature update speed, and the security framework has passed the test. The cause of this painting is to grow surety and safety and cast off the use of Automated Teller Machine credit score and debit cards.

Keywords: Biometric Authentication, ATM system, Security, Cards.

1. INTRODUCTION

Fingerprint integration into ATM system access control. Purpose of the framework for ATM systems with fingerprint authentication. The document has described various techniques and methods related to ATM security systems. Today, only one PIN is usually required for money transactions at ATMs. As you know, ATM systems are used to withdraw and deposit money, check bank balances, print bank statements and transactions, and more. Also, these actions require a PIN. Now, because of a boom in MITM (man-in-the-middle) assaults wherein messages are despatched from an "ATM Switch" to an "ATM host" and are tampered with through attackers to fraudulently take out cash, this PIN is for safety reasons. It's not right enough. Due to the current cyberattacks, all banks must build ATM security through end-to-end encryption within their networks. To cognizance of those points, we examined numerous studies and papers on strategies utilized in protection structures to enhance the protection degree and replace the charge of ATM structures and scanners. We are researching to refine the security of ATM systems in various kinds of techniques that can prevent fraudulent transfers and cyber-attacks. The biometric technology system uses company technology. Individuals must be registered or logged into the biometric authentication system. Their scheme combines cryptography and biometrics to increase security levels. we mainly focused on biometric authentication methods. The advent of the automated teller machine has had both positive and negative impacts on banking activity. An automated teller machine is a communication device. Customers can perform financial transactions such as termination of statements, transfers, and dips, in banks, human assistants, or employees. The personal identification number is an important essence of an ATM system detection or monitoring. PINs or OTP are widely used to keep client financial authorization secure and protected from suspicious access. A PIN is a major consideration for protecting your financial statistics. These PINs can be easily hacked. Biometric authentication can be used as a solution to this problem. Biometrics up to the minute deals with identifying individuals based on their physiological or behavioral manner.

The ATM usually consists of devices that control the user interface and transaction-related devices, as well as a smart card reader that identifies the patron, a pin, a steady crypto processor usually inside a steady shell, and a document printer that gives. The patron gives a document of transactions withinside the database. Some Needs are-

i.Easy access for the uneducated.
ii.If you lose your ATM card, no one will use or access it
iii.Block automatically.

Tasks which are performed in this project-

i.Biometric features are never lost or forgotten.
ii.Biometrics are hard to copy and share.

3. LITERATURE REVIEW

There is a serious issue with the ATM system. ATMs have emerged as much less steady due to the fact they're clean to trace. The security withinside the ATM gadget has now no longer been capable of dealing with the challenges. The proposed work involves security using fingerprints.

In ATMs, security is enhanced by fingerprint verification. In this document, fingerprint recognition is a biometric privacy system used to identify the holder of a specific bank account. In this system, if an ATM card is lost and an unknown person who knew this PIN received this ATM card. However, due to the fingerprint system, this unknown person cannot misuse this ATM card for the transaction. In, ATM security is enhanced by fingerprint recognition, even with PIN. Customers have historically used PINs to maintain ATM security. For secure transactions, fingerprint authentication is the best option. First, the customer has to register their fingerprint, and then an additional process is carried out. An ATM is designed so that after fingerprint verification, additional options appear on the screen

There are greater probabilities of lacking and misuse of ATM cards. The protection withinside the ATM has now no longer been capable of dealing with the challenges. It is viable to offer a far greater accurate and dependable consumer authentication technique by using fingerprint are:

i Users can use their fingerprints to make banking transactions.
ii Different human beings have different fingerprints. It is used for more accurate verification.
iii The User Identity and personal identification number are entered by the user.
iv The person can agree to continue with the transaction once they have tested their identity.
v The account will be blocked if there are three wrong attempts in a row.

This system was designed to propose this system in 3 ways :

1. To increase ATM security using fingerprints.
2. To provide highly secure identification.
3. To completely stop using ATM cards.

2. PROBLEM STATEMENT

In the past, cash withdrawals, cash deposits, and customer bank account details through banking were very difficult and tedious, but nowadays several banks have introduced electronic banking that allows customers to use the ATM because of the banking convenience involved in the above activities. Many banks around the world have installed ATMs in different locations/cities/villages/rural areas for bank customers to easily withdraw cash, check their balance and do all other ATM banking transactions.

4. PROPOSED TECHNIQUE OF THE PROJECT

The advanced system is an improvement over existing systems and does not require a card or PIN to operate.

The proposed system works only with a biometric fingerprint, the customer uses the fingerprint at his ATM and if the match is correct, the account is displayed in all the banks of the customer, the customer selects the bank of the transaction and selects your bank account type. then decided to withdraw and checked the balance.

Customers select the bank they wish to withdraw money from and indicate whether it is a checking or savings account. This is a means of securing her ATM transactions using biometric fingerprints.

A proposed system that introduces a fingerprint system to enhance security. The advantage of finger scanning technology is accuracy. Many drawbacks can be greatly reduced by using a fingerprint system. Those are things we don't need to wear.

ATM card in your wallet, there is no chance of losing it. CARD can be stolen and passwords can be shared.

Many customers are satisfied with our system for fast and excellent service. Also, save the fingerprint of the bank manager first. This is verified with the fingerprint you provided during authentication.

Unique authentication to confirm the identity of the person using the person's fingerprint, fingerprint, and PIN code, and to provide identification evidence by matching the person's data such as unique linkage with the PIN code. Finally, her entire fingerprint Automated Teller Machine framework can be described in her two stages:

Registration Stage

Validate Stage

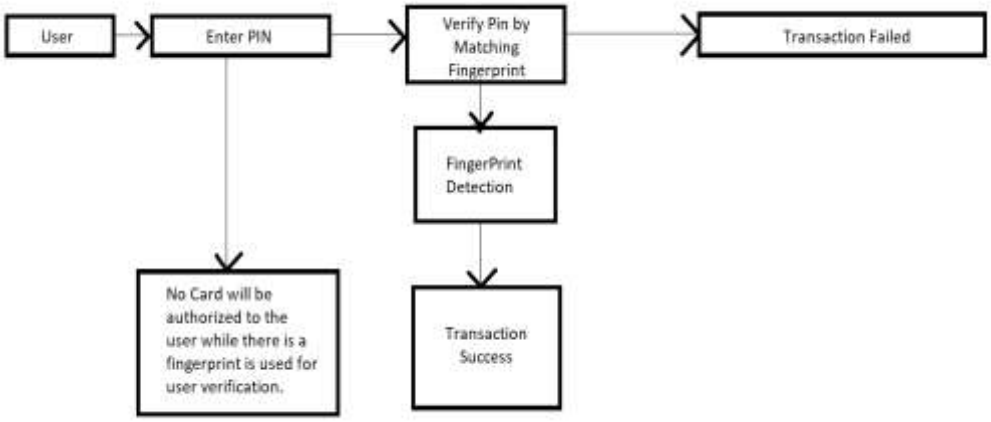
In this phase, customers are imagined to carry out transactions with their fingers. An individual should location their finger on a biometric scanner, and that individuals finger experiment is matched to a database that collects the fingerprints of all authenticated customers.

If a person desires to do banking, they can simply place their finger at the scanner and get their cash in no time. If the individual's fingerprint from the database no longer fits the random snip of the finger, a one-of-a-kind finger must be used. For your convenience, we additionally offer four PIN code options. Feature extraction: This manner from fingerprint snapshots is normally divided into 3 parts. This characteristic is meant for use to subdivide into main sample kinds together with loops.

This is the last interface a purchaser will interact with within the authentication process. Ask the purchaser to sign up their fingerprint into the fingerprint reader. A fingerprint reader takes your fingerprint and tries to suit the stay pattern with a

template already withinside the bank's database. If the fingerprint is decided to be correct, the purchaser proceeds to the exchange section where they pick out from exchange operations. Otherwise, the purchaser may be denied access.

Functionality



First, it authenticates by the PIN next to the fingerprint and then we perform the Transaction of the user successfully securely.

The functionality of the system will explain in the below steps.

Step 1: user enters the PIN.

Step 2: Entering PIN by user for further Processing.

Step 3: From the ATM, use no cards while using fingerprints for further authentication for the user.

Step 4: Verify PIN by checking if the fingerprint is matching or not by using the sensor.

Step 5: Enrol the fingerprint on a sensor. The user's fingerprint is already saved in the database. If authentication failure means the next step follows. If success means moving forward to the last phase.

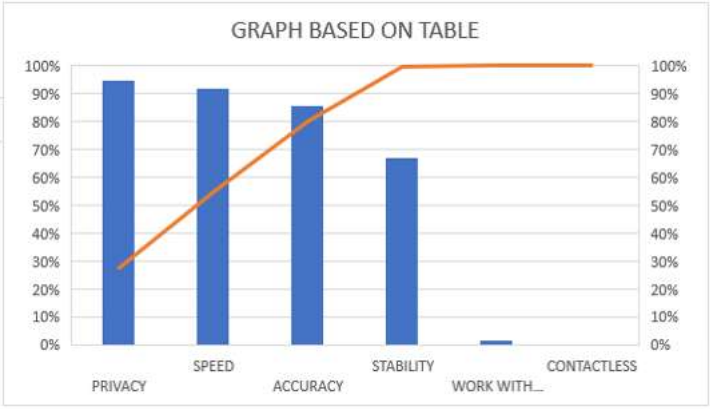
Step 6: When Fingerprint detect as per the Database user can finally withdraw their money from the ATM.

Step 7: Then the transaction begins after completion of the transaction the fingerprint will be removed from the sensor clearly while increasing the refresh rate of the fingerprint sensor for the user's protection and security.

Step 8: Then the withdrawal of money is a success by the user once it's matched the fingerprint from the database accordingly.

Table & Graph

BENEFITS	FINGERPRINT PERFORMANCE
STABILITY	67%
PRIVACY	95%
WORK WITH GLOVES	2%
ACCURACY	86%
CONTACTLESS	0%
SPEED	92%



5. USES

People use ATMs for transactions together with coins withdrawals, cash switches, and fees of energy and smartphone bills. ATM is the handiest to get the right of entry to the money owed and investment transactions.

6. ADVANTAGES

1. It will offer sturdy authentication.
2. One massive extrude integrated into the device, is the use of Biometrics. The consumer does now no longer ought to convey a separate ATM card to make the transaction. The consumer can sincerely make a transaction with the usage of his finger Using a Biometric is a mile greater steady device than the usage of a magnetic strip card, as each fingerprint is unique.
3. This device is simple to install, much less time ingesting and in the generally accepted biometric method.
4. The campaigner shopper is utilized therefore as critical the first consumer the nominee can get admission to the account just in case of emergency.
5. People are pressured to bear in mind numerous passwords. The biometric era does now no longer require using a PIN.
6. A major change that has been incorporated into the system is the use of biometric data. The user does not need to carry an ATM card to complete the transaction. The user can transact simply with their finger.

Using a biometric is a much more secure system than using a magnetic strip card since each fingerprint is unique.

Disadvantages

a. Once the PIN is forgotten, the card cannot be used.
b. A small scratch on the chips, the card is unusable.
c. The card can be stolen and the PIN can be hacked.
d. Card and PIN can be obtained at gunpoint.
e. The card will develop errors and may become corrupted if left in a wallet.
f. Money is not absolutely safe.
g. Cards can get caught in ATMs.
h. Customers with multiple accounts at different banks have multiple ATM cards.

7. EXPERIMENTAL RESULT DISCUSSION

As the frequency of ATM attacks increases around the world, different types of literature are proposing different technologies for enhancing ATM security. Various technologies have been proposed, such as facial recognition, fingerprint authentication, OTP authentication, and smartphone apps to prevent electronic theft.

Physical attacks can be prevented without using techniques by using temperature sensors, vibration sensors, tilt sensors, etc. Other technologies used include GPS and GSM technology.
Our main focus is end-users and people with low literacy. We created a simple login sheet using this method.

This registration sheet has two options. He or she uses a fingerprint and option card. Customers must use card selection and must select an option. Otherwise, they have to choose a different direction. After that, selecting a print of a finger, a person must put their finger into the scanner for recognition. Fingerprints must be recognized using a scanner. Their third step, following the second step, is a crucial one. The third step requires the customer to enter her PIN code correctly. All customers have a security number provided by their bank. After the customer correctly enters and submits the PIN, the customer provides banking services. If the customer enters the wrong number, they can enter only up to 3 times. The section below serves as the account transaction selection and selection section of the normal banking mechanism. So person's deal is the person's choice.

People have several options. The person needs to check his balance. Then the owner of the account has to withdraw money from the account and finally, they have to transfer money from one account to another and the the transaction is completed successfully.

(Fingerprint Scanner Tool [Hardware])

Other Biometric Fingerprint Examinations The advantage of using fingerprints to enhance ATM security is that it allows easy access, even for illiterate people. When the Automated Teller Machine card is misplaced, no one can access it, it can be automatically restricted and the Personal Identification Number code cannot be robbed or stolen by hackers. Hackers

that can occur at ATMs are becoming a major problem affecting bank customers and operators. Many people are skeptical about using ATMs because of related problems. Fingerprint mechanisms are the most proven and mature biometric authentication method, always easily accessible, and offering higher levels of protection at the touch of a button (picture). Fingerprint collection is shown along with other biometric data. Surveys show that all biometric systems have had great responses and success.

.

(Diagram of Fingerprint Results and Practical use of scanner)

This diagram explains what the fingerprint scanner scans. Fingerprint reputation structures scan by inspecting a finger pressed against a clean surface to verify account holders. A fingerprint scanner will play an important role in this project. Its sole purpose is that instead of ATM cards, fingerprint scanning is done for security purposes only. In this case, the person sticks the finger sensor and pulls it out, but if the fake person does this, the system will reject the operation, and if the authentication is easy, the operation will be completed successfully and continue with the next operation. I can do it. This helps users protect their accounts.

Code Screen

```
import cv2
import numpy as np
import os

fingerprint_test = cv2.imread("TEST_1.tif")
cv2.imshow("Original", cv2.resize(fingerprint_test, None, fx=1, fy=1))
cv2.waitKey(0)
cv2.destroyAllWindows()

for file in [file for file in os.listdir("database")]:
    fingerprint_database_image = cv2.imread("./database/"+file)
    sift = cv2.xfeatures2d.SIFT_create()
    keypoints_1, descriptors_1 = sift.detectAndCompute(fingerprint_test, None)
    keypoints_2, descriptors_2 = sift.detectAndCompute(fingerprint_database_image, None)

 matches = cv2.FlannBasedMatcher(dict(algorithm=1, trees=10),
            dict()).knnMatch(descriptors_1, descriptors_2, k=2)
   match_points = []

   for p, q in matches:
      if p.distance < 0.1*q.distance:
         match_points.append(p)

 keypoints = 0
   if len(keypoints_1) <= len(keypoints_2):
      keypoints = len(keypoints_1)
   else:
      keypoints = len(keypoints_2)

   if (len(match_points) / keypoints)>0.95:
      print("% match: ", len(match_points) / keypoints * 100)
      print("Fingerprint ID: " + str(file))
      result = cv2.drawMatches(fingerprint_test, keypoints_1, fingerprint_database_image,
                               keypoints_2, match_points, None)
      result = cv2.resize(result, None, fx=2.5, fy=2.5)
   cv2.imshow("result", result)
      cv2.waitKey(0)
      cv2.destroyAllWindows()
      break
```

Fig: sensor code

Output screens:

Fig 1: ATM pinboard

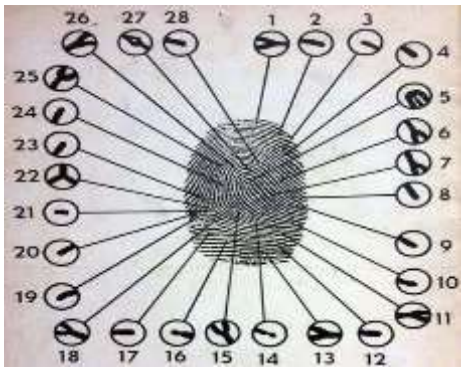


Fig 3: Fingerprint Structure

Fig 2: Fingerprint on sensor

8. CONCLUSION

This paper concludes that the traditional ATM device wishes to get replaced with Biometric structures where the transaction manner turns into easier, more reliable, secure, and casting off the want of wearing any form of swipe cards. Fingerprints are certainly considered one among many varieties of biometrics used to become aware of people and affirm their identification. It is primarily based totally on the traits of the user's fingerprint, like balance and reliability. Fingerprint permits the popularity of a registered man or woman via quantifiable physiological traits that affirm the identification of an individual. Biometrics offers more safety and luxury than traditional non-public identification methods. In some applications, biometrics can replace current generations or supplement them. Otherwise, that is an excellent feasible technique. Decision makers need to understand the difference between the volume of safety confidence through the approach of a biometric machine and the truth of her perceived and conveyed sense of safety. A biometric machine is one of the excellent components of the overall identification or authentication method, and exclusive components of that method play an equal characteristic in identifying its effectiveness. The variety one reason for imposing a biometric machine is to enhance not unusual place security. The maximum vital reason for introducing a biometric machine is to enhance not unusual place security. Performing ATM protection with the resource of the usage of inquiring for a fingerprint moreover has the conventional verification technique of coming into the consumer's fingerprint submitted with the resource of the usage of the administrator and efficiently verified. Much stepped forward protection for consumer identity power and robustness. A complete machine is built around a fingerprint machine, making the mechanism safe, reliable, and easy to use. It is said to be the cheapest era for digital or digital cash transactions.

9. REFERENCES

1. Oko, Selina, and Jane Oruh. "Enhanced ATM security system using biometrics." International Journal of Computer Science Issues (IJCSI) 9, no. 5 (2012): 352.

2. Preetam, I. Neenu, and Harsh Gupta. "Cardless cash access using biometric ATM security system." International Journal of Enhanced Research in Science Technology and Engineering 3, no. 11 (2014): 13-17.
3. Das, S. and Debbarma, J., 2011. Designing a biometric strategy (fingerprint) measure for enhancing ATM security in the Indian e-banking system. International Journal of Information and Communication Technology Research, 1(5).
4. Bhosale, S. T., and B. S. Sawant. "Security in e-banking via cardless biometric ATMs." International Journal of Advanced Technology & Engineering Research 2, no. 4 (2012): 457-462.
5. Gokul, S., Kukan, S., Meenakshi, K., Priyan, S.V., Gini, J.R. and Harikumar, M.E., 2020, August. Biometric-based smart atm using RFID. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 406-411). IEEE.
6. Shoniregun, Charles A., and Stephen Crosier. Securing biometrics applications. Springer US, 2008.
7. Siddiqui, Ahmad Tasnim, and Mohd Muntjir. "A study of the possible biometric solution to curb frauds in ATM transaction." IJASCSE, November (2013).
8. Sahar, Bayu Aji, Azel Fayyad Rahardian, and Elvayandri Muchtar. "Fingershield atm–atm security system using fingerprint authentication." In 2018 International Symposium on Electronics and Smart Devices (ISESD), pp. 1-6. IEEE, 2018.
9. Jaiswal, A.M. and Bartere, M., 2014. Enhancing ATM security using Fingerprint and GSM technology. International Journal of Computer Science and Mobile Computing (IJCSMC), 3(4), pp.28-32.
10. Padmapriya, V., and S. Prakasam. "Enhancing ATM security using fingerprint and GSM technology." International Journal of Computer Applications 80, no. 16 (2013).