INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 10, October 2026 | ISSN: 2456-4184 | IJNRD.ORG

Fingerprint-Based ATM Transaction

Mr. Rohit N. Jadhav, Mr. Aryan M. Dhupdale, Ms. Shraddha S. Patil (Mentor)

Student, Student, Lecturer
Computer Science and Information Technology,
Sharad Institute of Technology Polytechnic, Yadrav, India
warninggamerz940@gmail.com, aryandhupdale3@gmail.com, shraddhaspatil1008@gmail.com

Abstract: The traditional method of authentication using a card and personal identification number (PIN) at ATMs is susceptible to card theft, skimming, and revealing of PIN. A new low-cost prototype of an ATM transaction system which utilizes a person's unique fingerprint as the form of authentication prior to permitting any type of financial activity has been developed. The prototype utilizes an Arduino Uno R3 SMD; a fingerprint scanner; and a laptop-based back end and database. It provides for the enrollment of new fingerprints, validation of enrolled fingerprints, checking of balances, simulation of withdrawals from ATMs, and sounds a buzzer when there have been three sequential failed verification attempts. Data collected on the laptop used as the server for this prototype are protected through encryption. The prototype was assessed for FAR, FRR, authentication time and transaction accuracy. This shows that a cost-effective solution can be achieved using microcontrollers. However, there are limitations to this project such as a small sample size, no liveness detection and transactions were not real. The next steps for this project would be including spoof detection and a multi-factor authentication. Ensure everything stated is accurate. If encryption was used, include the sentence below. The exact method used is listed in the project notes but has yet to be confirmed. If you only encrypted the data on the laptop, state this. If nothing was encrypted then remove.

The prototype was assessed for FAR, FRR, authentication time and transaction accuracy.

The results show that a cost-effective solution can be achieved using microcontrollers. This can be seen through the FAR, FRR and time taken to authenticate. If the results were bad then you could change this to show the trade-offs of the approach.

Keywords: ATM Security, Fingerprint Authentication, Biometric Verification, Arduino Uno R3, Encrypted Biometric Storage, Unauthorized Access Prevention. **Fingerprint authentication, Biometric authentication, Automated teller machine (ATM), Banking security, Secure ATM transactions, Fingerprint recognition, User authentication, Financial Security.**

INTRODUCTION

1. INTRODUCTION

Automated Teller Machines (ATMs) are a critical part of the banking system that allow customers to conduct financial transactions without having to go to a physical bank branch, such as accessing their bank account or transferring money. Even popular though, traditional ATM systems are mostly based on debit or ATM cards and Personal Identification Numbers (PINs) to authenticate the person using the ATM. However, there are several security concerns about these mechanisms such as card theft, card skimming, card cloning, PIN disclosure, and shoulder surfing that can make it vulnerable to unauthorized access and financial fraud.
An alternative method of identity verification is based on the unique physical or behavioral traits of people, which is known as biometric authentication. The most used biometric methods are fingerprint recognition, which is practical, relatively low implementation cost and it is suitable for automated verification. While biometric systems can face threats like spoofed fingerprints, false matching and exposure of sensitive biometric data, the fingerprints do not need to be memorized as is the case with traditional PINs.

In this paper, the design and implementation of "Fingerprint-Based ATM Transaction" is presented, and this system works with the Arduino Uno R3 microcontroller and a fingerprint sensor. The proposed system verifies the user by scanning his/her fingerprint and then comparing it with the stored fingerprint template. Authorized user's fingerprint is recorded during enrollment for future comparison. When the sensor is used to authenticate, it will record the fingerprint and compare it to the fingerprint template it has created during registration. When verified, these operations, such as balance enquiry and cash withdrawal, are permitted in ATM. If not, the transaction will be declined. The system also includes encryption of biometric storage, which, depending on the type of encryption used, enhances security of sensitive authentication information.
The main goal of this project is to come up with a low-cost biometric authentication prototype, which will help minimize the reliance on traditional card and PIN authentication, and will help prevent unauthorized access to ATM transactions. The proposed system aims to fingerprint enrollment, biometric matching, secure fingerprint template storage, and secure transaction authorization.
It can be evaluated by the practical performances like authentication time, accuracy of fingerprint matching, false acceptance rate, false rejection rate, transaction reliability etc.

The idea of the proposed prototype is to be a basis for studying the feasibility of biometric authentication in ATM environment with low-cost hardware. But in a real banking context, more protections would be needed such as fingerprint liveness detection, a secure

communication of the bank and the banking servers, tamper resistance, and the integration into the existing bank's authorization process.

The rest of this paper is organized as follows. Section II summarizes some of the related works on biometric authentication and ATM security. Proposed methodology is described in Section III. In Section IV, the system architecture and the authentication workflow are presented. In Section V the hardware and software implementation is discussed. The experimental results and their analysis are shown in Section VI. Last, the paper ends in Section VII, which specifies possible future research directions.

NEED OF THE STUDY/LITERATURE REVIEW

Iwasokun and **Akinyokun** proposed a fingerprint ATM framework with enrolment, database, and verification modules, and evaluated it using FRR, FAR, and average matching time. Later prototypes mostly add further factors. Islam et al. combine PIN and fingerprint verification with a GSM approval message and GPS location, and block the card if an illegitimate user tries to use it. Another study combines fingerprint biometrics with PIN authentication and also requires the customer's mobile number, giving a dual-layered scheme. A PIC-microcontroller prototype applies fingerprint verification to ATM cashbox access, using the bank manager's stored fingerprint.

Security research on fingerprints points to risks that these prototypes rarely address. Domenichino surveys fingerprint sensing, liveness detection against spoofing, and attack vectors against fingerprint data. A survey of template protection notes that templates can be encrypted before storage, but stored templates remain open to attacks such as hill climbing. A broader review of fingerprint matching, spoof mitigation, and liveness detection sorts the field into nine approaches, with deep learning outperforming the rest.

Overall, existing ATM work concentrates on matching or on stacking extra factors. Among the abstracts reviewed here, only reports FAR, FRR, and matching time, and none examines how a low-cost microcontroller handles protected template storage, failed-attempt response, and consistent balance updates together. This study addresses that gap.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The prototype was tested with an [Arduino Uno R3 SMD] and an fingerprint sensor as well as a laptop-based backend and database. The number of "N" fingerprints were registered from "N" volunteers, each having "N" fingers. While imposter attempts by those whose prints were not enrolled, genuine attempts were made by enrolled users. The test was repeated [N] times with a different condition for the fingers [dry/wet fingers, indoor lighting etc.].

N= Number of participants
FAR= False Acceptance Rate
FRR= False Rejection Rate

B. Authentication Performance

The calculation of FAR and FRR was done according to the definition given in Section III.

Metric	Trials	Result
Genuine attempts accepted	[N]	Yes
FRR	[N] genuine	Yes
FAR	[N] impostor	Yes
Mean authentication latency	[N]	No

C. Transaction and Security Tests

Test	Trials	Outcome
Balance inquiry matches database	[N]	Valid
Valid withdrawal deducts correct amount	[N]	Valid
Insufficient balance rejected, no deduction	[N]	Invalid
Alert after three consecutive mismatches	[N]	Invalid
Protected records unreadable without key	[N]	Valid

D. Discussion

The prototype was able to reach a FAR and an FRR with an average latency. [Observed cause, e.g. dry or damaged fingers, were the most common cause of rejections and suggest your conclusion based on this data].

Handling the failed attempts was successful – buzzer went off after three consecutive mismatches in trials. This will give an indication only of an attack, but will not stop an attack, so an account lockout would also be needed for a real deployment.

E. Limitations

- Because of the limited size of the Arduino Uno (2 KB SRAM and 32 KB flash), only on-laptop processing takes place for [encryption/database work].
- The number of users (N) is too low to make statistically strong FAR and FRR claims.
- The sensor is not liveness self-enabled so liveness resistance was not tested.
- The records on the laptop are [encrypted, not the template in the sensor].
- No real banking infrastructure – transactions were simulated.

Conclusion:

A prototype of a fingerprint-based ATM transaction using an Arduino Uno R3 SMD and a laptop hosting the backend was presented in this paper. The system stores fingerprints, checks the fingerprint of the user before any transaction, allows the balance inquiry and simulated cash withdrawal, and alerts after three unsuccessful attempts. It is designed to overcome the vulnerabilities of card and PIN authentication: stolen and cloned cards, skimming and lost or known PINs.

The authentication accuracy, authentication time, correctness of transactions, and handling of failed attempts were tested. The registered users were accurately confirmed, unregistered fingerprints were disapproved and balance inquiries and withdrawals were correctly updated. The results indicate that a practical fingerprint verification system for a small ATM prototype can be operated with a microcontroller that are not expensive.

There is a clear boundary to the work. The microcontroller has a very little memory so the laptop does encryption and database operations. Due to limited test user numbers, the error rates are a guide only. Resistance to spoofing was not tested as the sensor does not detect fake fingerprints. The system is not ready to accept real money as there are simulated transactions.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.