iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6394

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Biometric ATM

Adrian Fernandes
MET Institute of Computer Science

Abstract: ***In the banking sector, there is an immediate need to improve security. With the emergence of ATM, banking has become much simpler, but it has become much more vulnerable. Owing to the exponential increase of 'intelligent' criminals every day, the chances of misuse of this much-hyped 'insecure' baby product (ATM) are manifold. Today ATM systems use no more than an access card and PIN to verify identity. The condition is unacceptable because considerable breakthroughs have been made in the techniques of bio-metric authentication, including fingerprinting, face recognition and iris scan. This paper suggests the implementation of a framework incorporating bio-metric technology into the process of identity authentication used in ATMs. Such a system will be designed to protect both consumers and financial institutions from fraud and other security breaches.***

I. INTRODUCTION

The growth of technology in India has put several forms of equipment into force which are aimed at more customer service. ATM (Automated Teller Machine) is one such system that makes money transactions simple for bank clients. The other side of this development is to raise the chance of the suspect to get his 'unauthentic' share. Protection is typically done by requiring the combination of a physical access card and a PIN or other password to enter a customer's account. This model encourages fraudulent attempts by stolen cards, poorly picked or randomly issued PINs, cards with little to no encryption systems, employees with access to unencrypted customer account information and other fault points.

II. LITERATURE SURVEY

The first ATMs were off-line machines, which means money was not immediately withdrawn from an account. The bank accounts were (at that time) not linked to the ATM through a computer network (The New York Times 1961). Thus, banks were very selective at first on who they gave ATM privileges to. Giving them only to holders of credit cards (credit cards used before the ATM cards) with clear bank (ATM Marketplace 2013). In modern ATMs, consumers authenticate themselves by using a plastic card with a magnetic stripe encoding the account number of the customer, and by entering a numeric pass code called a PIN (personal identification number), which can be modified with the computer in certain cases (BBC News 2010). Usually, if the number is entered incorrectly several times in a row, most ATMs would hold the card as a security precaution to deter an unauthorized user from using mere guesswork to work out the PIN (Telecommunications History 2008).

A. Problem Statement

Crime at ATM has become a wide-ranging notion problem that concerns not only customers but also bank operators and regularly rises the case of financial crime. Crime at ATM has become a wide-ranging notion problem that concerns not only customers but also bank operators and regularly rises the case of financial crime. Criminal customer steal card after illegally stealing the card 's criminal use of card details. The fraud involves Skimming card and Trapping money, as well as several other forms used in ATM fraud. Estimated ratio of ATM card related fraud is given in the table and Pie chart below.

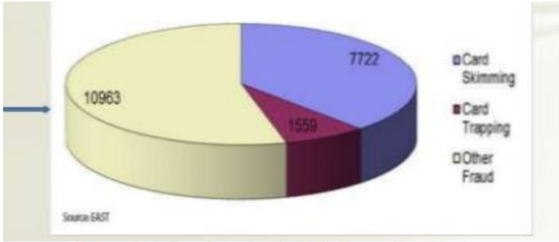


Fig -2: Pie chart of ATM card frauds

ATM Fraud's	Card Skimming	Card Trapping	Other Fraud
Fraud ratio	7722	1559	10963
Overall fraud ratio	20244	20244	20244

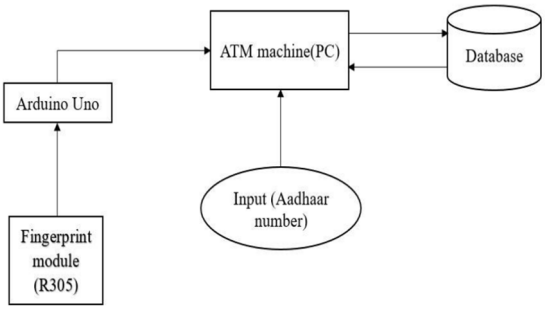
Table -1: sample table to estimate card fraud ratio

We may assume that the most common form of fraud is card skimming. Once a customer's card is lost and the password is stolen, the user's account could be hacked. We may provide ATM system authentication using debit cards, credit cards, smart cards and passwords or keys. If the credit card of the customer is compromised, there could be a risk that unauthorized users will also come with the right personal code to pick easily guessed pins and passwords that may be birthdays, phone numbers and social security numbers.

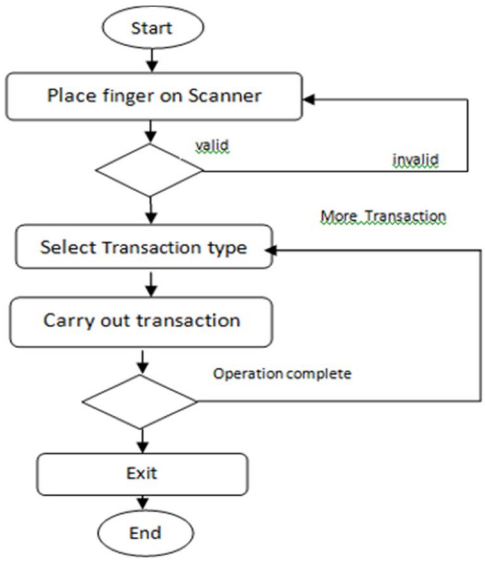
B. Proposed Methodology

The major issue in the ATM system is security. ATM machine access using PIN number has become less secure because it is easily traceable. It raised the risk of losing and misusing ATM cards. These challenges failed to address the existing security in the ATM system. The planned research includes biometric protection in order to address those obstacles. Especially fingerprint technology can provide a much more accurate and reliable method for authenticating users. This program requires users to use their fingerprint to make a banking transaction. For every human being the fingerprint minutiae features are different. Hence it is used to authenticate more accurately. The user enters the ATM card into the machine, then the machine asks for the fingerprint for user verification. The fingerprint is checked with the fingerprint data stored in the Aadhaar server. The fingerprint data is retrieved from the Aadhaar server based on the Aadhaar card which is linked to the user's bank account. The customer will be allowed to continue with the transaction after a biometric check. The account will be blocked if three consecutive attempts are made in error. This system has been developed to provide cost-effective banking ATM framework with Python-Database integration along with the use of hardware modules, Arduino as well as Fingerprint module (R305). Through this we have access to multiple banks and multiple accounts.

C. Functional Block Diagram



D. Activity Diagram for Customers Transaction



E. Disadvantages

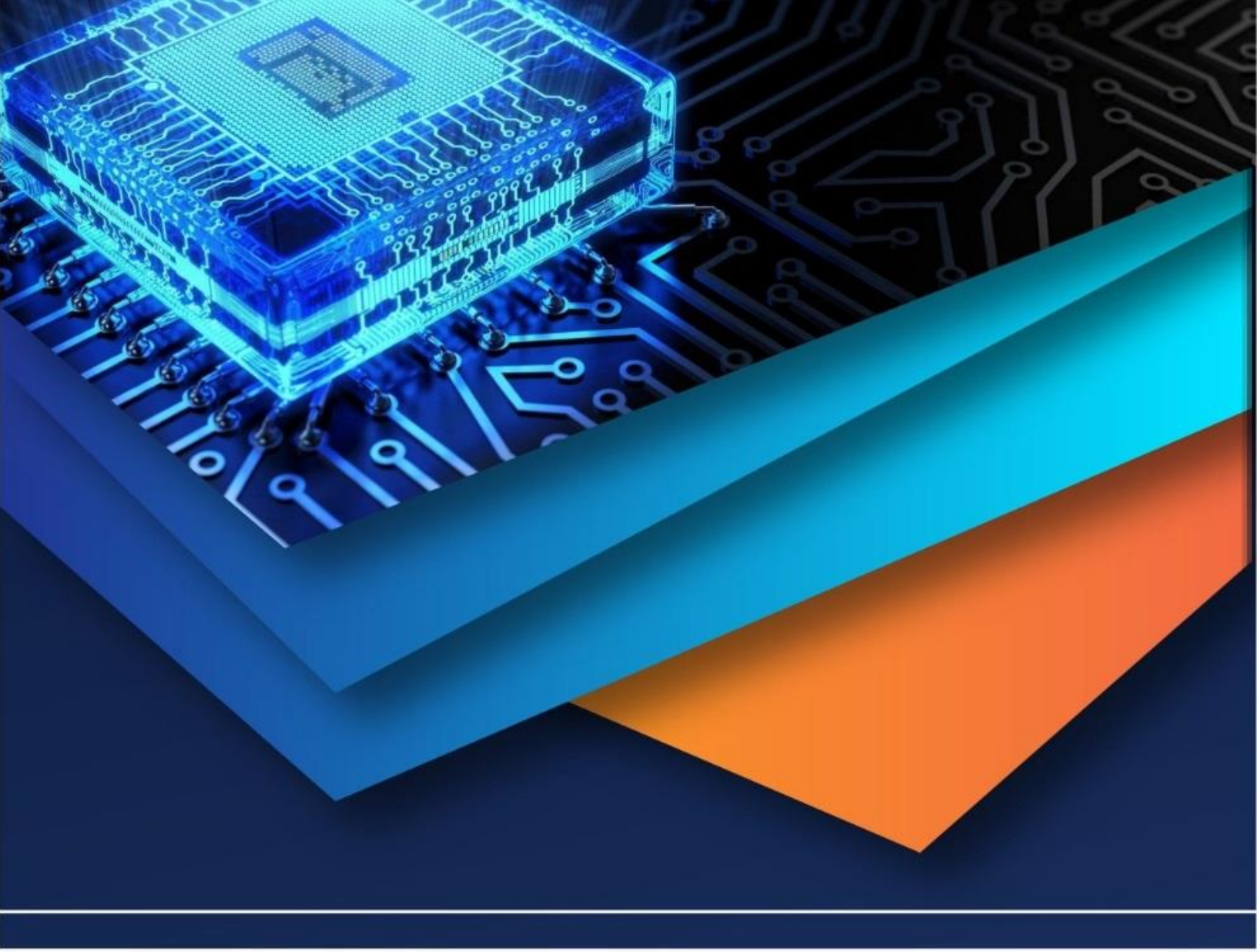
The amount of money spent and time required for implementing the system.
The error probability if the biometric server fails.
The original user of the account needs to be present to use the ATM machine. Any other member cannot use the account because of the biometric authentication.

III. CONCLUSION

ATM system improves bank organization's reliability by providing quick access to the cash transaction. Without waiting in queue, we can withdraw the cash anywhere and at any time. ATM card is still widely used but we have to face the ATM transaction-related fraud. We are using biometric scanning machine to identify the account holder to make ATM transaction more secure. Finger is every person's unique identity so we can avoid ATM related fraud by using the Biometric Fingerprint scanner. The Safety feature improved owner identification security and reliability. The entire system was designed using embedded system technology which makes the system safer, more reliable and easier to use.

REFERENCES

[1] Rishigesh Murugesh, "ADVANCED BIOMETRIC ATM MACHINE WITH AES 256 AND STEGANOGRAPHYIMPLEMENTATION", IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University,Chennai. December 13-15, 2012, 978-1- 4673-5584- 1/12/$31.00©2012 IEEE.
[2] Renee Jebaline.G, Gomathi.S, (2015) 'A novel method to enhance the se- curity of ATM using biometrics', International Conference on Circuit, Power and Computing Technologies.
[3] From punch card to prestaging: 50 years of ATM innovation. ATM Marketplace (2013-07-31). Retrieved on 2013-09-27.
[4] O.A.Esan and S.M.Ngwira "Bimodal Biometrics for Financial Infrastructure Security" I.O.Osunmakinde School of Computings, College of Science, Engineeringand Technology, University of South Africa, UNISA Pretoria, South Africa, 978-1-4799- 0808-0/13/$31.00 ©2013 IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY