Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint

Authors
Abhijeet S. Kale\textsuperscript{1}, Prof. Sunpreet Kaur Nanda\textsuperscript{2}

\textsuperscript{1}M.E 2nd year Dept. of Electronics and Telecommunication PRPCET, Amravati Maharashtra, India
\textsuperscript{2}H.O.D Dept. of Electronics and Telecommunication PRPCET, Amravati Maharashtra,
E-mail: abhijeetkales26@gmail.com, sunpreetkaurbedi@gmail.com

ABSTRACT:
This report focuses on building up a system that will increase the ATM security. Nevertheless, despite the numerous advantages of ATM systems, ATM fraud has recently become more widespread. The ATM will serve one client at a time. A customer will be required to insert a login id, validate his fingerprint and AADHAAR card, and then all will be sent to the bank for validation as part of each transaction. This progresses to the developed ATM software more secure as compared to the software that authenticates the user merely by utilizing a PIN or password.

Keywords: Fingerprint Verification, ARM7, AADHAAR card, GSM.

INTRODUCTION
An automated teller machine was first introduced in 1960 by City Bank of New York on a trial basis, the concept of this machine was for customers paying utility bills and get a receipt without a teller. Equally, we know that o'er the past three decades, consumers have been largely depending on and trust Automatic Teller Machine, known as an ATM machine to conveniently run into their banking needs. Using an ATM, customers can access their bank accounts in order to take in cash withdrawals, debit card cash advances, and mark off their account balances as well as purchase prepaid cell phone credit. With the convenient banknote trading is really coarse. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal a user's credit card and password by illegal means. In one case the user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring tremendous financial losses in customer.

Authentication methods for ATM cards have little changed since their first appearance in the 1960’s. Typically, the authentication design involves a trusted hardware device (ATM card or token). The card holder’s Personal Identification Number (PIN) is ordinarily the sole way to affirm the identity of the user.
The security limitations of ATM are mostly derived from the security pitfalls of the magnetic media. We tried to propose a prototype model for the same, which uses a PIN number along with the fingerprint verification scheme to verify the user before he can access his/her account and make the transactions. However, ATMs using a single layer of verification, i.e. biometric verification can also be developed using our prototype model.

RELATED REVIEW
Amurthy and Reddy developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers’ finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer places a finger on the fingerprint module it automatically generates every time different 4digit code as a message to the mobile of the authorized customer through a GSM modem connected to the microcontroller. The code received by the customer is recorded into the ATM machine by pushing the keys on the touch screen. After entering it checks whether it is a valid one or not and leaves the customer further access.

Mr. Aru et al. Suggests that ATM systems today use no more than an access card and PIN for identity verification. The recent advance in biometric identification techniques, including fingerprinting, retina scanning, and facial recognition has taken in a large endeavor to rescue the unsafe state of affairs at the ATM. This research looked into the evolution of a system that integrates facial recognition technology into the identity confirmation process used in ATMs. An ATM model that is more reliable in providing security by using facial recognition software is proposed. The development of such a system would serve to protect consumers and financial institutions alike from intruders and identity thieves. This report offers an automatic teller machine security model that would mix a physical access card, a PIN, and electronic facial recognition that will move as far as withholding the fraudster’s card. Still, it's obvious that man’s biometric features cannot be replicated; this proposition will go a long way to resolve the problem of Account safety making it possible for the real account owner alone have access to his stories. The combined biometric features approach is to suffice the purpose both the identification and authentication that card and PIN do.

AUTOMATED TELLING MACHINE
ATM stands for “Automated Teller Machine”. This machine allows the account holder to have transactions with their own accounts without allowing them to access the entire bank's database. ATM machine was invented by John shephhardbaren on June 1967 at Barclays bank in Enfield, United Kingdom. In India, Hong Kong and Shanghai banking corporation (HSBC) installed the first ATM in 1987. Indian bank 2and Citi bank introduced ATMs at various levels. For Asynchronous Transfer Mode, network technology based on transporting data in cells or packets of a specified size. The cell used with ATM is relatively small.
compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line. Or so people think that ATM holds the answer to the Internet, bandwidth problem, but others are doubting. ATM creates a specified channel, or route, between two points whenever data transfer starts. This differs from TCP/IP, in which messages are split into packets and each packet can take a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it arrives at it less adaptable to sudden surges in web traffic.

2.1 EXISTING ATM SYSTEM:
People utilize the ATM for transactions such as cash withdrawal, money transfer and payment of electricity and telephone bills. ATM is the most convenient to access the accounts and financing transactions. Personal Identification Number (PIN) is an important facet of the current ATM system in supplying security and it is a commonly employed method of protecting the transaction of one’s account. The PIN is a four digit number which is generated by the respective financial institution. The PIN is very easily remembered and is also changeable according to the user. But, sometimes PIN’s strength is decreased as the tracking of the code is increased. “Most commonly PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN.” In the existing system, the user has to insert the card and the PIN number. If the PIN is correct, the system allows for the transaction. Else, the system asks for PIN again and it allows maximum of three times to enter it.

Fig 1: Existing ATM System
PROPOSED SYSTEM

The purported plan is drawn up of hardware and software tools, the hardware used are FPM, Aadhaar card scanner, LCD, GSM module, all is interfacing with the help of ARM7 and the software is designated by the Keil µVision software.

![Block Diagram of ATM Security System Using Various Recognition Tools](image)

**Figure 2**: Block diagram Block Diagram of ATM Security System Using Various Recognition Tools

Proposed design methodology:

![Flow chart of proposed system](image)

**Fig 3**: Flow chart of proposed system
From the above flow chart 4.1, the main protocol of our scheme is providing a security with various biometric techniques. After entering into the ATM center, insert the card properly in the ATM system once it has been recognized by the system then it gives some option for languages. At one time it is selected, then it ask for password & verify it with the standard value stored in the bank server. If correct, then switch to the next, if not, then immediately message will be sent to the higher authority of bank & the nearest police station so transaction stop there; but if correct, then verify for “AADHAAR” card & same must be happening as above afterwards switch for the fingerprint, but if it is not authorized then message send to not only higher authority of the bank also with the nearest police station but if it is authorized then it will access the transaction. Then it asks for what to suffice? Means want to do: balance inquiry, withdrawal, etc., then in that respect must be transaction successful.

RESULTS & CONCLUSIONS
The Implementation of ATM security by using fingerprint & AADHAAR card recognition and GSM Modem took advantage of the constancy and reliability of fingerprint & AADHAAR card characteristics. GSM Modem used for transmitting messages in an unauthorized mode to the nearest police station & higher authority of the bank. Additionally, the system also contains the original verifying method which was inputting owner's password which is sent by the controller. The protection features were enhanced largely for the dependability and stability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use.

ACKNOWLEDGMENT
I would like to thank my guide Prof. Sunpreet Kaur Nanda, P.R. Patil College of Engineering & Technology, Amravati. She gave me moral support and guided me in different matters regarding the topic. She had been very kind and patient while suggesting me the outlines of this project and correcting my doubts. I thank her for her overall supports.

REFERENCES