ATM PIN RECOVERY USING MACHINE LEARNING

BATCH NO:06

GIRISHA M V-310819104713

AISHWARYA M-310819104722

OBJECTIVES:

- Usually the user inserts the ATM card in the ATM machine and enters Personal Identification Number (PIN) for the transactions.
- If the user forgets the PIN and enters the wrong PIN then the ATM machine will provide two more attempts to enter the valid PIN.
- If the user fails to provide the correct PIN after three attempts, the bank server will block the ATM card of the user.
- Now user has to visit the bank to reactivate his/her ATM card, which is time consuming,

1) To avoid the user to visit the bank and do the formalities to reactivate his/her ATM card.

2) To activate the ATM card of the user at the ATM centre itself with the help of finger print of the user.

3) To alert owner of the ATM card in case of misuse.

ABSTRACT:

- ATM (Automated Teller Machine) is an electronic telecommunication device that is used to perform financial transaction without need for human clerk or bank teller.
- ATMs extend traditional banking hours by dispensing cash and making other transaction available 24 hours a day. In ATM machines, the user is identified by inserting an ATM card and authentication is provided by the customer entering a PIN. The PIN provided to the customer is compared with recorded reference PIN number in the bank server. 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. Otherwise, the system asks for the PIN again and it allows maximum of three times to enter it. After 3 trials the ATM card will get blocked.
- To reactivate the card user need to visit the bank and do the bank formalities, which is tedious and time consuming job.
- Biometrics is the science of establishing the identity of an individual based on physical, chemical or behavioral attributes of a person. Fingerprint is a pattern of ridges and valleys on the surface of a fingertip. It often used for biometric identification. Fingerprints are detailed, nearly unique, difficult to alter and durable over the life of an individual. To reactivate that ATM card in the ATM center itself we are using fingerprint biometric.
- Fingerprint scanner identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, and MEMS. Optical scanners take a visual image of the fingerprint using a digital camera. Capacitive or CMOS scanners use capacitors and thus electrical current to form an image of the fingerprint.

SYSTEM REQUIRMENT:

- HARDWARE REQUIREMENT:

  RAM: 4GB

  Fingerprint scanner with USB cable

  Processor: Intel core-i5, 64-bit

- SOFTWARE REQUIREMENT:

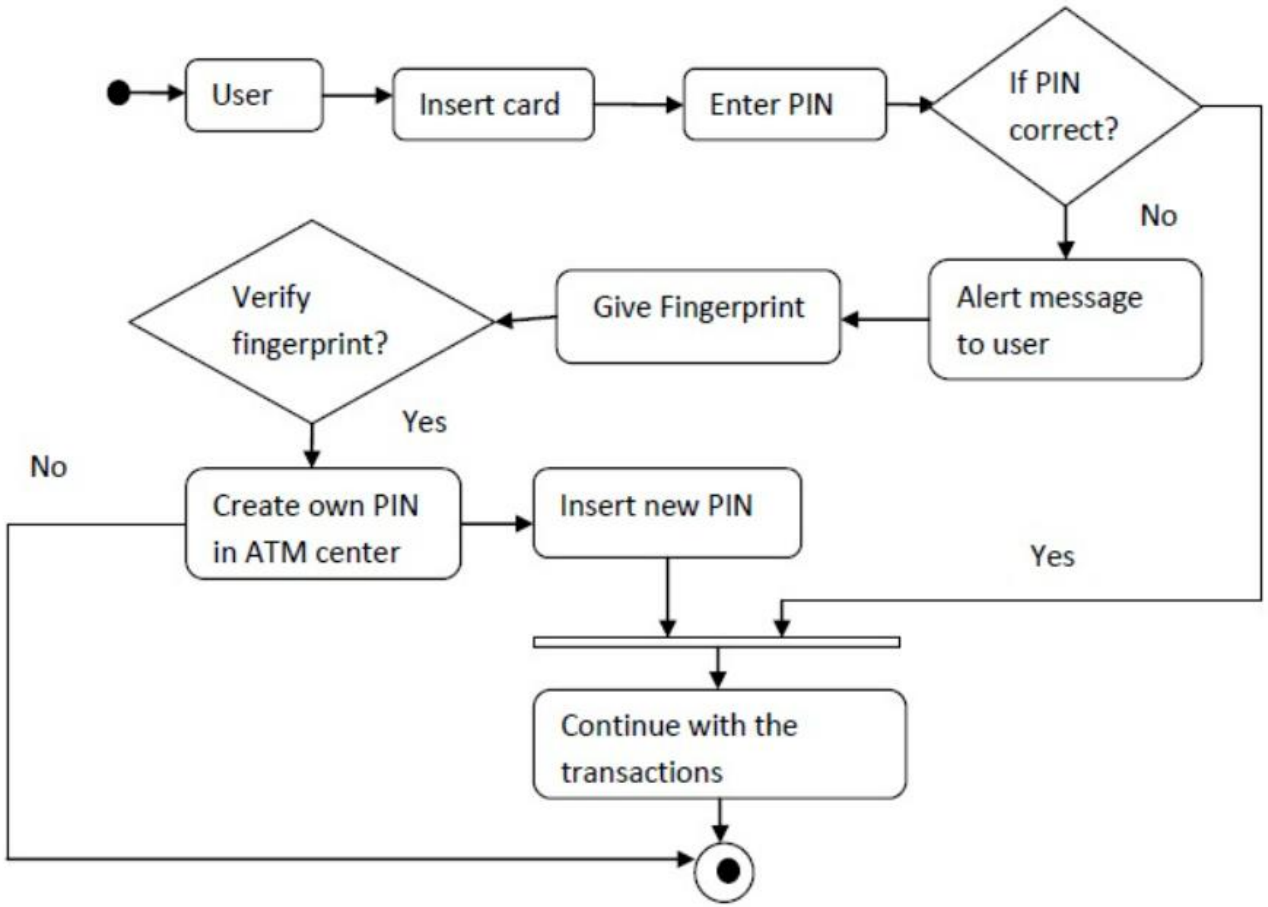
  OS: Windows 7 & above

- LANGUAGE USED:

  Java

  Python

OVERALL ARCHITECTURE:



LITERATURE REVIEW:

S.NO	Title of project	Author Name	Algorithm and Methodology used	Advantage	Disadvantage
01.	Smart ATM Pin Recovery and Secured ATM Transactions Based on Fingerprint Identification	MS.ANKITA SHETTY	The proposed methodology is based on identification of fingerprint of the ATM user. If the user enters the invalid PIN for three times, an alert message will be sent to registered mobile number and also a pop-up window will open on the ATM machine.	• TIME EFFICIENCY • SAFETY • EASILY ACCESSIBLE	• TRANSACTION PROBLEM • LACK OF MONEY IN ATM

MODULES IDENTIFIED:

Exisiting module	Problems detected	Researches	Solution
PIN based verification is mostly done in the automatic teller machine transactions. Enhancing this security, user authentication process is an important activity.	The major problems include shoulder-surfing attacks, replay attacks, card cloning and PIN sharing.	Multiple researches have also been conducted to create systems supporting card-less transactions. These are getting popular, where users can use additional personal devices, such as mobiles phones, to perform atm transactions. Shoulder-surfing attacks, also known as observation attacks, are most common threat for ATM authentication.	The developed system is able to authenticate the user based on fingerprint identification. The system is able to send an alert message to ATM card owner for entering the wrong PIN. The alert message is also sent to the owner of the card upon successful creation of new PIN.

THANK YOU