VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering (SCOPE)
M.Tech – Software Engineering (5 Year Integrated)
Fall Semester 2022-23

November, 2022

A project report on

FINGERPRINT BASED ATM SYSTEM

Submitted in partial fulfillment for the J Component project of

SWE2019 - Design Patterns

by

NIRANJANA O (19MIS1156)

SAHELI DAS (19MIS1164)

KHUSHI KANTULA (19MIS1186)

ABSTRACT

Fingerprint technology is quickly evolving these days. Fingerprint is a type of fingerprint that is used to identify people. In recent years, the fingerprint recognition algorithm has been continuously updated, providing new verification means for us. The original password authentication method combined with biometric identification technology verify the clients’ identities better and achieve the goal of using ATM machines to improve security. The fingerprint data is saved in a database via the Bank's enrollment process. Customers are given authentication by the bank, which they can use during the transaction process. If there is a fingerprint match in the database, the transaction will proceed. If the fingerprint does not match, the transaction will be cancelled. A user can make a safe transaction using a fingerprint-based ATM system. The main purpose of our system is to make online transaction more secure and user friendly.

PROBLEM STATEMENT

- In present scenario, the traditional ATM System accepts only on the pin code security system enabling the other person rather than the owner to access the account easily.
- Automates Teller Machine(ATM) fraud recent occurrence of ATM fraud include techniques such as shoulder suffering and card skimming steal user's credit card and password by illegal means use of ATM card duplicators inability to trace the wrongful users.
- To avoid this insecurity, Fingerprint based ATM system is introduced which is secured and authenticated.

OBJECTIVE

The objective of our project is to provide biometric security through fingerprint authentication in ATM applications. Also the experiments illustrate the key issues of fingerprint recognition that are consistent with what the available literatures say. The underlying principle is the phenomenon of biometrics "AUTHENTICATION", in this project we propose a method for fingerprint matching based on minutiae matching.

INTRODUCTION

Fingerprinting is a technology that helps to keep your data safe by making each user unique based on their physical traits. People's fingerprints, faces, pronunciation, iris, handwriting, and hand geometry, among other things, can be utilized to accurately identify them. Biometric identifiers provide various advantages over existing and traditional approaches. Passwords can be shared, forgotten, hacked, or mistakenly observed by a third party. Tokens such as magnetic stripe cards, smart cards, and physical keys can be stolen, lost, cloned, or left behind. A biometric system performs two primary functions. Identification is one way, while verification is another. In this work, we focus on using fingerprint recognition to identify and validate a user. A modern ATM is typically made up of devices such as a CPU to control the user interface and transaction related devices, a magnetic or chip card reader to identify the customer, a PIN Pad, a secure crypto-processor generally contained within a secure cover, and a display for the customer to use to complete the transaction. Function key buttons, Record Printer to provide the consumer with a record of their transaction, Vault to store portions of the machinery that require restricted access, Sensors and Indicators The most extensively used and mature biometric approach is fingerprint technology.

FEATURES:

- Login: User will login to the system using his fingerprint.
- Add Fingerprint: User has to add fingerprint in order to do transactions.
- Withdrawal of cash: User can withdraw cash by entering the amount he want to withdraw.
- View Balance: User can view balance which is available in his respective account.

ADVANTAGES:

- Fingerprint based ATM System is more secure than ATM card.
- User can make transaction using his fingerprint anywhere and at any time he need not have to carry ATM card.

DISADVANTAGES:

- If the User finger pattern has some cut or got damaged the system might not recognize the user.

LITERATURE SURVEY:

RBI 3X-Fingerprint Based ATM Machine (IJARCCE, Vol. 5, Issue 3, March 2016)

Nowadays security becomes a great issue in every part of life. Passing of information faces massive problems due to various types of attacks to the communication link. Many security algorithms are available to protect information from being hacked. The biometric authentication process adds a new dimension of security for any person sensitive to authentication.

This paper presents a secured and an energy efficient ATM banking system that is a highly secured system compared with the existing one. At present most of the ATM systems use triple data Encryption Standard (3DES). Which has some drawbacks; such as, it is vulnerable to differential attacks and also slow in performance. Issues in current ATM network: ATM Card frauds, use of ATM Card duplicators card sharing by family and friends, inability to trace the wrongful users, ATM PINs can be shared on phone or recorded using secret cameras. In this system 3 vital things are to be matched i.e. 6 digits unique code, fingerprint and 4 digit password. In this system, a 6 digit number will be given to every user. The second thing will be the users' fingerprint which will be detected by finger print recognition sensor. The third thing which is to be matched is the 4 digit pin code. The 4 digit pin code is the same concept which we are using nowadays for withdrawing money from ATM. The design of ATM systems based on fingerprint recognition took advantage of the stability and reliability of fingerprint characteristics, The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded systems which makes the system more safe, reliable and easy to use.

(a) Fingerprint module,(b)motor,(c)motor driver,(d)ATMEGA 16 Microcontroller,(e)Lcd (f)keypad .LCD is used in a project to visualize the output of the application.LCD can also used in a project to check the output of different modules interfaced with the microcontroller. Thus lcd plays a vital role in a project to see the output and to debug the system module wise in case of system failure in order to rectify the problem. Keypad is basically used to provide the input to the microcontroller. ATMEGA 16 has 16 Kbytes of InSystem Programmable Flash, Program memory with Read-While-Write capabilities, 512 bytes EEPROM, 1 Kbyte SRAM, 32 general purpose I/O lines, 32 general purpose working registers, a JTAG interface for Boundary scan, On-chip Debugging support and programming, three flexible Timer/Counters with compare modes. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

The security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded systems which makes the system more safe, reliable and easy to apply for better use. In these systems, bankers will collect the customer fingerprints and mobile number while opening the accounts then customer only access ATM machines. The design of ATM terminal system based on fingerprint recognition took advantages of the stability and reliability of fingerprint characteristics, a new technology which was designed for the sake of human beings when their ATM card is stolen, based on the image enhancement algorithm of Gabor and direction filter.

Fingerprint Based ATM System: Survey (IJIRSET Vol. 6, Issue 11, November 2017)

Biometric can be used to identify physical and behavioral characteristics of user fingerprints. There are many biometric devices like iris detection, face recognition, and fingerprint. In our Project, we are using fingerprint biometrics. Users' fingerprints are scanned using biometric traits and stored in a database. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. Fingerprint biometrics are easy to use, cheap and most suitable for everyone. Characteristics of fingerprints vary from person to person. Fingerprints are the unique identity of the user.

Data of a fingerprint is stored in a database using the enrollment process through the Bank. Banks provide authentication to the customer that can be accessed while performing the transaction process. If a fingerprint match is found in the database then a transaction takes place. After verification if fingerprint does not match, transaction will be cancelled. Using fingerprint based ATM system user can make secure transaction.

Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of the user such as pin code and fingerprint matching. Basically we can explain the complete Fingerprint based ATM system in two phases: 1) Enrolment Phase 2) Authentication phase.

Enrolment phase: In the robust fingerprint application, 3-4 fingers should be enrolled. This enables the system to set a high security threshold and still be able to cope with everyday real life issues like skewed finger placement, dirty, wet dry, cut or worn fingers. The Enrolment is crucial because the once recorded reference data will normally be used over the active lifetime of the user or his/her biometric hardware device. Multiple Finger enrolment: It is strongly recommended enrolling more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts not affect a robust sized sensor system.

Authentication Phase: In this phase users can make transactions by using their fingers. Users can place their finger on the Biometric scanner and the user's finger scan can be matched through a database, where all authenticated user's fingerprints are stored .If User wants to do a transaction they simply place their finger on biometric scanner and get their money in a few seconds. If a user's fingerprint cannot be matched by the database due to some accidental cuts on their fingers then they can use their other fingers and we will also provide a 4 pin code option, users can also use this option with their convenience.

ATM machines increase the reliability of the bank organization by providing easy access to the cash transaction. We can withdraw the cash anywhere and anytime without waiting in the queue. Hence, ATM cards are used wildly but we have to face the fraud related to the ATM transaction. To make ATM transactions more secure we are using a biometric scanning machine to identify the account holder. Finger is the unique identity of each person so using a Biometric Fingerprint scanner we can avoid ATM related fraud. The Security feature enhances stability and reliability of owner recognition .The whole system is designed by using technology of embedded systems which makes the system more secure, reliable and easy to use.

ATM Security using Fingerprint Authentication and OTP (IJERECE Vol 5, Issue 5, May 2018)

By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming devices, etc. In our proposed system, Bankers will collect the customer’s as well as respective nominee’s fingerprint and mobile number at the time of opening the account. The primary step is to verify the currently provided fingerprint with the fingerprint which is registered in the Bank’s database at the time of account opening. If the two fingerprints get matched, then a message will be delivered immediately to the user’s mobile number which is the random 10 digit pin number called as One Time Password (OTP). This OTP can be used only once, thus this avoids various problems associated with the present system. For every transaction, a new OTP will be sent to the account holder’s mobile number, thus there will not be a fixed PIN number for every transaction. Thus, PIN number will vary during each transaction assuring security.

Project proposes the idea of using fingerprint and OTP in ATMs as password instead of the traditional pin number. By using fingerprint recognition, the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. We also have an OTP feature along with the fingerprint authentication which will definitely not allow any criminal to use the password for any kind of fraud as the OTP is valid only once. Thus, it becomes useless for the next time even if any criminal gets hold of it. The main modules of a fingerprint verification system are:

a) fingerprint sensing, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation

b) Preprocessing, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction

c) Feature extraction, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors

d) Matching, in which the feature vector of the input fingerprint is compared against one or more existing templates.

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint scanning, continues to gain acceptance as a reliable form of securing access through identification and verification processes. This paper identifies a high level model for the modification of existing ATM systems using both Biometric fingerprint strategy and GSM technology. We have been able to develop a fingerprint mechanism as a biometric measure to enhance the security features of the ATM for effective banking. The developed application has been found promising on the account of its sensitivity to the recognition of the cardholder’s finger print as contained in the database. This system when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines.

Fingerprint Based Security System Format (IRJET Volume: 06 Issue: 06 | June 2019)

Biometrics is a technology that helps to make our data tremendously secure, distinguishing all the users by way of their personal physical characteristics. Biometric information can be used to accurately identify people by using their fingerprint, voice, face, iris, handwriting, or hand geometry and so on. Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. It is simple to install and also it takes little time and effort to acquire one's fingerprint with a fingerprint identification device. If an unauthorized person tries to login then, the user will be alarmed with the help of a buzzer which is linked with the controller. An authorized user is given 3 chances to re-enter the id if he/she forgets.

The system uses R305 fingerprint scanner to capture fingerprints. This system can be employed at any application with enhanced security because of the uniqueness of fingerprints. It is convenient due to its low power requirement and portability. Although fingerprint images are initially captured, the images are not stored anywhere in the system. Instead, the fingerprints are converted to templates from which the original fingerprints cannot be recreated, hence no misuse of the system is possible. In the verification, the system compares the input fingerprint to the fingerprint stored in the database of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares the input fingerprint with the prints of all registered users in the database to determine if the person is already known under a replica or false identity (1: N match).

Fingerprint images cannot be recreated from templates, hence no one can misuse the system. Speed of execution can be enhanced with the use of more sophisticated microcontrollers. The same hardware platform can be used with IRIS scanner to put forward another potential biometric security to the ATMs.

Securing Automated Teller Machine (ATM) TransactionUsing Biometric Finger print (AJER Volume-9, Issue-9, pp36-43, 2020)

A biometric system is a recognition system that allows personal identification by determining the authenticity of a particular physiological or behavioral characteristic of the user. This identification method is preferred to traditional methods that involve passwords and PINs for several reasons. Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral Characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost

The proposed system works with biometric fingerprint only, the customer uses fingerprint at ATM and if matched correctly, then all banks of the customer have an account with appears, the customer will select the bank to transaction with, then select the account type with that bank , then chose to withdraw, check account balance and so on.

Customer will now choose or select the bank he wants to withdraw money from and specify if the account is Current or Savings, this is a means of securing ATM transactions using biometric fingerprint.

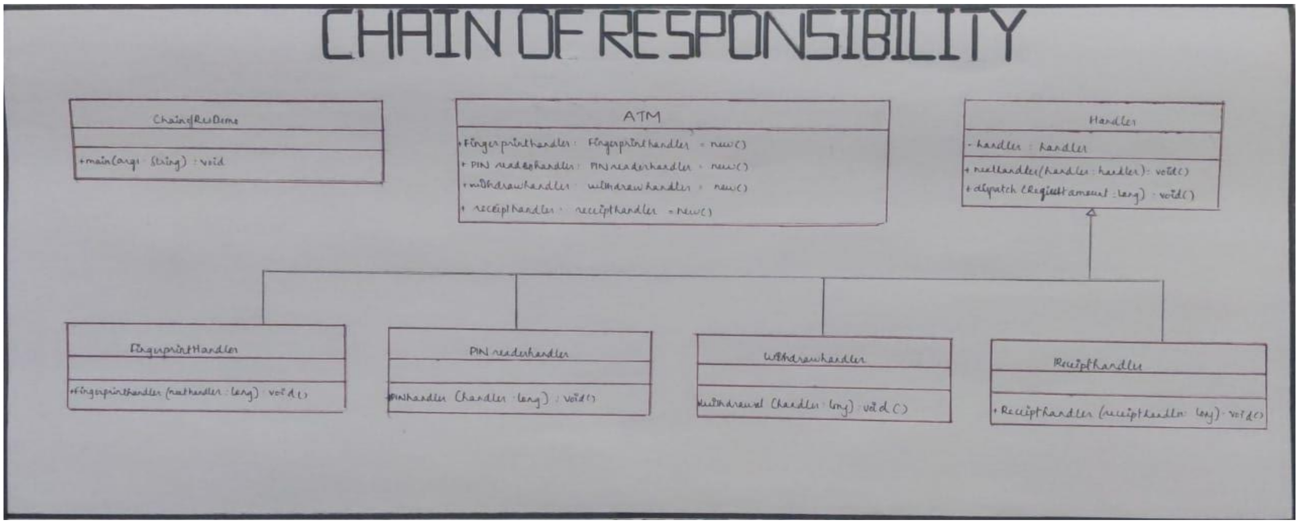
Conventional methods of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It cannot be borrowed, stolen or easily forged.

Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology using fingerprint identifiers may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. Biometrics is not only a fascinating pattern recognition research problem but, if carefully used, could also be an enabling technology with the potential to make our society safer, reduce fraud and lead to user convenience by broadly providing the following three functionalities (a) positive identification (b) large scale identification and (c) screening.

PATTERN RELATIONSHIP:

CHAIN OF RESPONSIBILITY PATTERN:

Chain of responsibility pattern is used to achieve loose coupling in software design where a request from client is passed to a chain of objects to process them. Then the object in the chain will decide themselves who will be processing the request and whether the request is required to be sent to the next object in the chain or not.

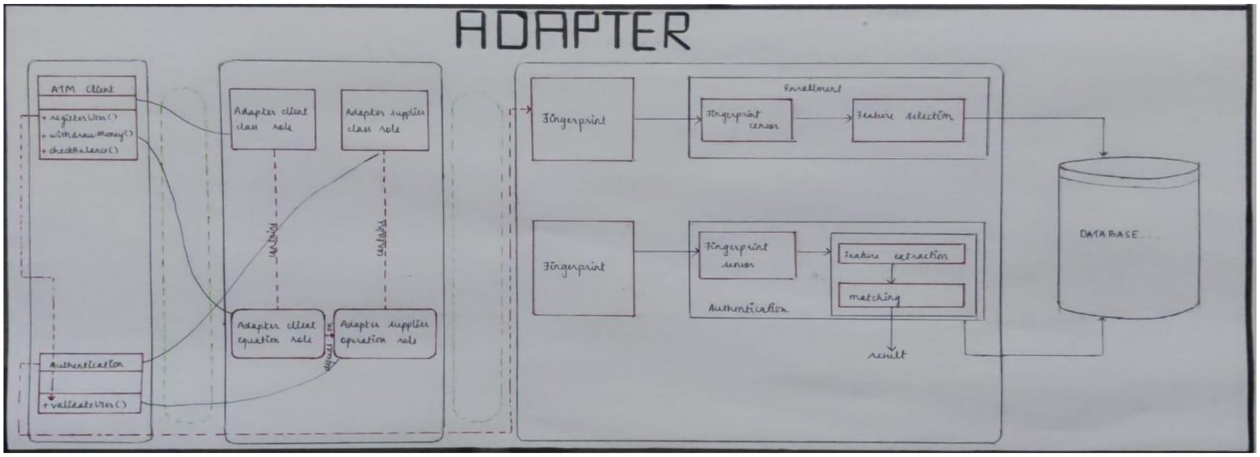

CHAIN OF RESPONSIBILITY
ChainofResDemo
+main(args : String) : void
ATM
+Fingerprinthandler : Fingerprinthandler = new()
+ PIN readerhandler : PINreaderhandler = new()
+withdrawhandler : withdrawhandler = new()
+ receipthandler : receipthandler = New()
Handler
- handler : handler
+ nexthandler(handler : handler) : void()
+ dispatch (Requestamount : long) : void()
FingerprintHandler
+Fingerprinthandler (nexthandler : long) : void()
PIN readerhandler
+PINhandler (handler : long) : void()
Withdrawhandler
withdrawal (handler : long) : void()
Receipthandler
+ Receipthandler (receipthandler : long) : void()

JUSTIFICATION:

The Chain of Responsibility pattern allows a number of classes to attempt to handle a request independently. The Receiver objects of the requests are free from the order and can be use in any order for processing. This pattern decouples sender and receiver objects based on type of request. This pattern defines a chain of receiver objects having the responsibility, depending on run-time conditions, to either handle a request or forward it to the next receiver on the chain. This pattern helps us avoiding coupling of sender and receiver objects of a requests and allows us to have more than one receiver as well for the request. It is suitable for our project because using different types of Loggers is possible in chain of responsibility. The ATM will apply the requested amount in each bucket and compare if it is need or not to process the final withdrawal. The chain of responsibility is this in theory. Creating several buckets of behavior that is loosely coupled to the end product. If the ATM didn't have money the whole system does not collapse, rather they are removed from the chain links. To implement this pattern we need to create an abstract handler that outlines the handler request behavior and points to the next handler in the chain of operations. Each concrete handler implements the abstract Handler with the required processing (+HandlerRequest()) for that handler. Once the request is handled by each concrete handler in the chain the results are sent to the next handler successor. The Chains Pattern allows us to create a stream of workflows across several classes without hard coding specific dependencies.

ADAPTER PATTERN:

The adapter pattern is a structural pattern that converts the interface of a class into another interface that a clients’ wants. The role types in the adapter pattern are class and operation. The class roles are the adaptee class and the client class. The operation roles are the operation in the adapter client class that needs the service, and the service operation in the adaptee supplier class.

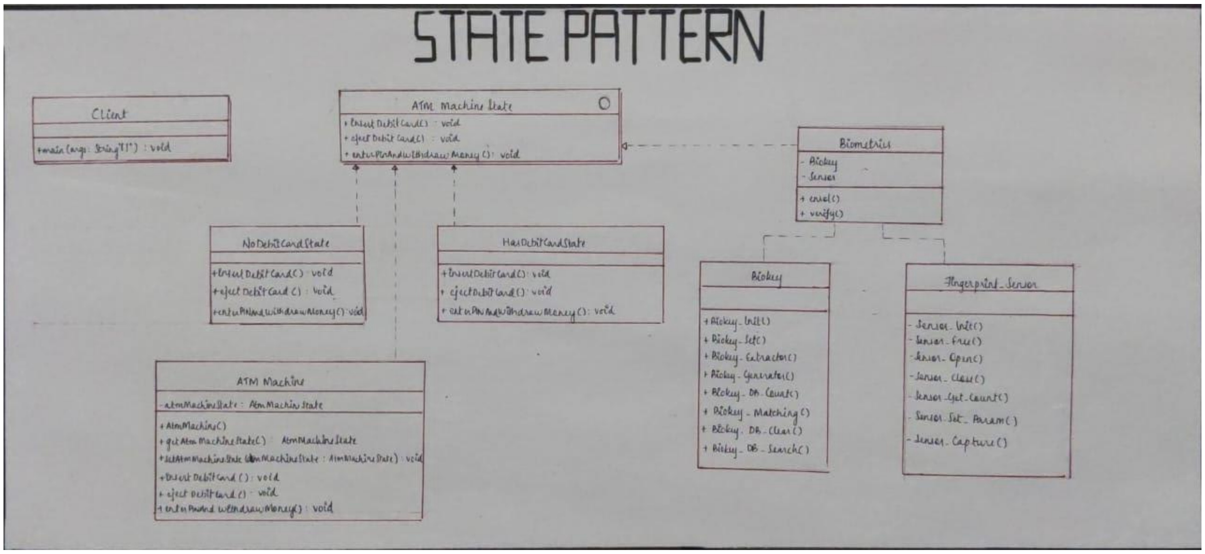


JUSTIFICATION:

Adapter pattern allows the changing of the interface of a service provider without affecting the clients, by introducing a wrapper class between the client and the service provider.In the future the provider of authentication services may change, and a new authentication component may have different interface, although it provides the same logical services. The Adapter pattern can be applied to make the rest of the system independent of the interface of the authentication component. This makes it possible to change the authentication component without touching the clients. By changing the authentication component, it is enough to introduce an adapter component that translates the calls according to the new interface.In this project, the pattern constraints are obtained directly from the preconditions of the pattern, so adapter pattern is used. Adapter is supposed to be applied only for COTS components, or that messaging is allowed only for certain types of components. Adapter pattern is applied by binding the roles of patterns to the elements of the initial design. The binding can be made only if the preconditions of the pattern hold when applied to the bound elements.

STATE PATTERN:

State pattern is one of the behavioral design pattern. State design pattern is used when an object changes its behavior based on its internal state.

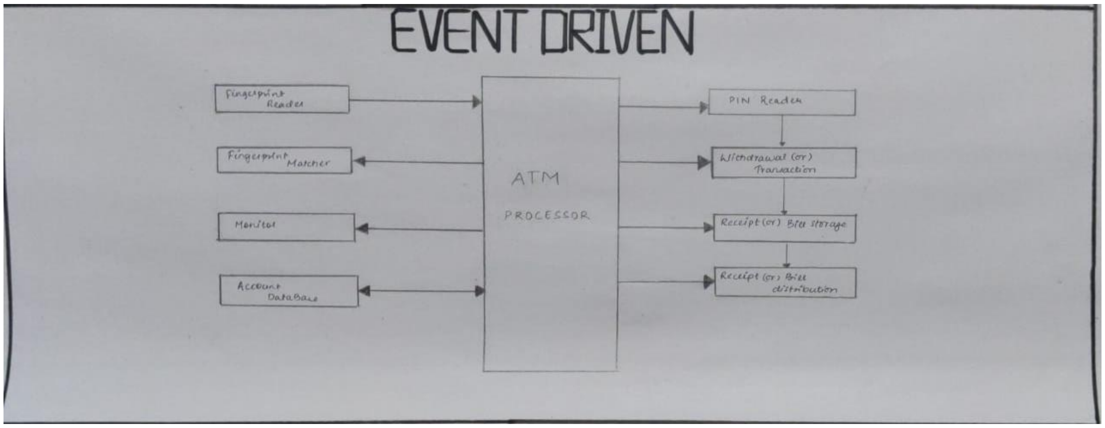


JUSTIFICATION:

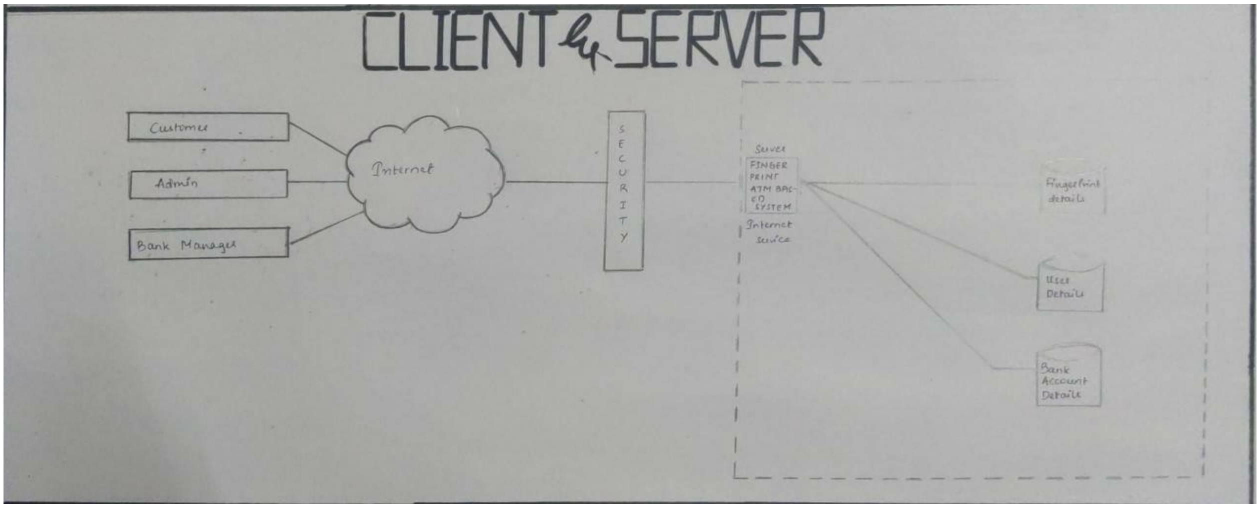
The State pattern suggests that we create new classes for all possible states of an object and extract all state-specific behaviors into these classes. Since ATM class functions as a finite-state machine, we can incorporate the State design pattern. For every state-transition, the reference to the specific state class is modified. In state pattern, coupling of states is eliminated and a new state can be easily defined and plugged into the existing state with minimal change. The individual states will process the command and perform a state transition by resetting the state in the context.

ARCHITECTURE DIAGRAMS:

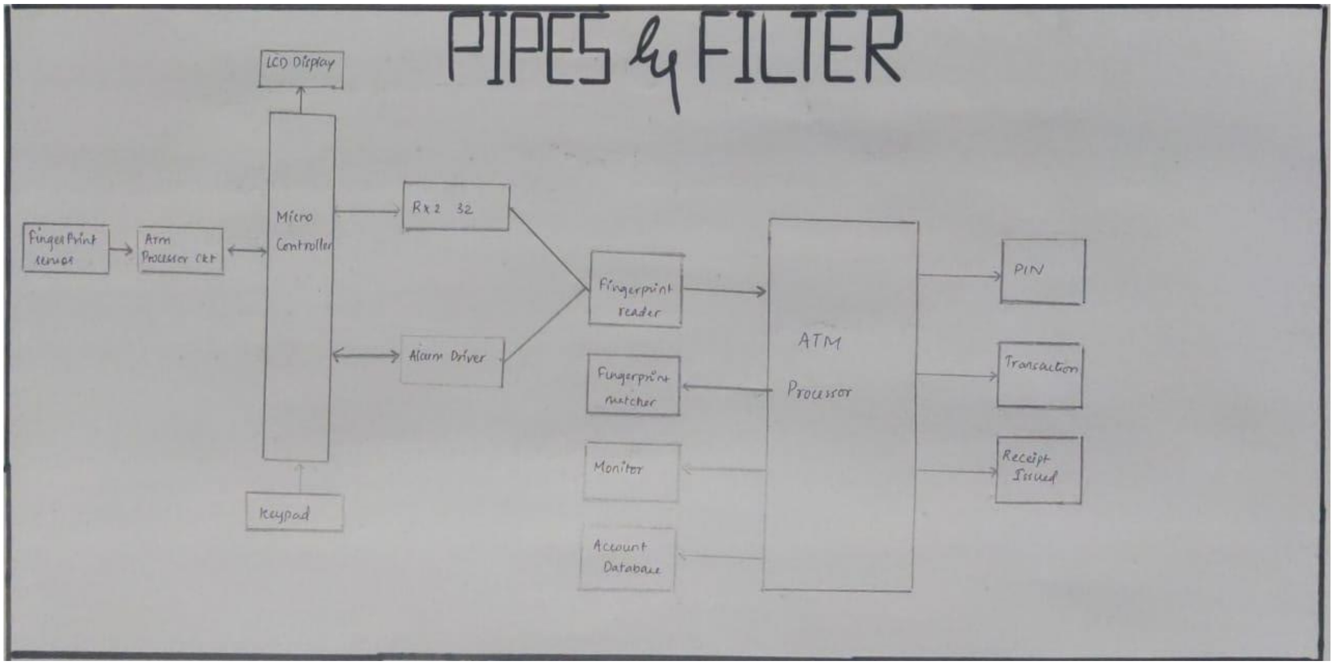
Event Driven:



Client Server:



Pipes & Filter:



CONCLUSION:

The implementation of ATM protection using fingerprints includes the standard ways of inputting the client's fingerprints, which are then sent by the administrator and double-checked. For the strength and stability of the client's identity, the protection function was greatly increased. The entire system is based on a fingerprint method, making the mechanism safe, dependable, and simple to use. In electronic or digital money transactions, this will be the most advantageous technology.

REFERENCES:

- Bharti Patil , Bhagwan S. Chandrekar , Mahesh P. Chavan , Bhavesh S. Chaudhri; RBI 3X-Fingerprint Based ATM Machine, IJARCCE Vol. 5, Issue 3, March 2016.
- Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha; Fingerprint Based ATM System: Survey, IJIRSET Vol. 6, Issue 11, November 2017.
- Aruna R, Sudha V, Shruthi G, Usha Rani R, Sushma V; ATM Security using Fingerprint Authentication and OTP, IJERECE Vol 5, Issue 5, May 2018
- Steffy Mathew, Mohammed Arshak C, Muhammed Ajmal KP, Mohammed Fazil KK, Honey Susan Eldo; Fingerprint Based Security System for ATM, IRJET Volume: 06 Issue: 06 | June 2019.
- URANG Awajionyi S. and Ojekudo Nathaniel A; Securing Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint, AJER Volume-9, Issue-9, pp-36-43.
- Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha
- U.G. Student, Dept of Computer Science Engineering, JIT College, Lonara, Nagpur, India U.G. Student, Dept of Computer Science

Engineering, JIT College, Lonara, Nagpur, India Assistant Professor, Dept of Computer Science Engineering, JIT College, Lonara, Nagpur, India

CONTENTS OF REVIEW 2 and REVIEW 3 PPT

REVIEW 2	**REVIEW 3**
Problem Statement	Problem Statement
Patterns and its Justifications:	Abstract
Chain of Responsibility	Introduction
Adapter	Objective
State Pattern	Features
References	Advantages and Disadvantages
	Patterns:
	Chain of Responsibility
	Adapter
	State Pattern
	Conclusion
	Future Work
	References

CONTRIBUTION:

Niranjana O (19MIS1164):

Problem statement, Features, Advantages & Disadvantages, Chain of Responsibilty Pattern, Pipes & Filter.

Saheli Das (19MIS1164):

Abstract, Objective, State Pattern, Literature Survey, Client-Server

Khushi Kantula (19MIS1186):

Introduction, Conclusion, Future Work, Adapter Pattern, Event Driven