Fingerprint Authentication for ATM

BY:-
Parul Varshney – 0919213069
Paras Garg – 0919213067
Upendra N. Giri – 0919213121

G. L. Bajaj Institute of Technology, Gr Noida
Major Project

CONTENT

PROBLEM STATEMENT

- In present scenario, traditional ATM system accepts only on the PIN CODE security system, enabling the other person rather than the owner to access the account very easily.

- This ensures that the traditional ATM system is not fully secured.

OBJECTIVE

- The objective of our project is to provide biometric security through fingerprint authentication in ATM application.

- The underlying principle is the phenomenon of biometrics “AUTHENTICATION”, in this project we propose a method for fingerprint matching based on matching algorithms.

INTRODUCTION

- The fingerprint is a person's most unique physical characteristic.
- This software can pick only authentic fingerprint out of crowd, extract that fingerprint is compared from rest of which those are stored in database.
- Fingerprint recognition software is based on the ability to first recognize fingerprint, in this technological fingerprint measure the various features of each fingerprint.

What Fingerprint Is?

- A fingerprint is the feature pattern of fingers (Figure 1), and each fingerprint is unique, and every person has unique fingerprints. So fingerprints have being used for identification.
- A fingerprint is composed of many ridges and furrows, fingerprints are not distinguished by their ridges And furrows, but by Minutiae, which are some abnormal points on the ridges (Figure 2).
- Two types of minutiae are called termination, which is the immediate ending of a ridge and the other called bifurcation, which is the point on the ridge from which two branches derive.

Figure 1

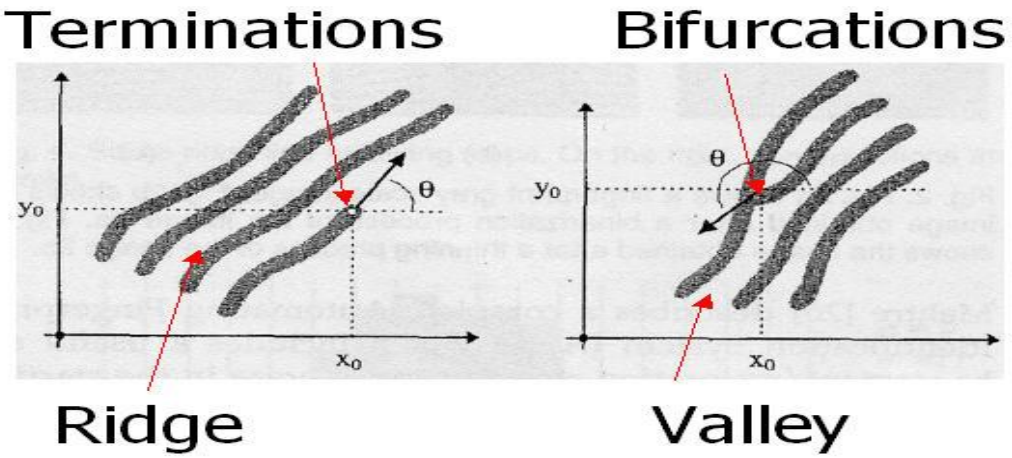
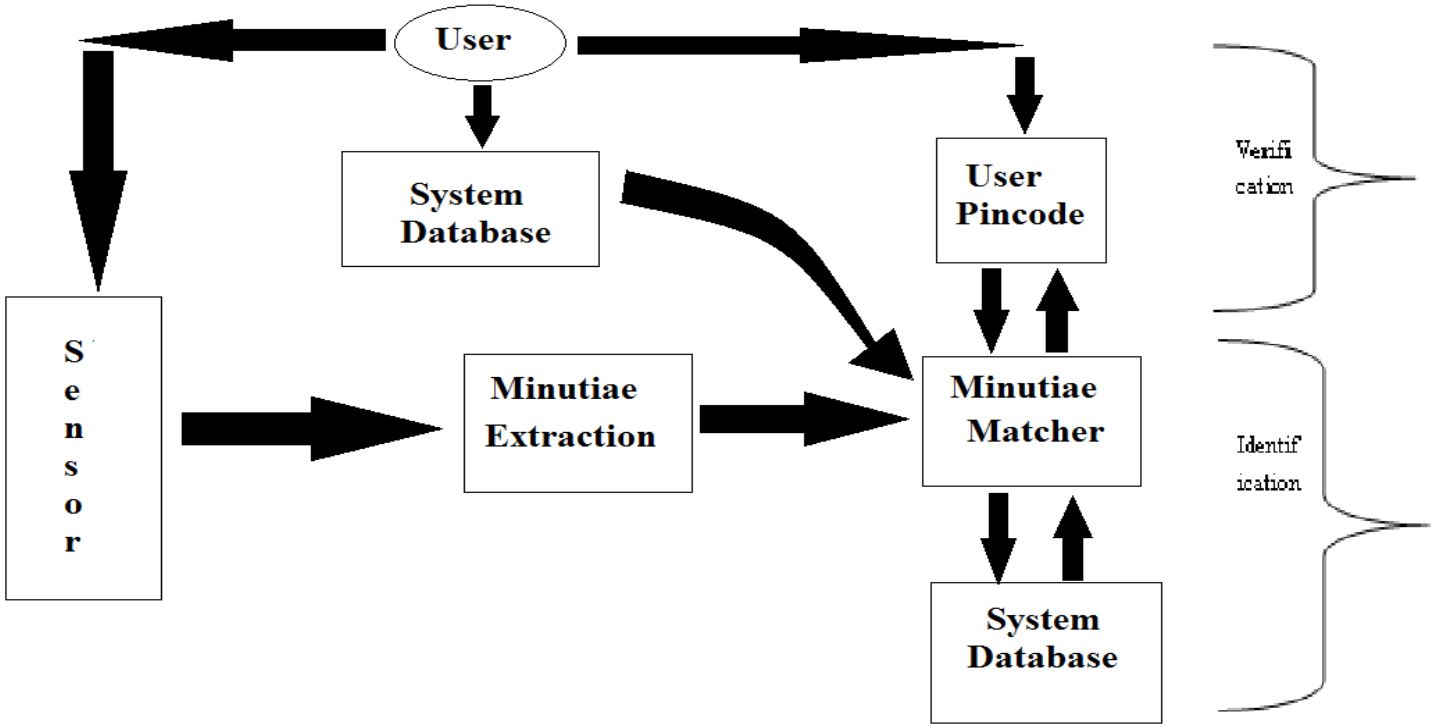


Figure 2

What is Fingerprint Authentication?

- The fingerprint authentication problem can be grouped into two sub-domains i.e. fingerprint verification and fingerprint identification.
- 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 user such as PIN Code and Fingerprint matching.



Approaches For Fingerprint Recognition

- The first approach, which is **minutiae-based**, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products.

- The second approach, which uses **image-based methods**, tries to do matching based on the global features of a whole fingerprint image. It is an advanced approach. And it is useful to solve some intractable problems of the first approach.

Procedure

Pre-Processing

Feature Extraction

Template Generator

Enrollment

Database

Test

Test

Matcher

No

Yes

Sensor

SOFTWARE REQUIREMENT SPECIFICATION (SRS)

INTRODUCTION

- **Purpose**

  This Software Requirements Specification provides a complete description of all the functions and specifications of the ATM system of bank. The purpose is to provide extra security to the ATM systems

- **Scope**

  The ATM system is designed to run for 24 hours and to allow bank clients to carry out transactions in a secured way. The data will be held in a bank database. The system is connected to the bank database using a modem.

- **Document Overview**

  The remainder of this document is two chapters, the first providing a **full description** of the project for the bank's ATM with fingerprint security. This SRS gives the details about the various **requirements** & about the various hardware & software interfaces.

OVERALL DESCRIPTION

The ATM system encompasses various GUI menus including the SENSOR, to provide high security. It provides secure access to the account of a customer. The ATM must be able to provide the following **services** to the customer:

Enter Pin: A customer is allowed to enter the PIN Code for his/her Account.

Change Pin: A customer must be able to change the pin linked to the card.

Enroll Finger: A customer is allowed to enroll the fingerprint impression which has been used to provide security to the Account

Change Fingerprint: A customer is allowed to change the fingerprint impression.

Functional Requirements Definition

The software to be designed will control a simulated automated teller machine (ATM) having :

- A sensor to enroll and detect fingerprint.
- A customer console (keyboard and display) for interaction with the customer.(for entering PIN Code)

- **Facility of Aborting transaction**

  A customer must be able to abort a transaction in progress by pressing the Cancel key instead of responding to a request from the machine.

- **PIN Code format**

  Pin should be of exactly 4 digit.

- **Facility of PIN Re-entering**

  If the customer's PIN is invalid, the customer will be required to re-enter the PIN before a transaction can proceed.

- **Denial of service, if PIN goes wrong.**

  If the customer is unable to successfully enter the PIN after three tries, the service would be denied for particular card.

- **Enroll finger**

  Enroll your finger from first joint to the tip.

- **Facility of Re-enrolling the finger**

  If the customer's Fingerprint is invalid, the customer will be required to re-enroll the Fingerprint before a transaction can proceed.

- **Denial of service, if fingerprint goes wrong**

  If the customer is unable to successfully enroll fingerprint after three tries, the service would be denied for that particular card.

- **Explanation of problem**

  If a transaction fails for any reason other than an invalid PIN and fingerprint, the ATM will display an explanation of the problem.

NON FUNCTIONAL REQUIREMENT

There are requirements that are not functional in nature. Specifically, these are the constraints the system must follow. They are often called qualities of a system. Other terms for non-functional requirements are “constraints”,” quality attributes”,” quality goals”,” quality of service requirements” and “non-behavioral requirements”.

- **Scope:** The scope of this project is to allow the user to get access to their account through the ATM using fingerprinting functionality.
- **Functionality:** One customer at a time can process their account in the ATM machine.
- **Usability:** The desktop user interface shall be Windows 95/98/2000/XP/7 complaint.
- **Reliability:** The ATM machine must be able to scan or read the card and the fingerprint properly and identify the customer account.

- **Performance:** The ATM machine support only one customer at a time. The speed and accurate transaction decides the performance factor. The screen must be clearly visible to the user.
- **Security:** The pin number and the fingerprint in the card guarantee the security of a customer's account. The ATM system must not store any of this data in its database. The customer with a pin number and a valid card with valid fingerprint impression is allowed to do all transactions.

FRONT END DESCRIPTION

For developing the front – end interface, we have decided to use ASP.NET platform, with C# as the programming language, due to the following reasons:-

- Easy to use and flexible interface.
- A number of options for customizability.
- Proven to provide good performance and high reliability.
- Attractive and visually pleasing interface.

BACK END DESCRIPTION

For developing the database (back – end), we have decided to use MS-SQL Server 2008 database, due to the following reasons:-

- Native support and full compatibility with ASP.NET platform .
- Flexible, scalable and robust database architecture.
- Used by market-leading companies worldwide.
- Strong data protection and ease of management.

DATABASE DESCRIPTION

Tools Used:

- Database - MS SQL Server 2008 R2

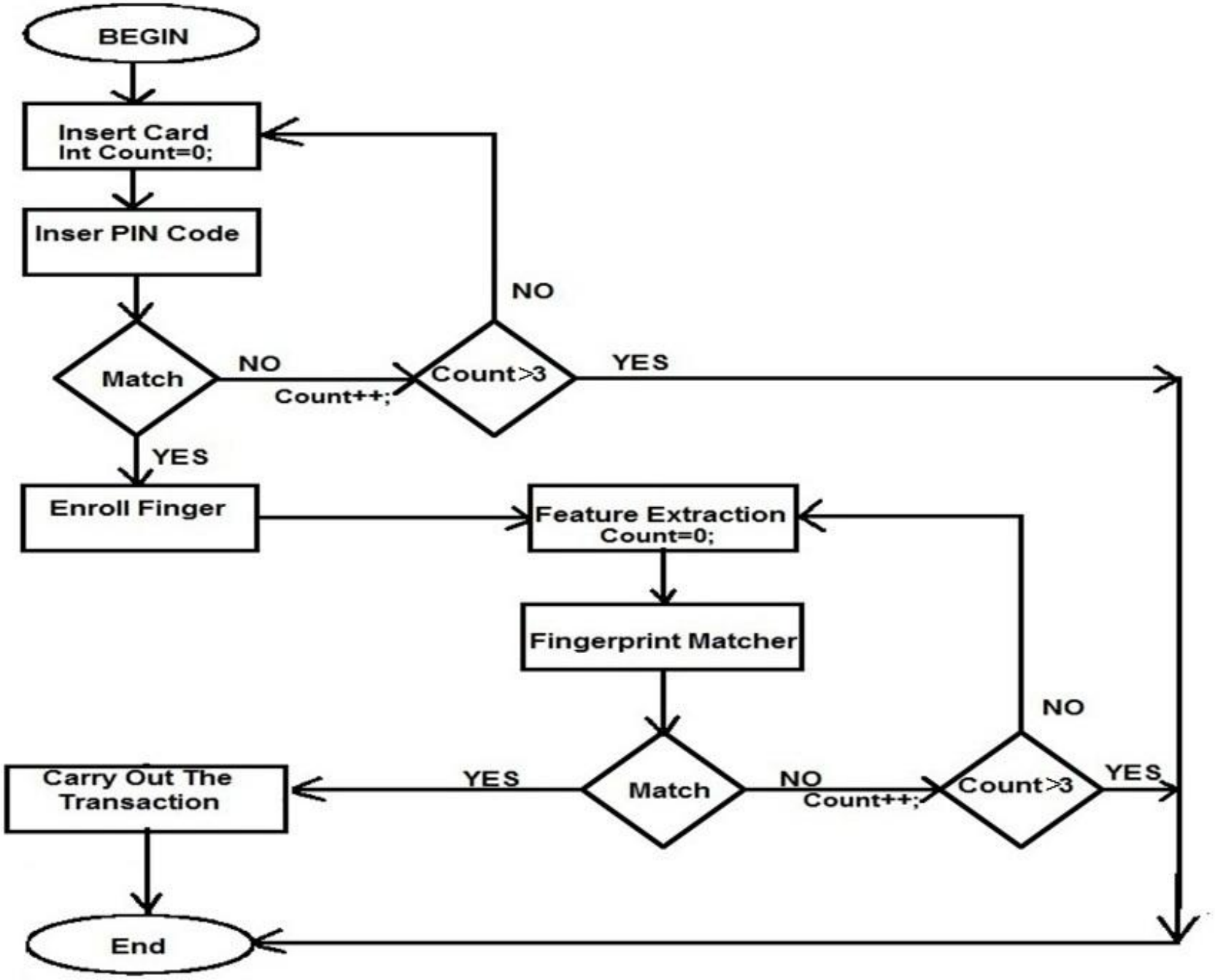
HARDWARE REQUIREMENT

- Processor - Pentium 4
- Hard Disk - 5 GB
- RAM - 256 MB
- Sensor - Fingerprint Recognizer

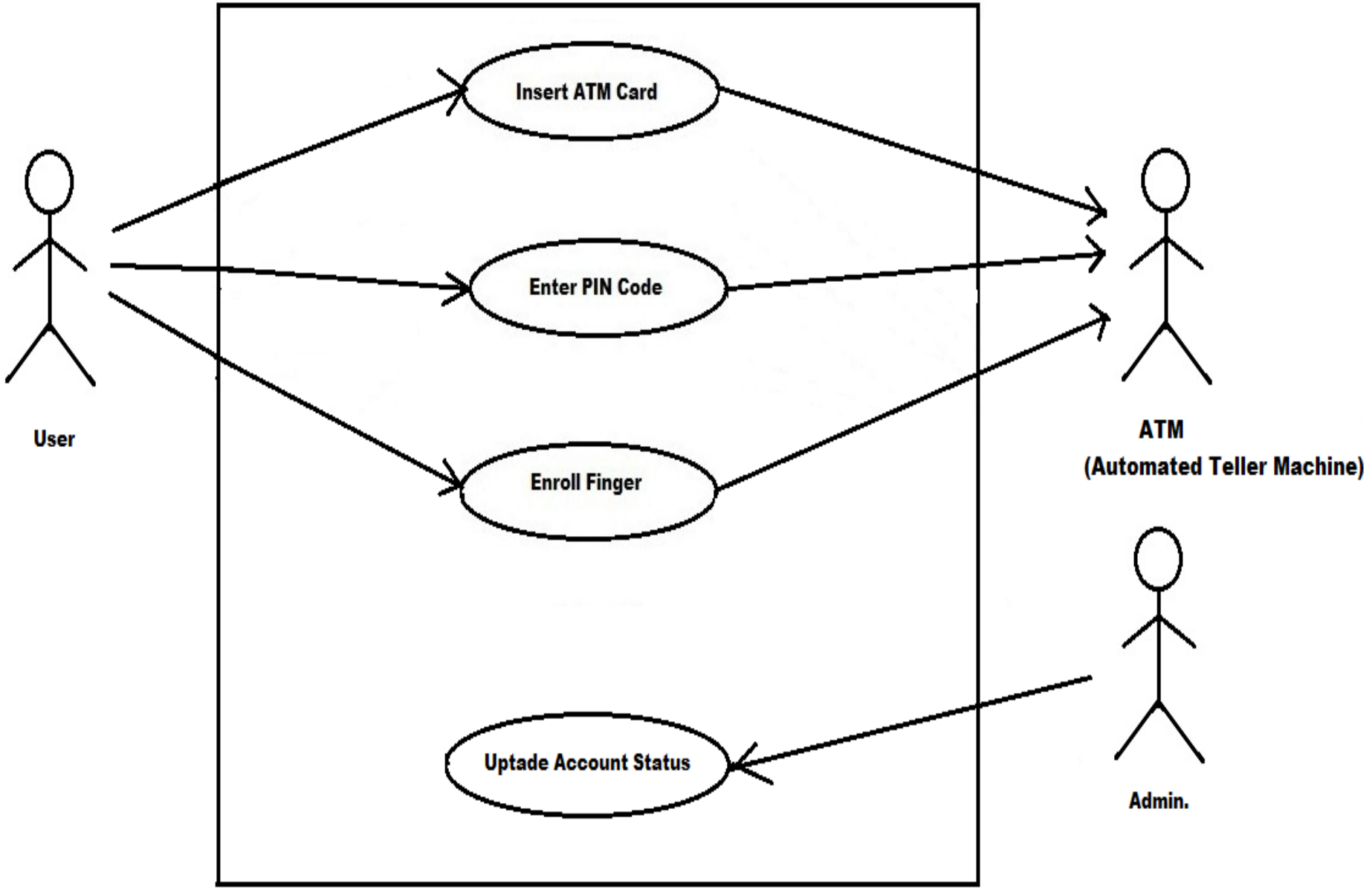
SOFTWARE REQUIREMENT

- Operating System - Windows 7
- Database System - MS SQL Server 2008 R2
- Front End - Visual Studio 2010
- Framework - .NET Framework 4.0

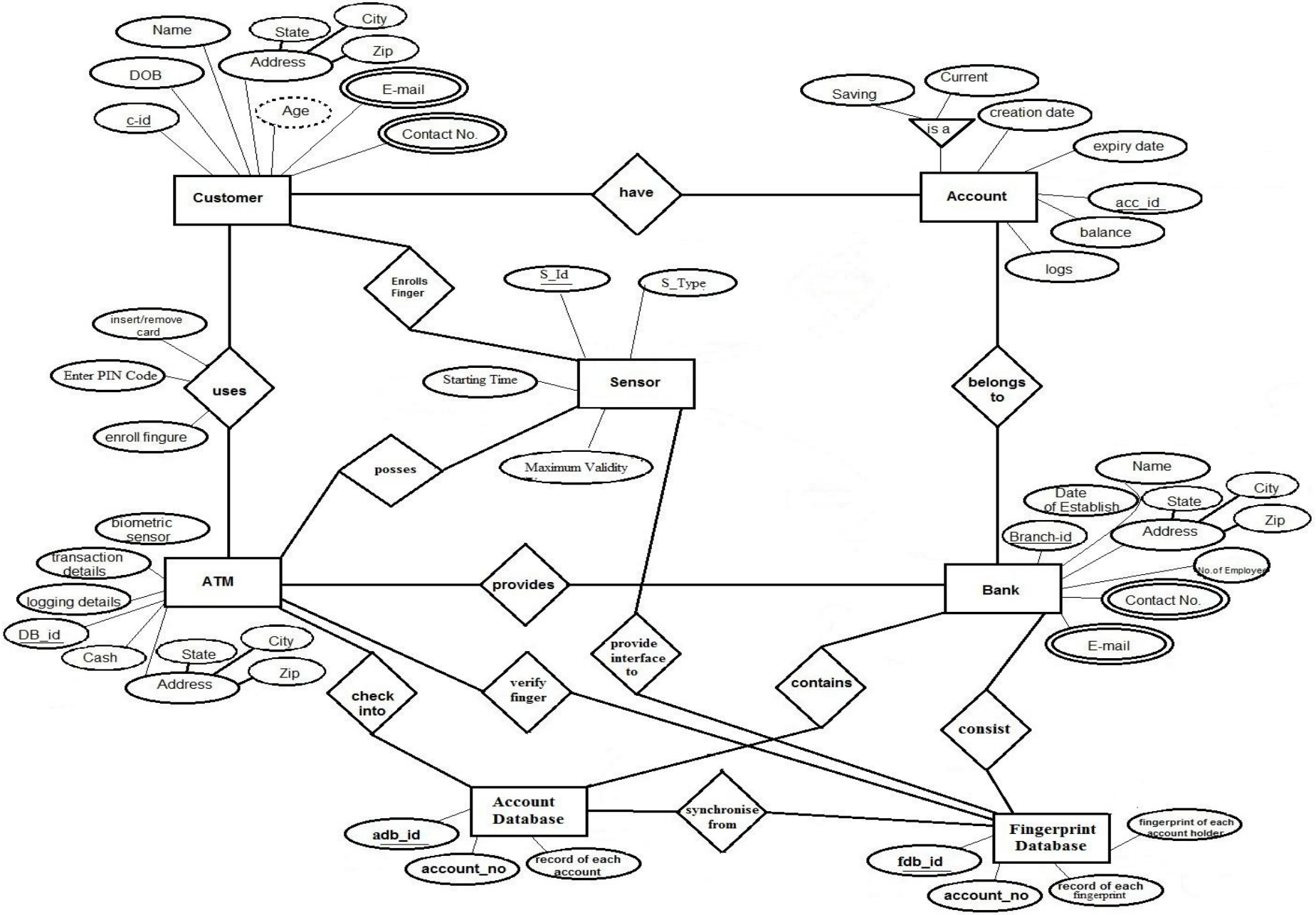
FLOW CHART


BEGIN
Insert Card
Int Count=0;
Inser PIN Code
Match
NO
Count++;
Count>3
NO
YES
YES
Enroll Finger
Feature Extraction
Count=0;
Fingerprint Matcher
Match
YES
NO
Count++;
Count>3
NO
YES
Carry Out The
Transaction
End

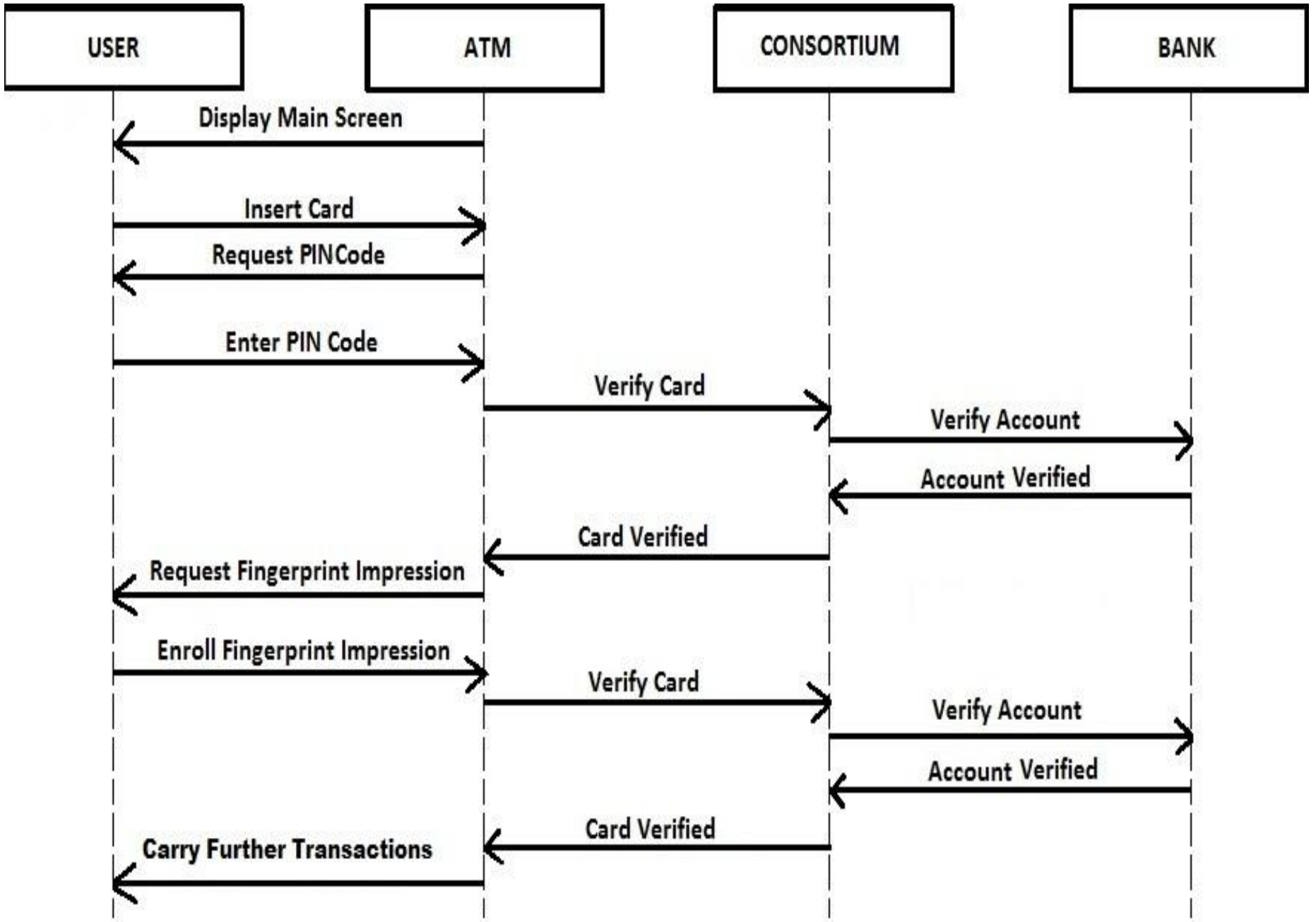
USE CASE DIAGRAM


Insert ATM Card
Enter PIN Code
Enroll Finger
Uptade Account Status
User
ATM
(Automated Teller Machine)
Admin.

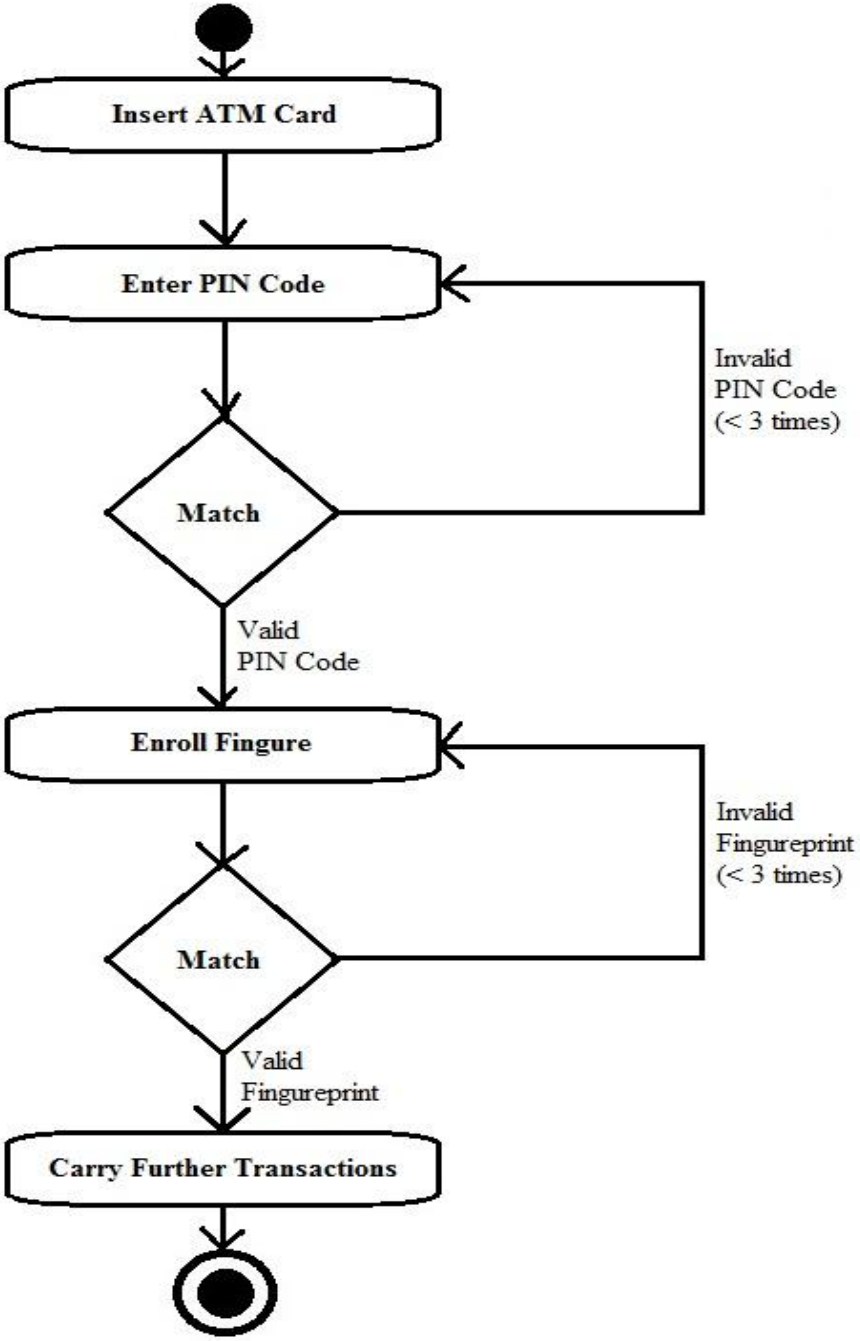
E-R DIAGRAM


Name
State
City
Address
Zip
DOB
E-mail
Age
c-id
Contact No.
Customer
have
Saving
Current
is a
creation date
expiry date
Account
acc_id
balance
logs
Enrolls Finger
S_Id
S_Type
Sensor
insert/remove card
Enter PIN Code
uses
enroll fingure
Starting Time
posses
Maximum Validity
belongs to
biometric sensor
transaction details
logging details
DB_id
Cash
ATM
provides
Name
Date of Establish
State
City
Zip
Branch-id
Address
No.of Employee
Contact No.
E-mail
Bank
provide interface to
contains
check into
verify finger
consist
Account Database
adb_id
account_no
record of each account
synchronise from
Fingerprint Database
fingerprint of each account holder
fdb_id
account_no
record of each fingerprint

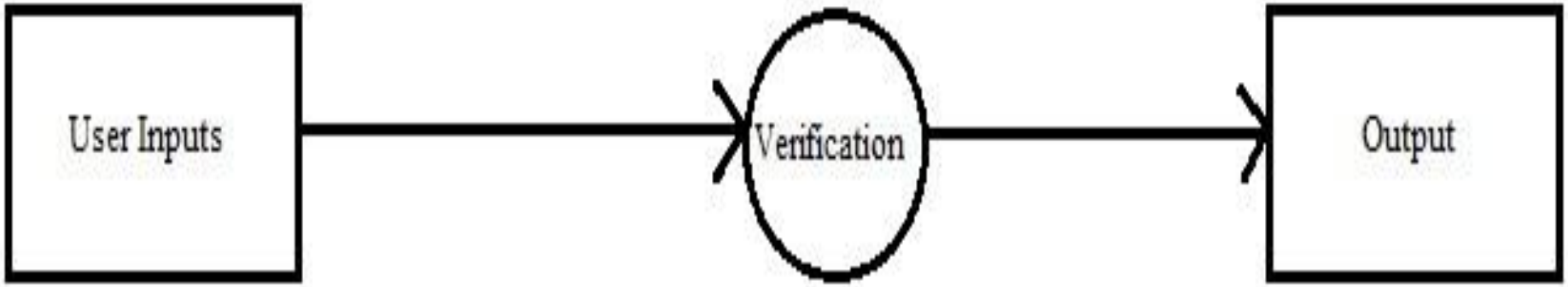
SEQUENCE DIAGRAM


USER
ATM
CONSORTIUM
BANK
Display Main Screen
Insert Card
Request PINCode
Enter PIN Code
Verify Card
Verify Account
Account Verified
Card Verified
Request Fingerprint Impression
Enroll Fingerprint Impression
Verify Card
Verify Account
Account Verified
Card Verified
Carry Further Transactions

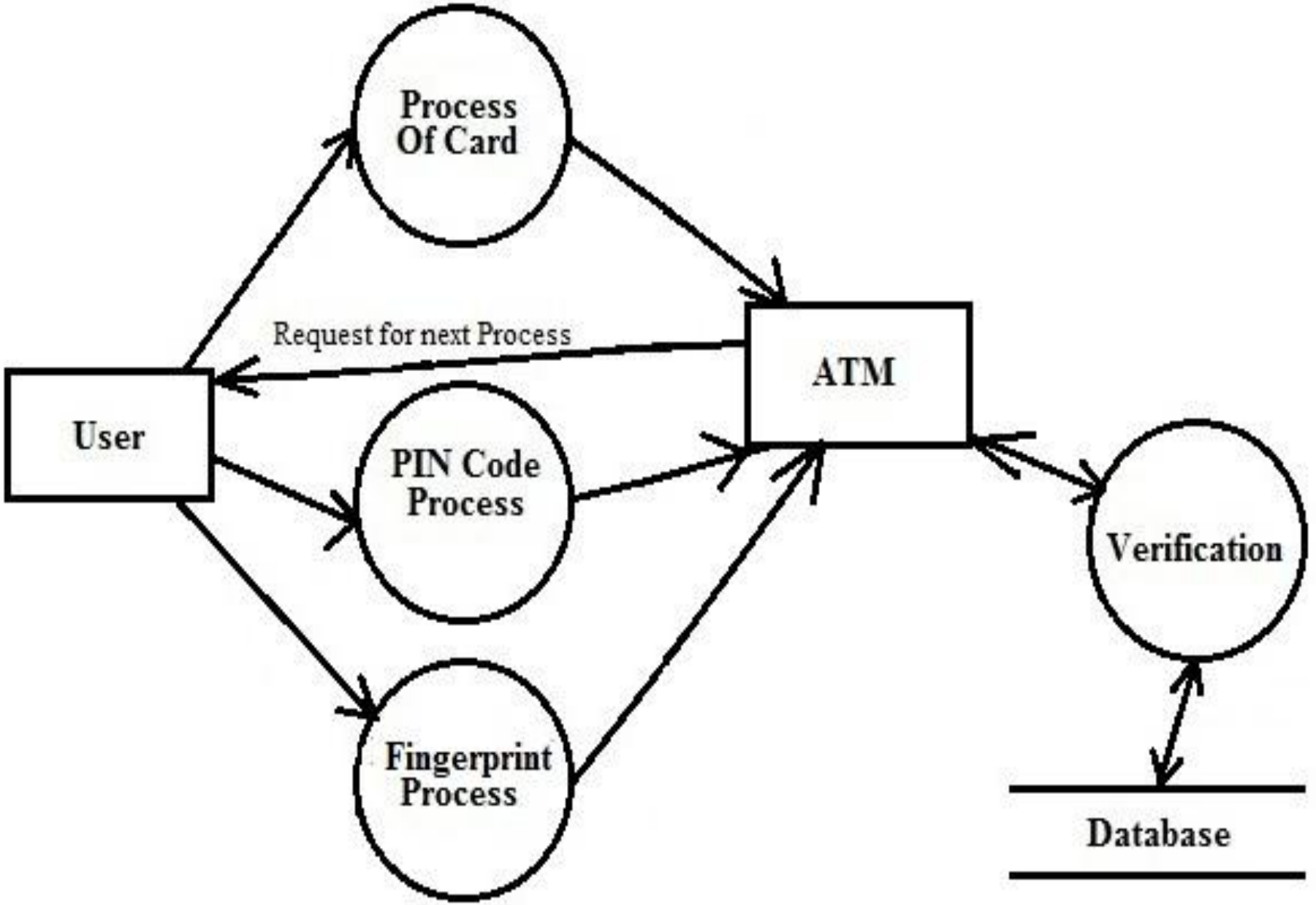
ACTIVITY DIAGRAM


Insert ATM Card
Enter PIN Code
Invalid
PIN Code
(< 3 times)
Match
Valid
PIN Code
Enroll Fingure
Invalid
Fingureprint
(< 3 times)
Match
Valid
Fingureprint
Carry Further Transactions

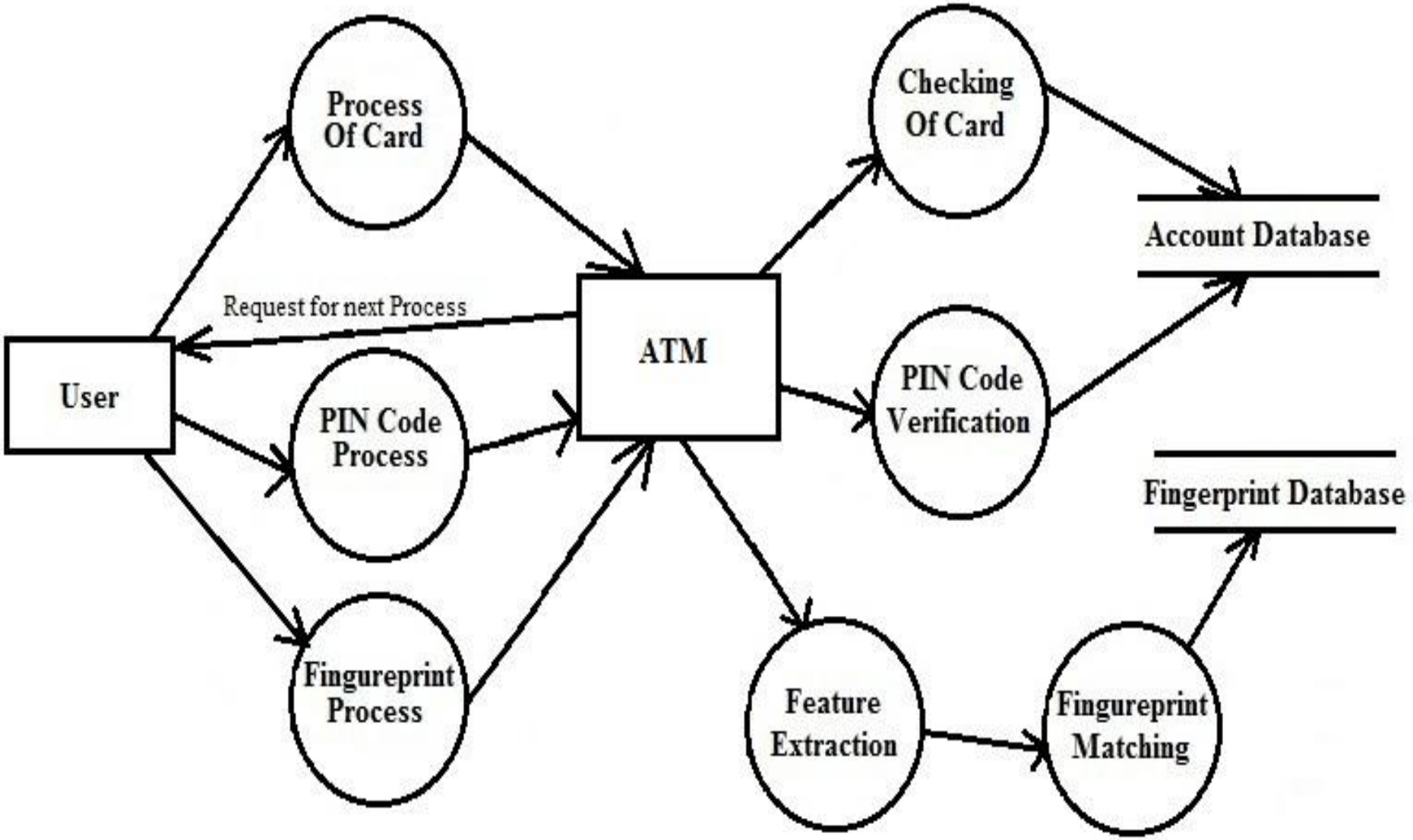
DATA FLOW DIAGRAM LEVEL-0


User Inputs
Verification
Output

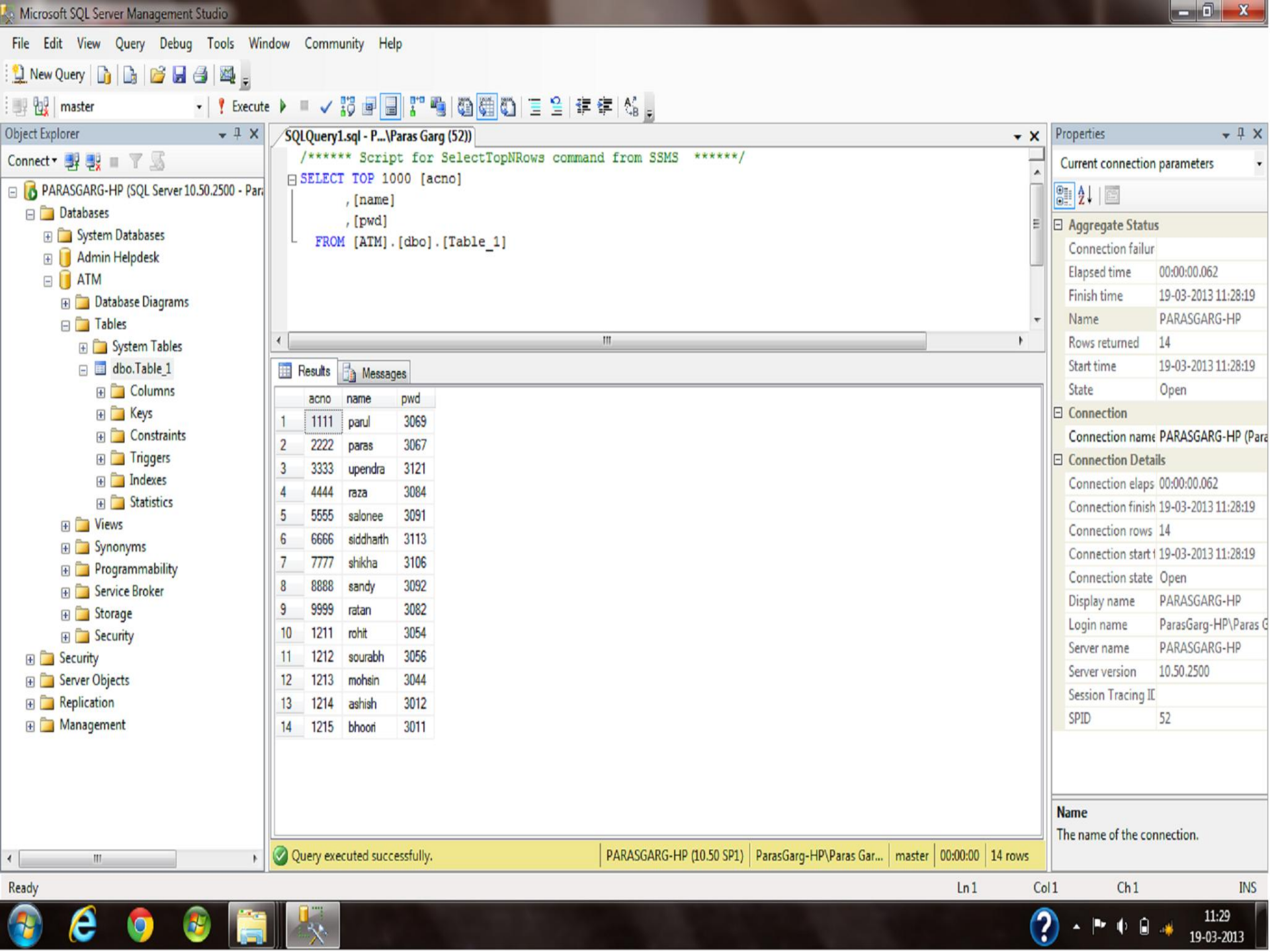
DATA FLOW DIAGRAM LEVEL-1


Process
Of Card
Request for next Process
ATM
User
PIN Code
Process
Verification
Fingerprint
Process
Database

DATA FLOW DIAGRAM LEVEL-2


Process
Of Card
Checking
Of Card
Account Database
Request for next Process
User
ATM
PIN Code
Process
PIN Code
Verification
Fingerprint Database
Fingureprint
Process
Feature
Extraction
Fingureprint
Matching

SNAPSHOTS


Microsoft SQL Server Management Studio
File Edit View Query Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
PARASGARG-HP (SQL Server 10.50.2500 - Para
Databases
System Databases
Admin Helpdesk
ATM
Database Diagrams
Tables
System Tables
dbo.Table_1
Columns
Keys
Constraints
Triggers
Indexes
Statistics
Views
Synonyms
Programmability
Service Broker
Storage
Security
Security
Server Objects
Replication
Management
SQLQuery1.sql - P...\Paras Garg (52))
/****** Script for SelectTopNRows command from SSMS ******/
SELECT TOP 1000 [acno]
,[name]
,[pwd]
FROM [ATM].[dbo].[Table_1]
Results
Messages
acno name pwd
1 1111 parul 3069
2 2222 paras 3067
3 3333 upendra 3121
4 4444 raza 3084
5 5555 salonee 3091
6 6666 siddharth 3113
7 7777 shikha 3106
8 8888 sandy 3092
9 9999 ratan 3082
10 1211 rohit 3054
11 1212 sourabh 3056
12 1213 mohsin 3044
13 1214 ashish 3012
14 1215 bhoori 3011
Query executed successfully.
PARASGARG-HP (10.50 SP1)
ParasGarg-HP\Paras Gar...
master
00:00:00
14 rows
Properties
Current connection parameters
Aggregate Status
Connection failur
Elapsed time 00:00:00.062
Finish time 19-03-2013 11:28:19
Name PARASGARG-HP
Rows returned 14
Start time 19-03-2013 11:28:19
State Open
Connection
Connection name PARASGARG-HP (Para
Connection Details
Connection elaps 00:00:00.062
Connection finish 19-03-2013 11:28:19
Connection rows 14
Connection start 19-03-2013 11:28:19
Connection state Open
Display name PARASGARG-HP
Login name ParasGarg-HP\Paras G
Server name PARASGARG-HP
Server version 10.50.2500
Session Tracing ID
SPID 52
Name
The name of the connection.
Ready
Ln 1 Col 1 Ch 1 INS
11:29
19-03-2013


Fingerprint Authentication For ATM
Welcome to the ATM
Enter Your ATM Card
1 2 3 CLEAR
4 5 6 cancel
7 8 9 BACK
* 0 c ENTER


Fingerprint Authentication For ATM
Welcome to the ATM
Enter Your ATM Card
1111
1 2 3 CLEAR
4 5 6 cancel
7 8 9 BACK
* 0 c ENTER


Fingerprint Authentication For ATM
Welcome panul
Enter your password
1 2 3 CLEAR
4 5 6 cancel
7 8 9 BACK
* 0 c ENTER


Fingerprint Authentication For ATM
Welcome parul
Enter your password
3069
1 2 3 CLEAR
4 5 6 cancel
7 8 9 BACK
* 0 c ENTER


Fingerprint Authentication For ATM
NCR
Congrates parul
Swipe your finger
1
2
3
CLEAR
4
5
6
cancel
7
8
9
BACK
0
c
ENTER


Fingerprint Authentication For ATM
Thanks to visiting here
Now you are ready for your further Transaction with Details
Name: parul
accont no:1111
1 2 3 CLEAR
4 5 6 cancel
7 8 9 BACK
* 0 c ENTER


Fingerprint Authentication For ATM
acno
name
pwd
1111
parul
3069
2222
paras
3067
3333
upendra
3121
4444
raza
3084
5555
saloree
3091
1
2
3
CLEAR
4
5
6
cancel
7
8
9
BACK
*
0
c
ENTER

ADVANTAGES

1. Very high accuracy and security
   - Identification (Do I know who you are?)
   - Verification (Are you who you claim to be?)
2. Is the most economical biometric PC user authentication technique.
3. It is one of the most developed biometrics.
4. Easy to use.
5. Small storage space required for the biometric template, reducing the size of the database memory required.
6. It is standardized.
7. Enhance traditional methods (PINs, Passwords).

DISADVANTAGES

- General Limitations

1. Misidentification
   - False Acceptance
   - False Rejection
2. Privacy
3. Image captured at 500 dots per inch(dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 KB approximately → Compression required (a factor of 10 approximately).

- Limitations for individual

1. Dry, wet or dirty hands.
2. For some people it is very intrusive, because it is still related to criminal identification.

CONCLUSION

- A smartcard based ATM fingerprint authentication scheme has been proposed. The possession (smartcard) together with the claimed user's Biometrics (fingerprint) is required in a transaction. The smartcard is used for the first layer of mutual authentication when a user requests transaction. Biometric authentication is the second layer. The fingerprint image is encrypted via 3D map as soon as it is captured, and then is transmitted to the central server via symmetric algorithm. The encryption keys are extracted from the random pixels distribution in a raw image of fingerprint.

- The stable features of the fingerprint image need not to be transmitted, it can be extracted from the templates at the central server directly.

- After this, the minutiae matching is performed at the central server. The successful minutiae matching at last verifies the claimed user. Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.

THANK YOU