MULTIMODAL BIOMETRIC TRANSACTION SYSTEMS

A Project Report

by

Achal Sancheti, Pallak Jain, Shabbir Hussain, Shilpi Bundela, Tanisha Jain

In partial fulfillment for the course
of

INFO 6210

Database Management and Database Design Report

Date: Dec 17th 2016

Information Systems Engineering
College of Engineering, Northeastern University
Boston, MA 02115

ABSTRACT

Multimodal Biometric Transactional Systems aims to develop robust and extremely secured transactional systems worldwide. In the present scenario, there is a need to enhance the security and safety of existing transactional systems. The level of security is raised by introducing composite multimodal biometric techniques for user's authentication. Highly transactional databases are also prone to attacks by unauthorized users. An encryption technique SHA-2 is utilized to perform database encryption to make the user's private data templates secured. Template comparison is presented by a stored procedure named sp_verifier which compares the biometric data with customer's input and displays results if users are verified.

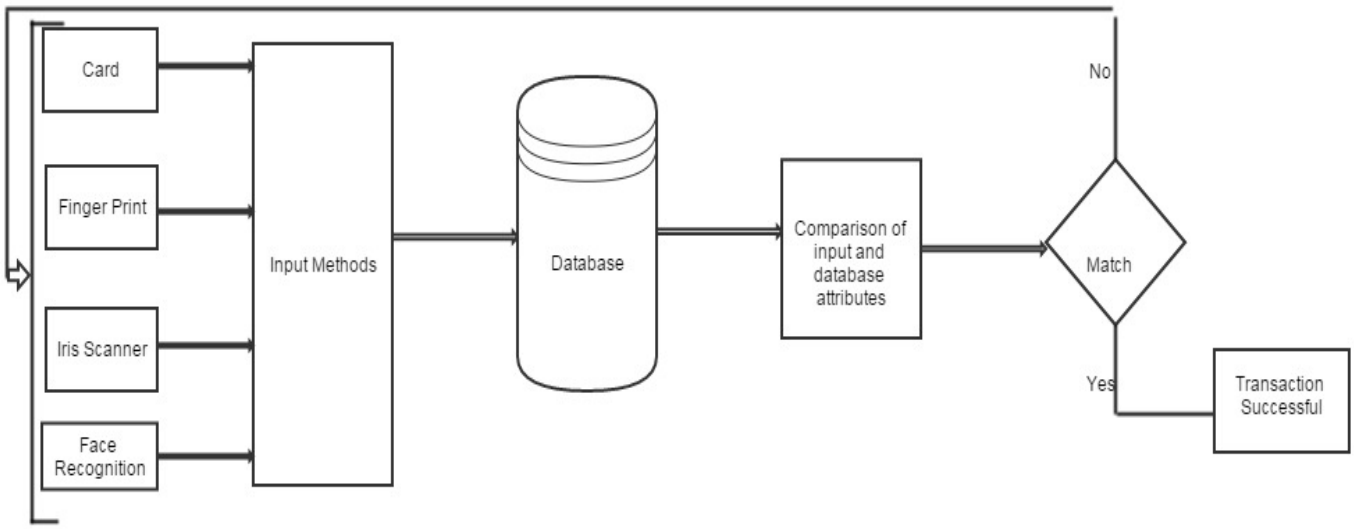
Table of Contents

CHAPTER – 1

1.1 Introduction:

The purpose of our project is to introduce a multimodal biometric system which will enhance the security of all cashless transactions. It can be widely implemented in card reading and user authentication machines.

The authentication will be performed on the basis of the stored data of the customer in the database. If combination is validated, transaction can be done, else a case of fraud.



- Biometric template of user's fingerprints, facial schema and retina scan are stored in database at the time of account creation in bank.
- When a user performs any transaction, his biometric information is verified.
- Verification is successful if the transactions are validated on comparison with the stored templates.
- Encryption techniques used to secure private information in database.
- Multimodal authentication system can be widely implemented in ATMs, automatic cars and all existing card reading machines.

1.2 Problem Definition:

Since 2012, Identity theft victims suffered direct or indirect losses of more than $24.7 billion dollars every year. On average, victims whose personal information was misused experienced a great loss. Victims whose personal information is misused are more likely to experience financial problems such as dealing with debt collectors, repeatedly correcting credit reports because of identity theft than those whose existing account information is stolen, but victims of all categories may experience these issues. Therefore, there is a need to improve the security of existing transactional systems, which uses person's identity as a parameter of authentication.

1.3 Proposed Solution:

The solution provided to this problem is that a composite biometric authentication is provided in all card-reading machines. The biometric techniques utilized in the project are-

- Finger print Scan
- Facial Recognition
- Retina Scan

Customer's biometric templates are stored in the bank at the time of account creation. User selects a combination out of the given authentication methods:

- Facial Recognition + Iris Scan
- Iris Scan + Finger Print
- Finger Print + Facial Recognition
- Card + Any of the Biometric method

The authentication is performed on comparison with the stored template of the customer in the database.

If combination is validated, transaction can be done, else a case of fraud.

SHA-2 algorithm converts the customer's sensitive data i.e. biometrics and card details into encrypted text and stores encrypted value in database.

CHAPTER – 2

2.1 Why Multimodal Biometric:

Unimodal systems perform person recognition based on single source of evidence which may sometimes be affected by sensory noise.

It can be useful for people with hand-related disabilities.

A small portion of population can have nearly identical facial appearance due to genetic factors.

2.2 Key Functions:

Biometric template of user's fingerprints, facial schema and retina scan are stored in database at the time of account creation in bank.

When a user performs any transaction, his biometric information is verified.

Verification is successful if the biometrics at the time of transactions are verified in comparison with the stored templates.

Encryption techniques used to secure private information in database.

Multimodal authentication system can be widely implemented in ATMs, automatic cars and all existing card reading machines.

CHAPTER – 3

3.1 Use-Case Diagram:

(a) CUSTOMER ROLE

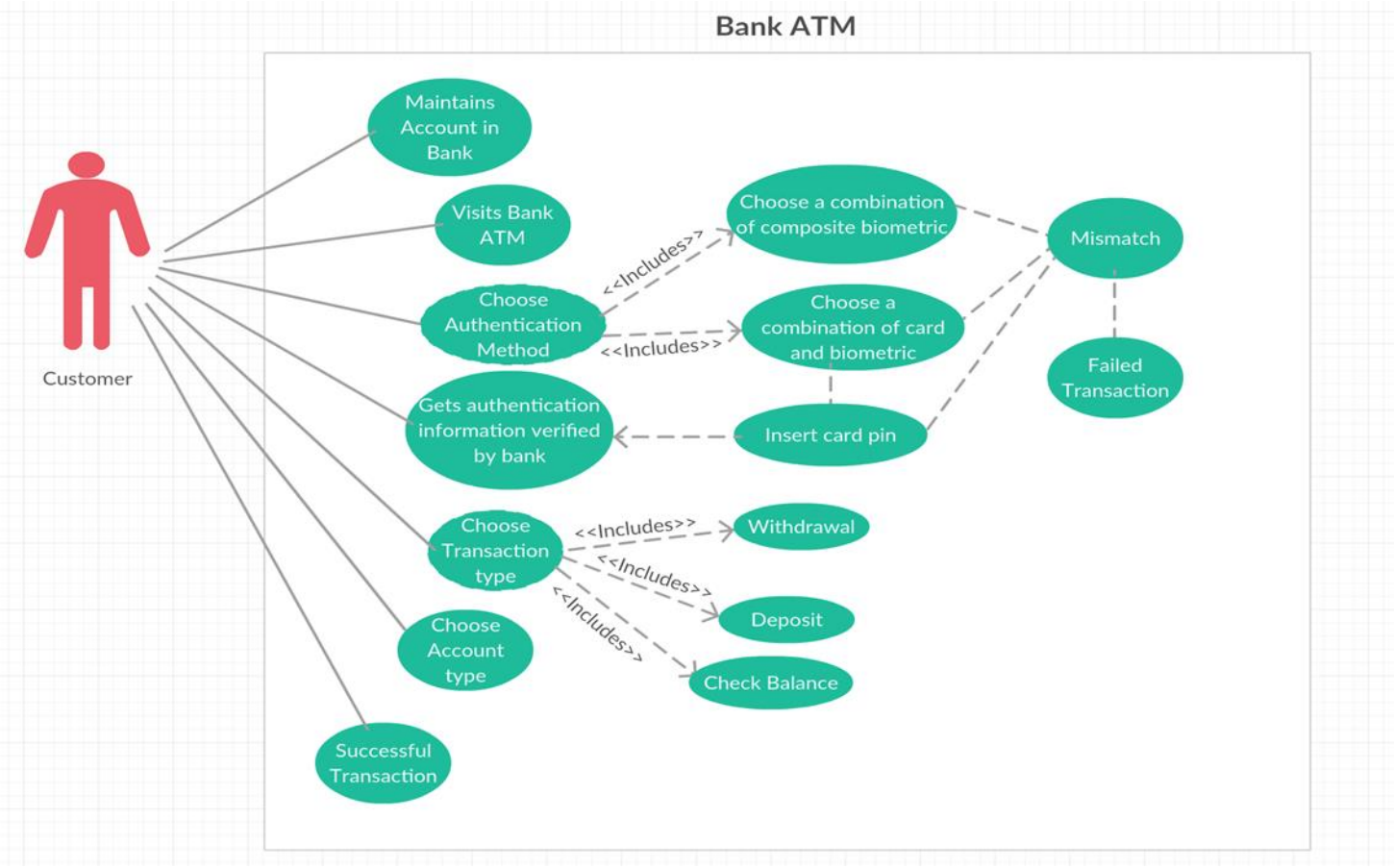


Figure (a)

- Customer, first, registers and opens an account in the bank. For direct transactions, he visits the bank ATM and chooses one set of authentication methods.

- Either he can choose a combination of a composite biometrics or he can select one biometric along with providing card details.

- Bank authenticates the information and as soon as there is a mismatch, the customer is prompted to start over and transactions fails. But in case of matching of the results with the one stored in the bank, the customer is then given liberty to choose the type of transaction.

- There are three types of transactions – withdrawal, deposit and checking the balance. The customer then chooses his account (if he has more than one account in that bank) and the transaction status is said to be completed or successful.

(b) BANK ADMIN ROLE

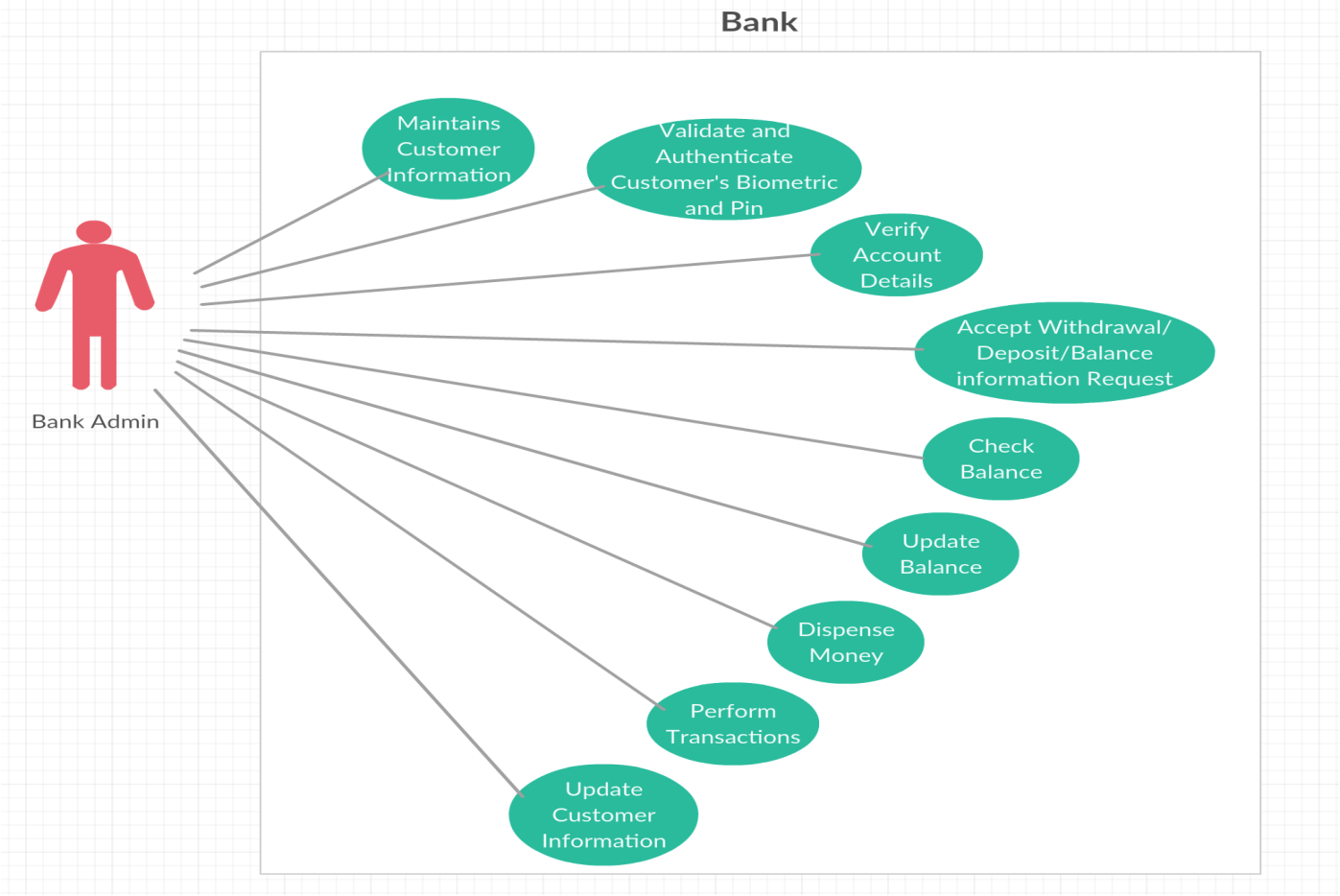


Figure (b)

- The bank admin maintains the customer information - validate and authenticate Customer's biometric and pin whenever customer is expected to make a transaction.
- The bank admin is responsible for verifying account details of the customer.
- Admin has the authority to accept or reject withdrawal, deposit or balance information request to be provided to the customer.
- The admin can check or update the balance and it can also dispense the money. The transactions are performed by the customer and if it is a successful transaction, the customer information is updated with the particular transaction.

3.2 Entity Relationship Diagram:

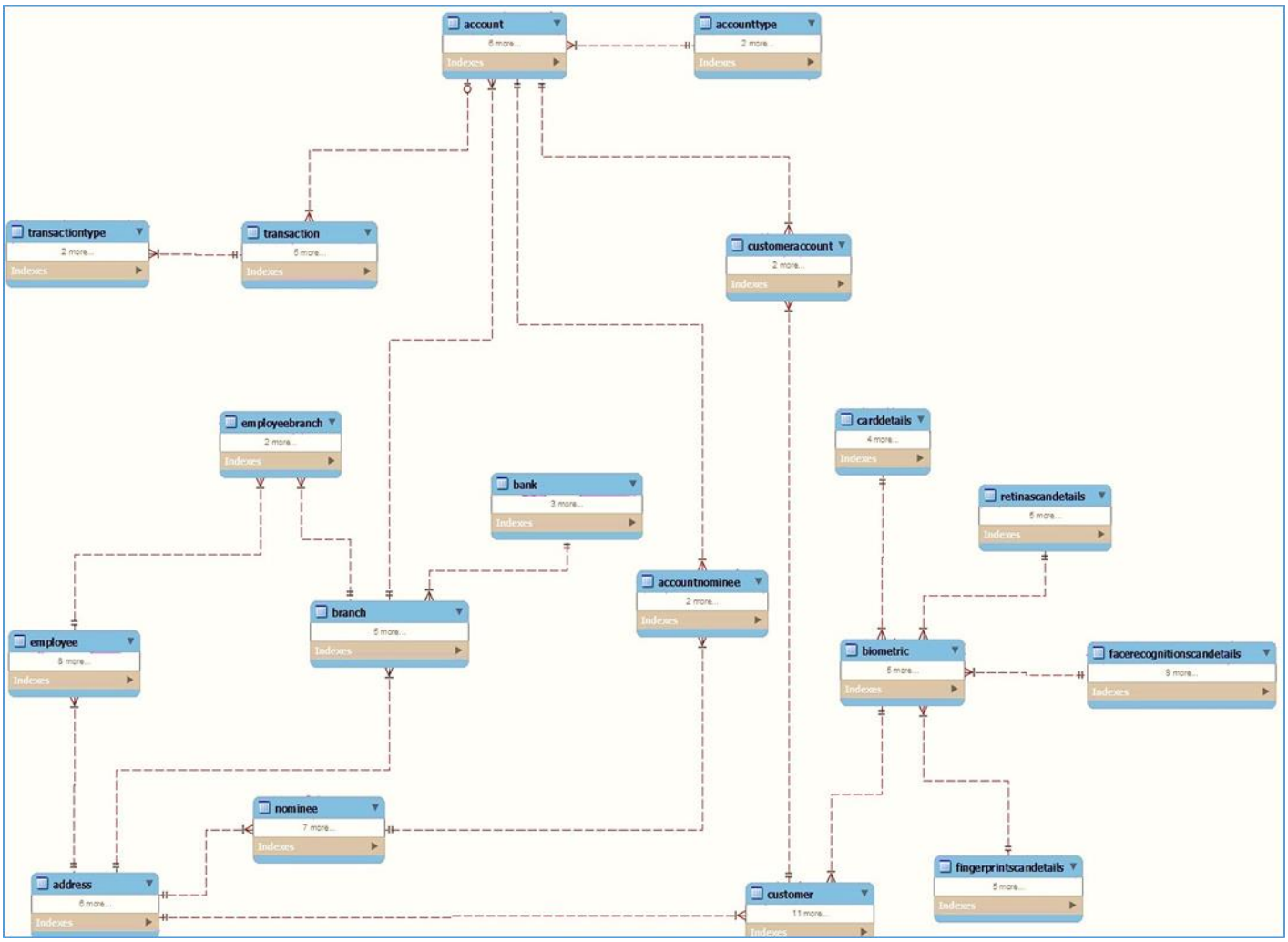


Figure 3.2 Entity Relationship Diagram

The main entities in the project are
1. Bank
2. Branch
3. Customer
4. Employee
5. Accounts
6. Biometric
7. Nominee
8. Transaction

These entities are connected to each other with the following relationships

1. Bank and Branch has one to many one relationship.

2. Branch and customer has many to many relationship

3. Branch and employee has one to many relationship

4. Branch and account has one to many relationship

5. Customer has one to many relationship with biometric

6. Customer has one to one relationship with account

7. Account has many to many relationship with nominee

8. Account has one to many relationship with the transaction

As seen above there are many entities which have many to many relationship with each other, thus to link them we have made following linking tables

1. Employee Branch Table

2. Customer Account Table

3. Account Nominee Table

For the purpose of normalization, the following has been done

1. An Address table has been added which contains detailed information about addresses of all customers and employees

2. Transaction type table has been added giving more details about transaction

3. Account type table has been added giving info of the type of account

4. Biometric table has further been broken down into Finger Print Details, Retina Scan details,

Facial Recognition details and Card Details giving detailed information about each biometric, for the purpose of normalization.

3.3 Enhanced Entity Relationship Diagram:

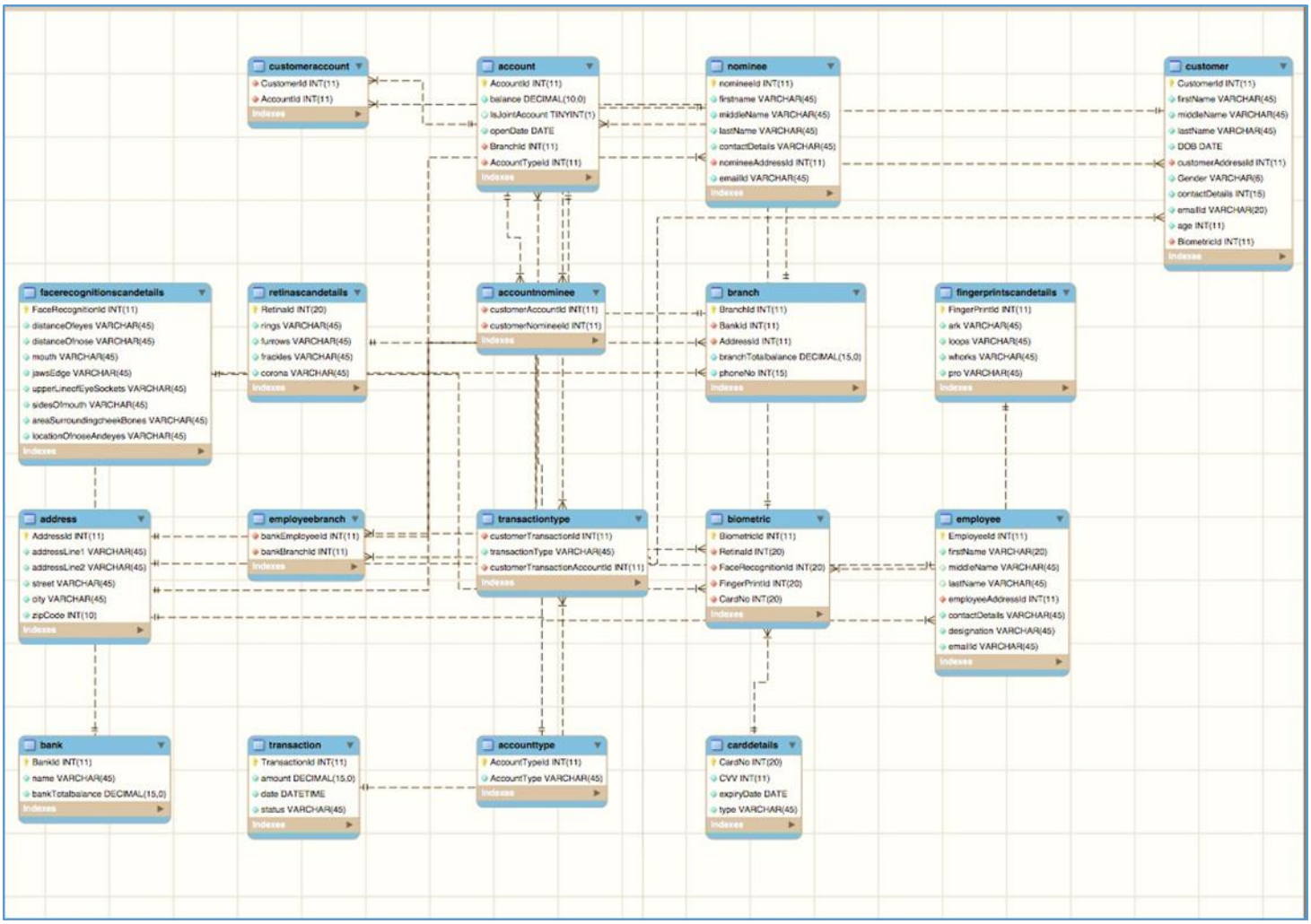


Figure 3.3 Enhanced Entity Relationship Diagram

CHAPTER – 4

4.1 Encryption:

Highly transactional databases are prone to database attacks. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

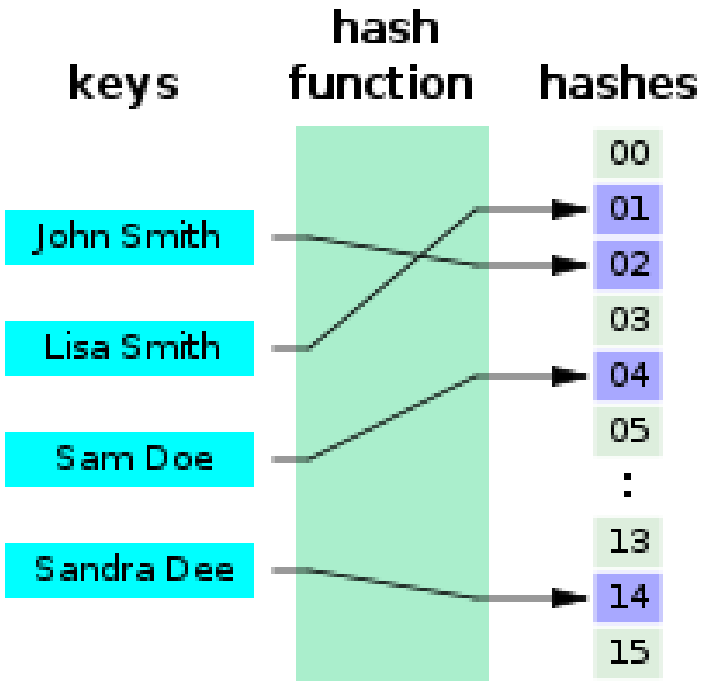
The solution to secure the sensitive data in database is Encryption.

4.2 Encryption Technique:

The technique used in the project is SHA-2.

SHA -2 Algorithm: Secure Hash Algorithm 2 uses a set of cryptographic hash functions which are collision resistant**.** SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively.

This technique improves the robustness of secured transactions. The SHA-2 family consists of six hash functions with digests.



4.3 Database Encryption:

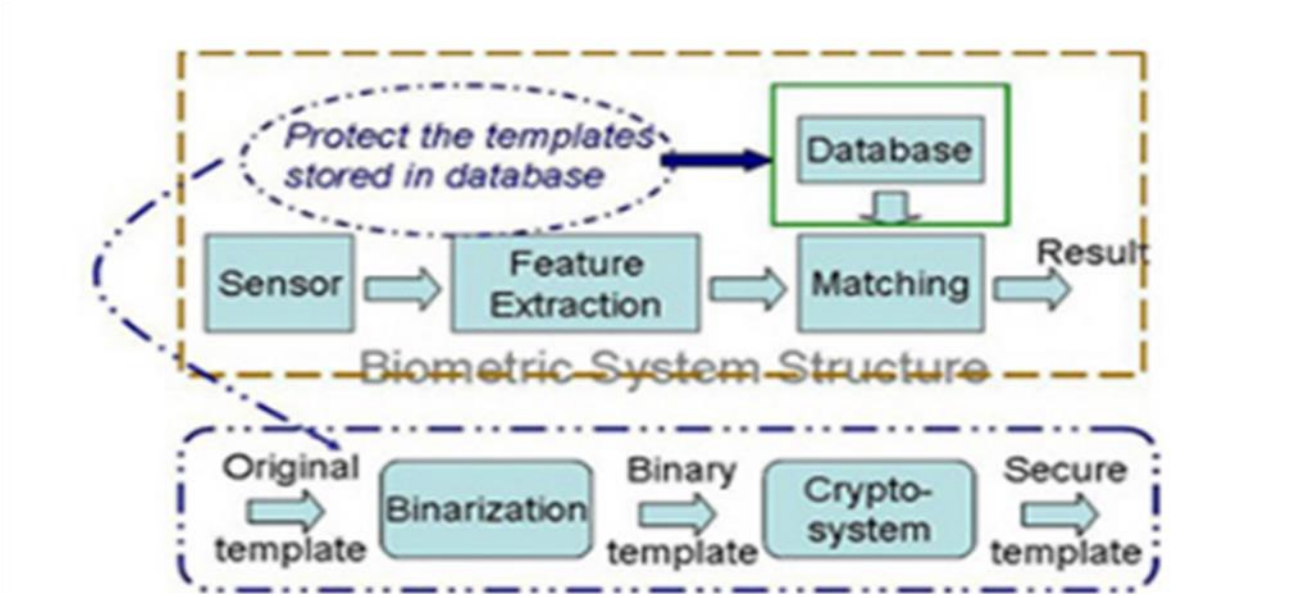


Figure 4.3 (a) Process of encryption

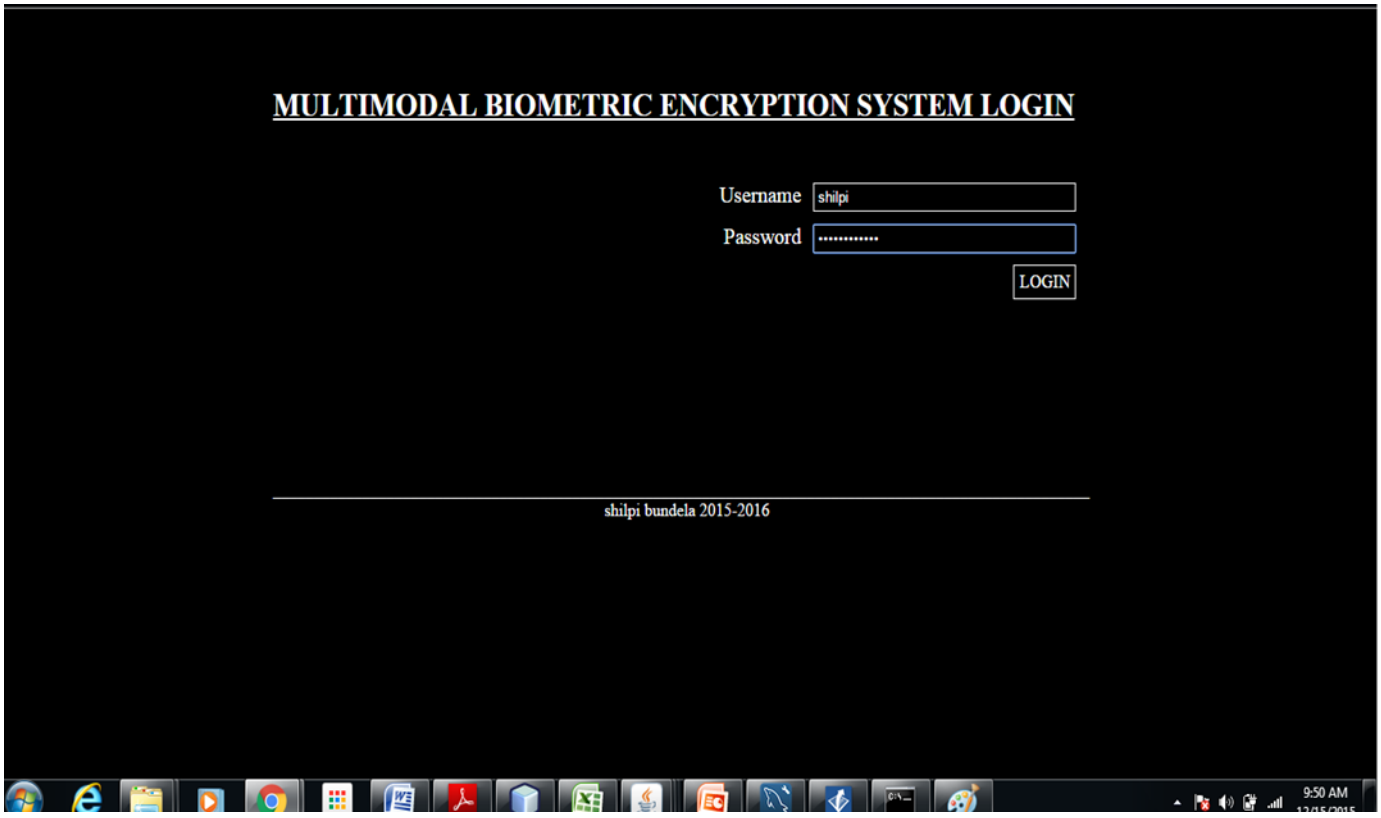


Figure 1.6 (b) : GUI for the encryption system login

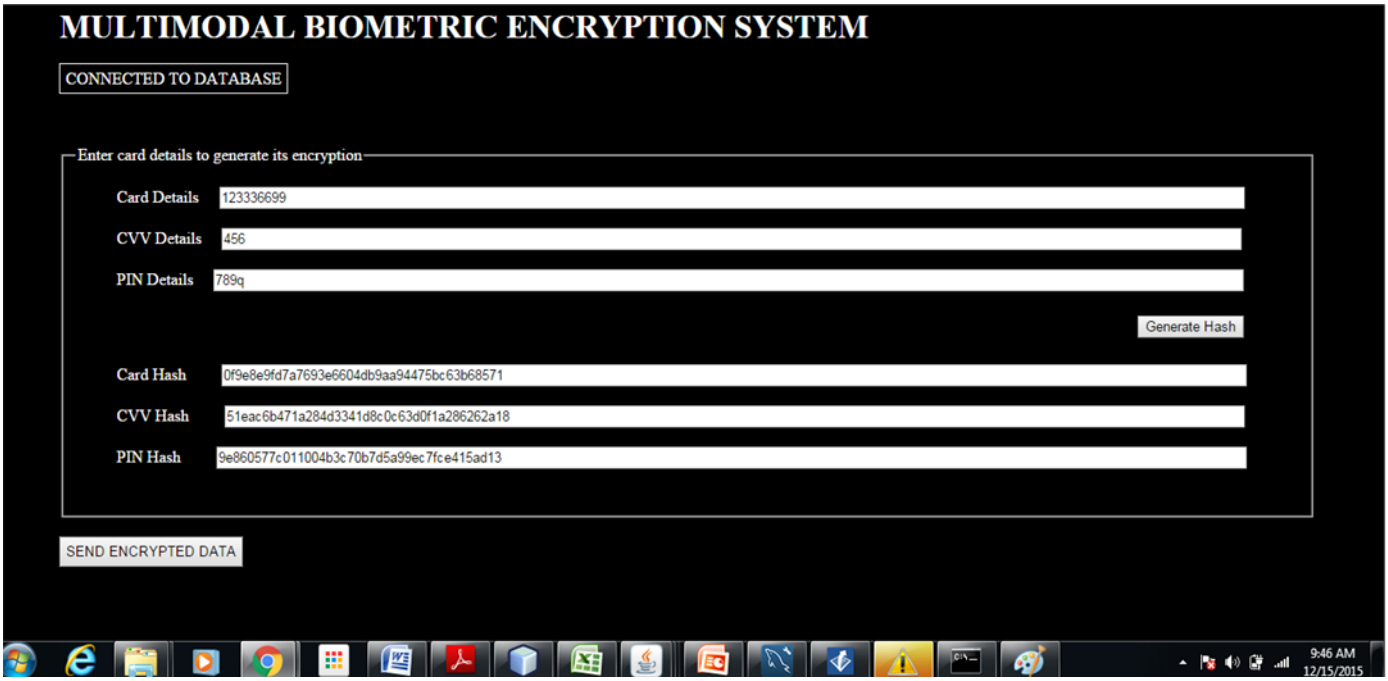


Figure 4.3 (c) : Enter the card details to encrypt

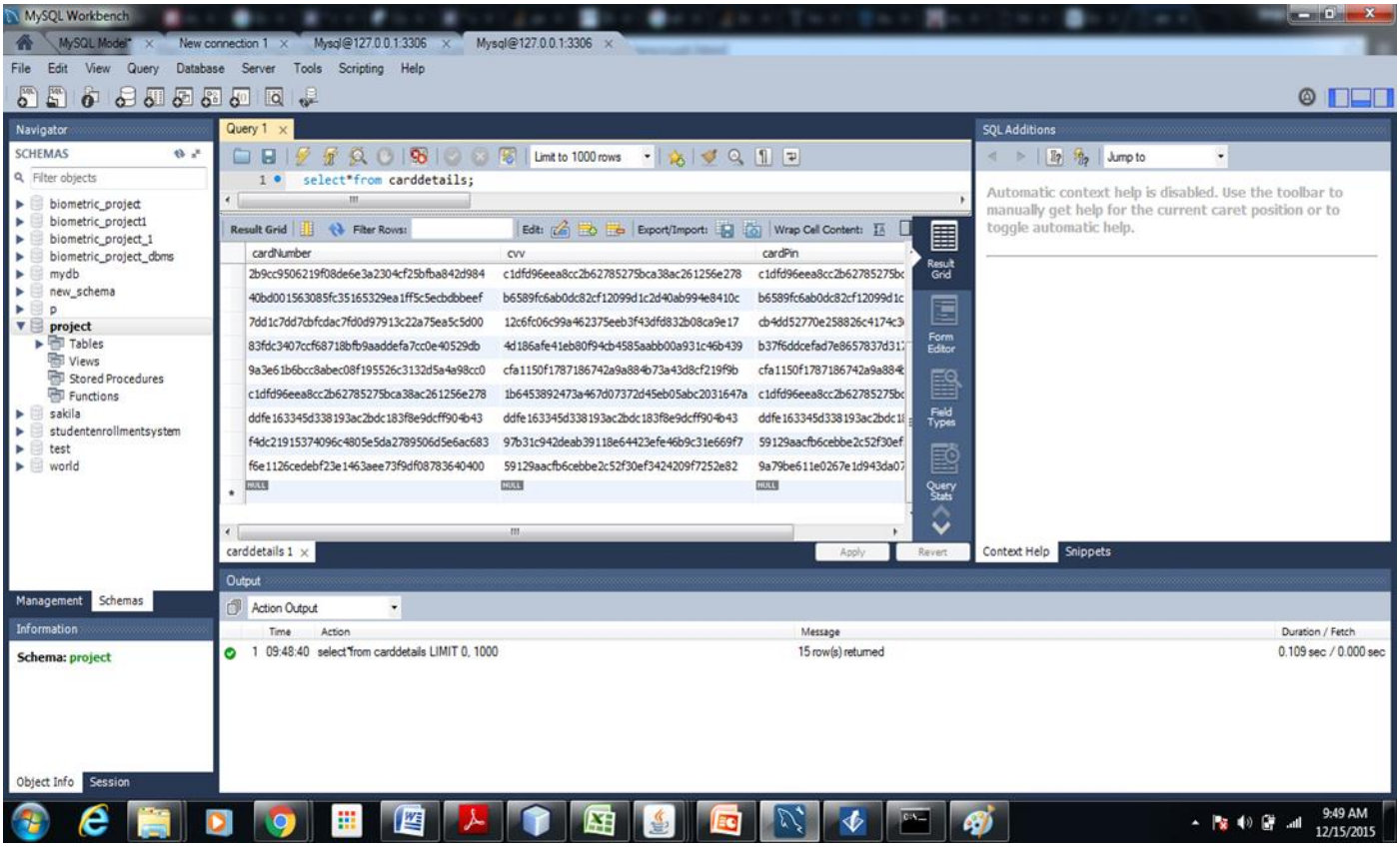


Figure 4.3 (d) : Database that will store the encrypted information in hash codes

CHAPTER – 5

5.1 Tables and Attributes:

Attributes / Properties

Attributes (also called properties) describe the characteristics of the entity, thus giving it definition. The table properties include the physical name and conceptual name (which in this case are the same), columns, primary key, and indexes. Properties for columns include the physical name, display name, data type and length, and whether or not it is a primary key and or required. The attributes of our ingredients are self-describing, and therefore make transaction easier to understand. A transactional database has to be highly normalized. The project schema tables are normalized to 3NF. All attributes in the table are defined by the candidate keys.

1) Account:

AccountID	Balance	IsJointAccount	OpenDate	BranchID	AccountTypeID

2) Account Type:

AccountTypeID	AccountType

3) Account Nominee:

CustomerAccountID	CustomerNomineeID

4) Address:

AddressID	AddressLine1	AddressLine2	Street	City	ZipCode

5) Bank:

Bank ID	Name	BankTotalBalance

6) Biometric:

BiometricID	RetinaID	FaceRecognitionID	FingerprintID	CardNo.

7) Branch:

BranchID	BankID	AddressID	BranchTotalBalance	PhoneNo.

8) Card Details:

CardNo.	CVV	ExpiryDate	Type

9) Customer:

CustomerID	FirstName	MiddleName	LastName	DOB	CustomerAddressID

Gender	ContactDetails	EmailID	Age	BiometricId

10) Customer Account:

CustomerAccountID	AccountID

11) Employee:

EmployeeID	FirstName	MiddleName	LastName	EmployeeAddressID	ContactDetails

Designation	EmailID

12) Employee Branch:

BankEmployeeID	BankBranchID

13) Face Recognition Scan Details

FaceRecognitionID	DistanceofEyes	DistanceofNose	Mouth	JawsEdge

UpperLineofEyeSocket	SidesofMouth	AreaSurroundingCheek	LocationofNoseAndEyes

14) Fingerprint Scan Details:

FingerprintID	Ark	Loops	Whorks	Pro

15) Nominee:

NomineeID	FirstName	MissdleName	Last Name	Contact Details	NomineeAddressID	Email ID

16) Retina Scan Details:

RetinaID	Rings	Furrows	Frackles	Corona

17) Transaction:

TransactionID	Amount	Date	Status

18) Transaction Type:

CustomerTransactionID	TransactionType	CustomerTransactionAccountID

5.2 Relationships and Cardinalities:

- Relationships describe how entities are associated with each other. There are three types of relationships, one to one, one to many, and many to many. These relationships define how entity instances relate.
- Relationships also provide us with critical information about entity interactions.
- In general, each relationship can also have a minimum and maximum cardinality associated with it to show which relationships are optional, which are mandatory and any numerical limitations on these relationships.

Following list shows the important relationships with their cardinalities in Multimodal Biometric Transaction System database design.

1) Account and AccountType relationship (One to One)

2) Account and CustomerAccount (One to One)

3) Account and AccountNominee (One to Many)

4) Branch and Account (One to Many)

5) Account & Transaction (One to Many)

6) EmployeeBranch and Employee (One to Many)

7) Bank and Branch (One to Many)

8) Customer & Biometrics (One to One)

9) AccountNominee and Account (One to Many)

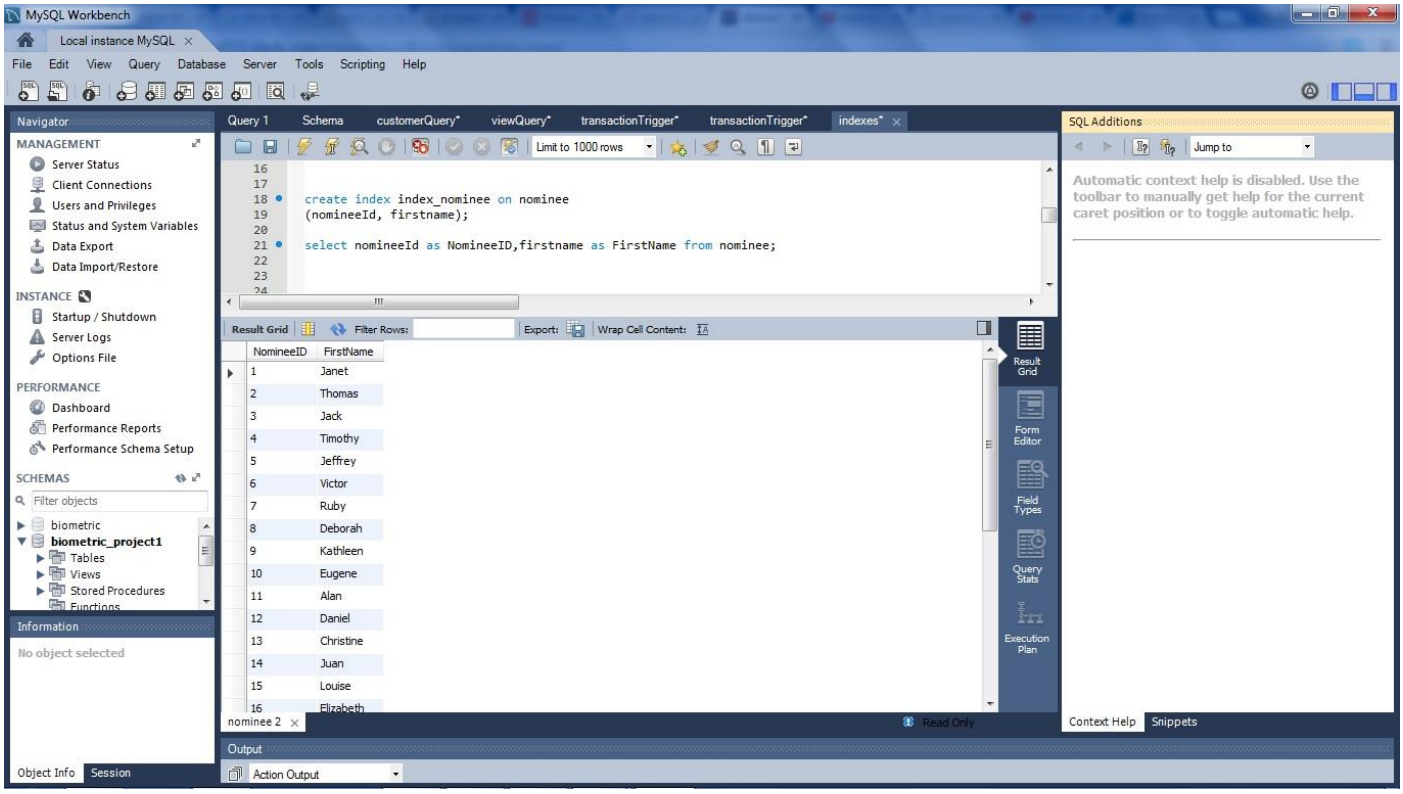
10) Employee and Address (One to One)

11) Transaction and TransactionType (One to One)

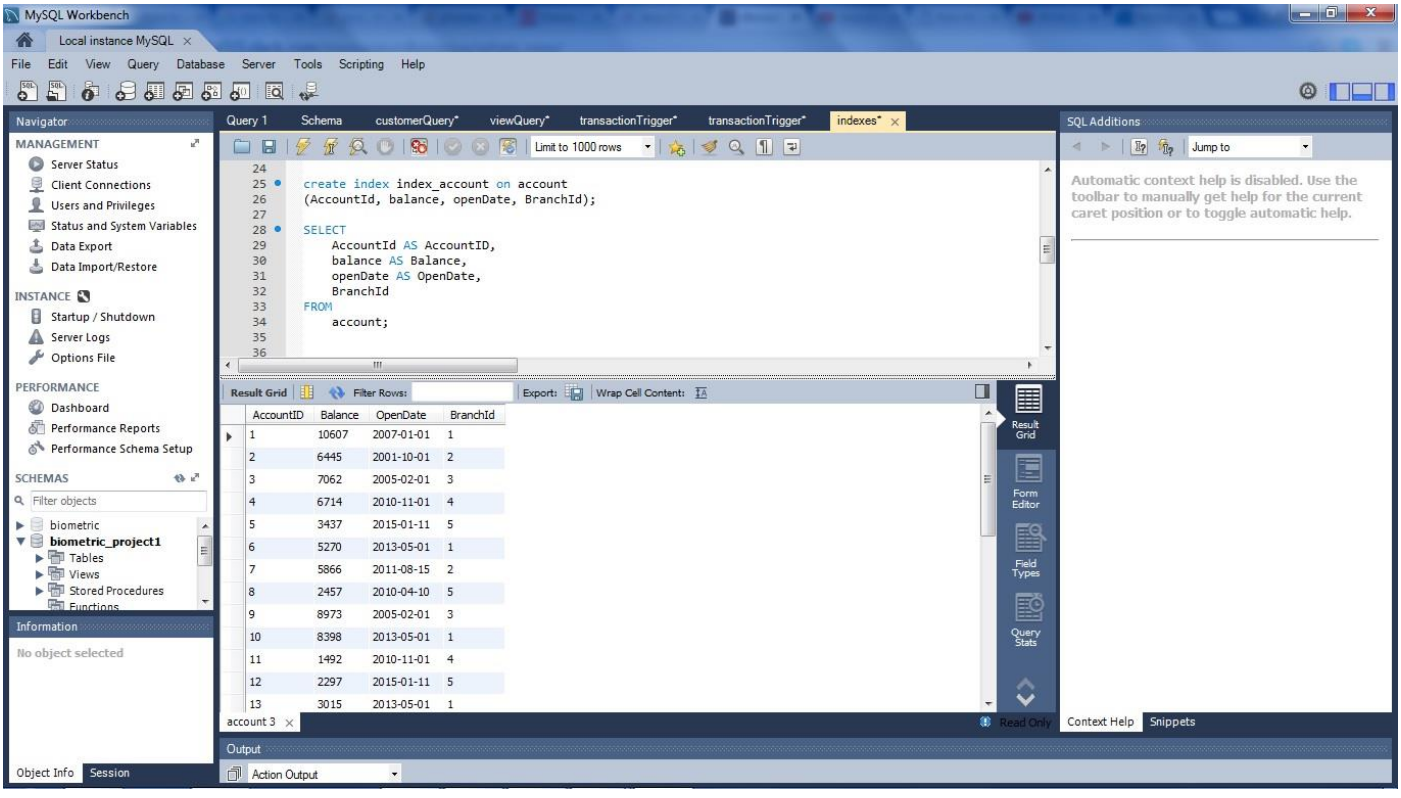
5.3 Queries:

5.3.1 Index:

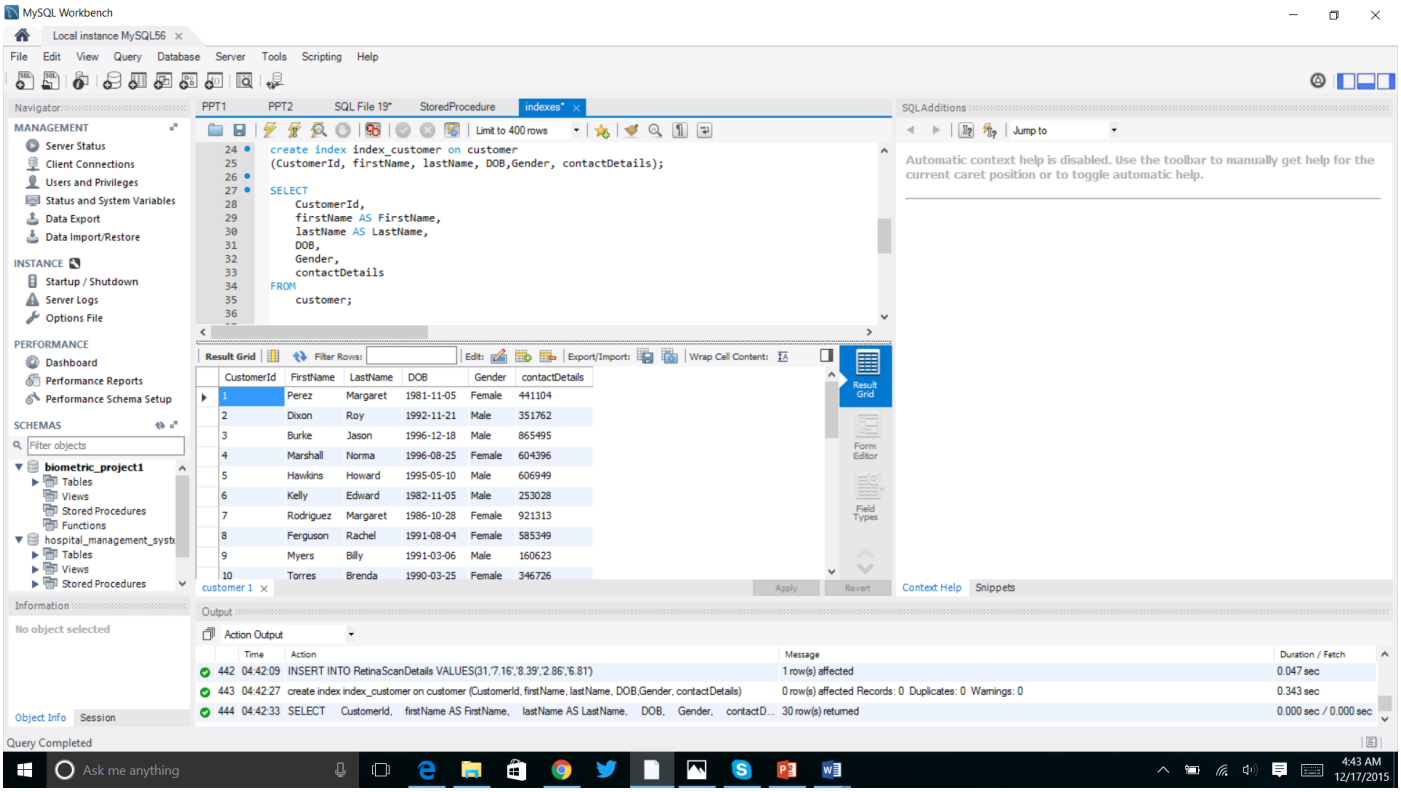
(a) Index on nominee table



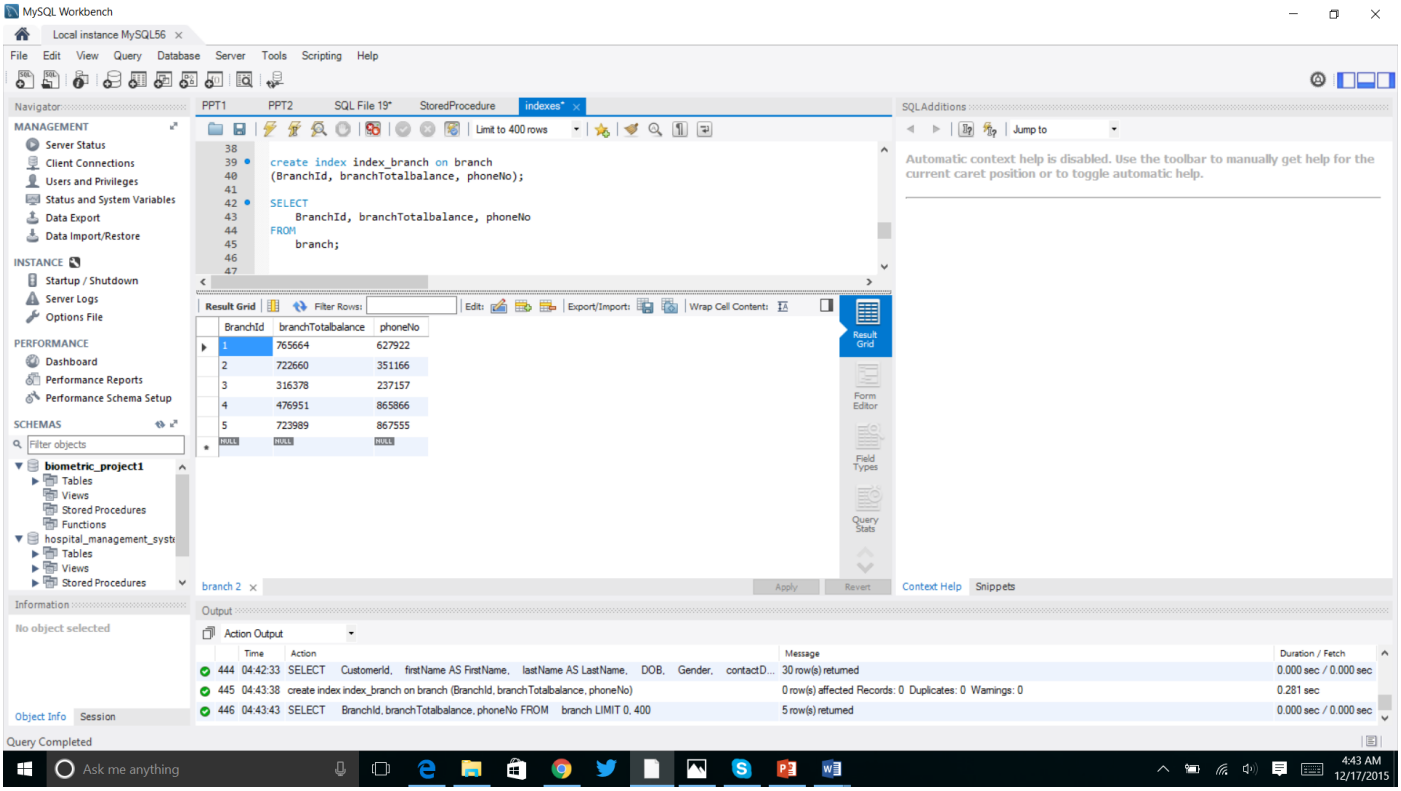
(b) Index on Account table



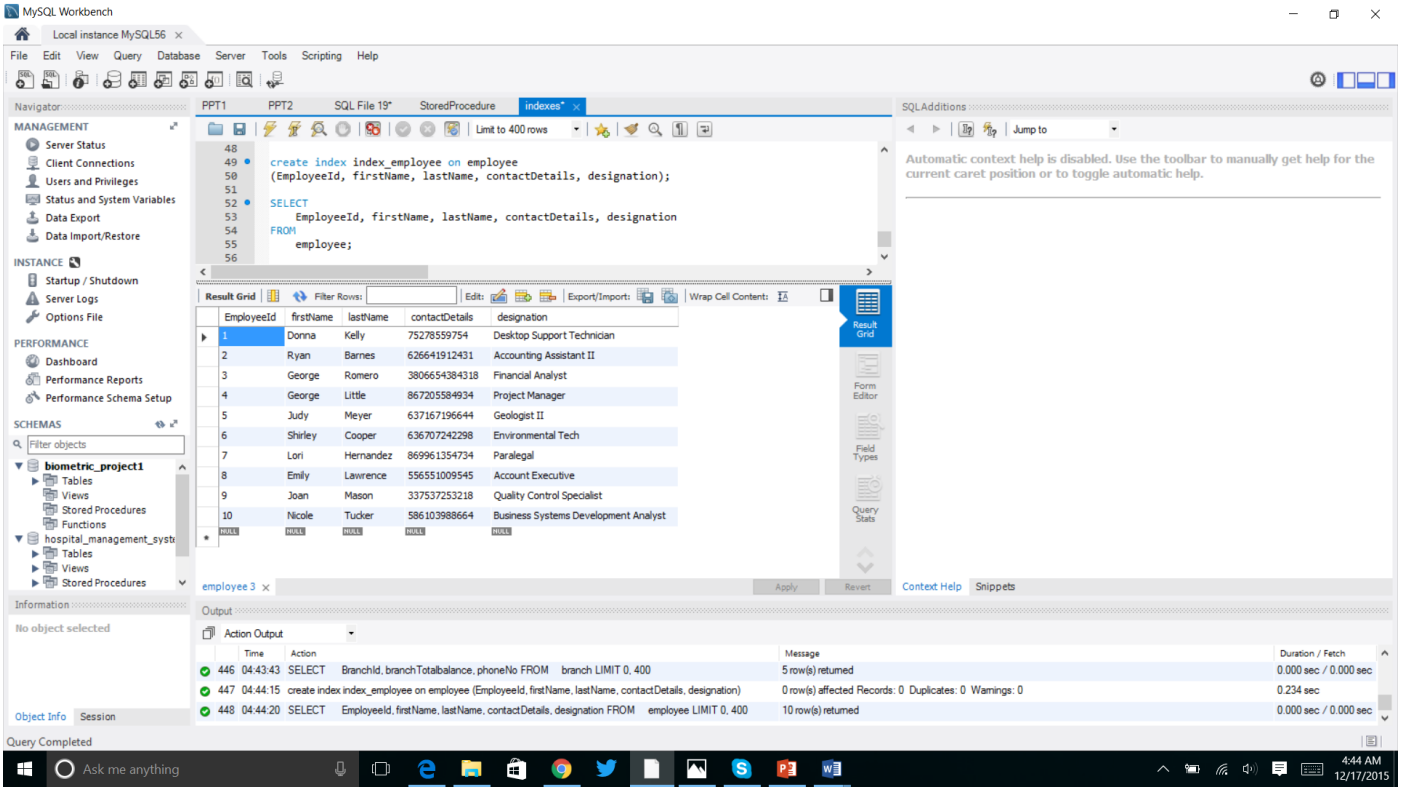
(c) Index on Customer table



(d) Index on Branch table

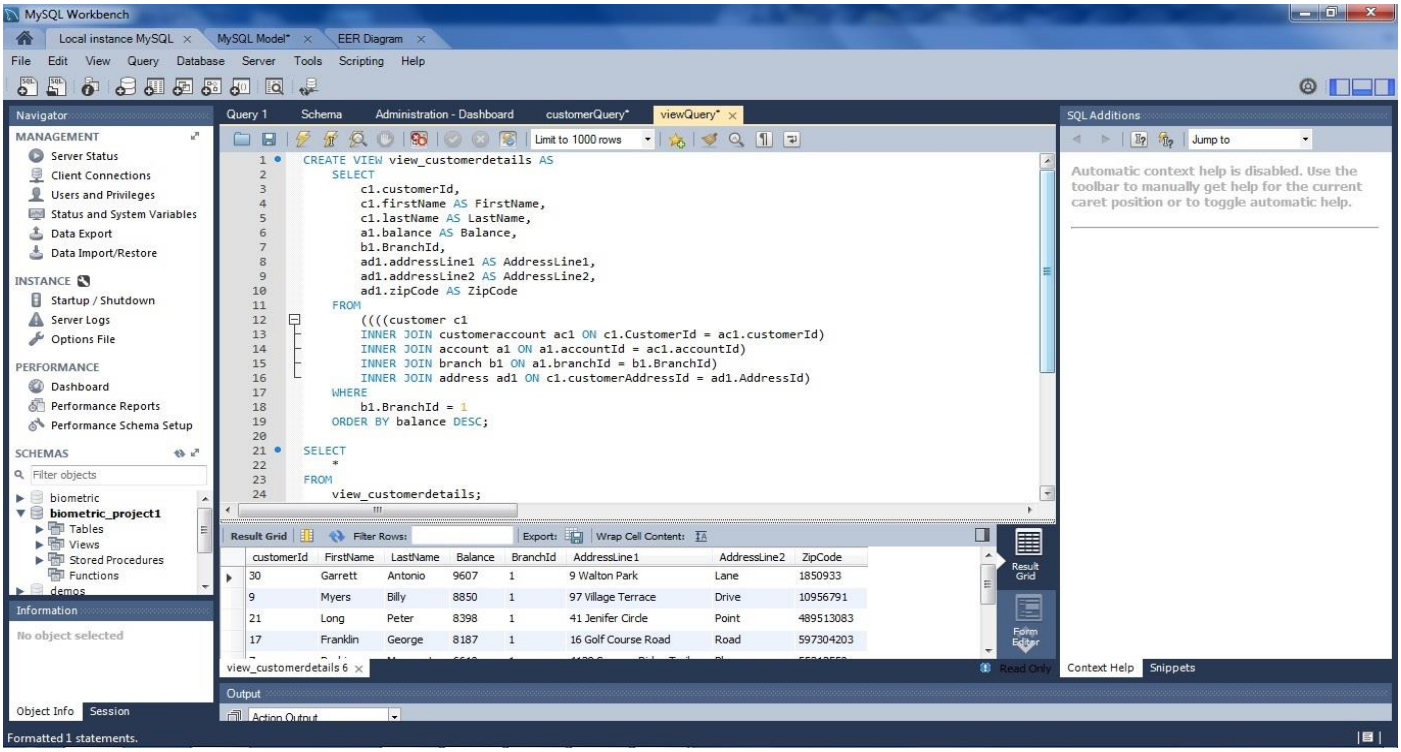


(e) Index on Employee table

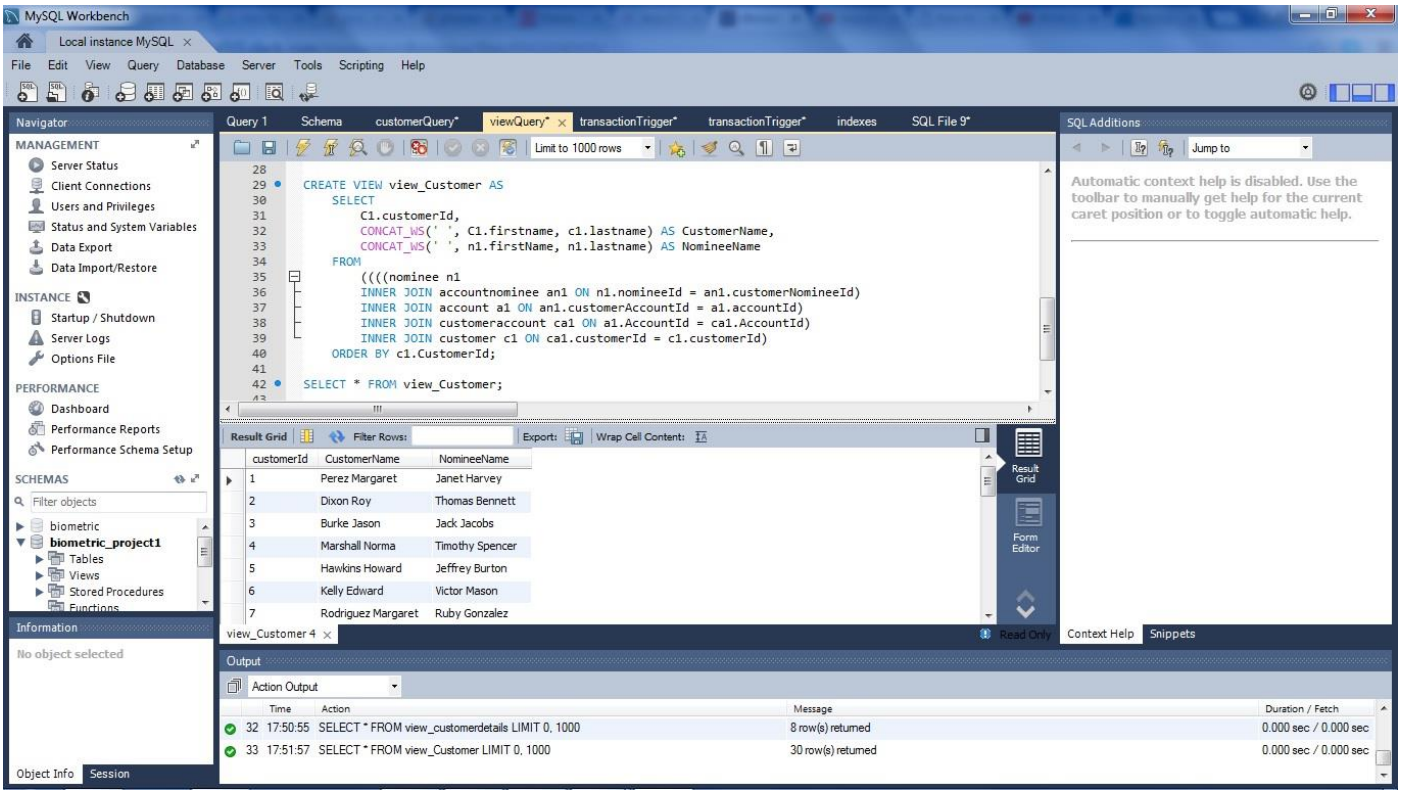


5.3.2 View:

(a) View to show customer details

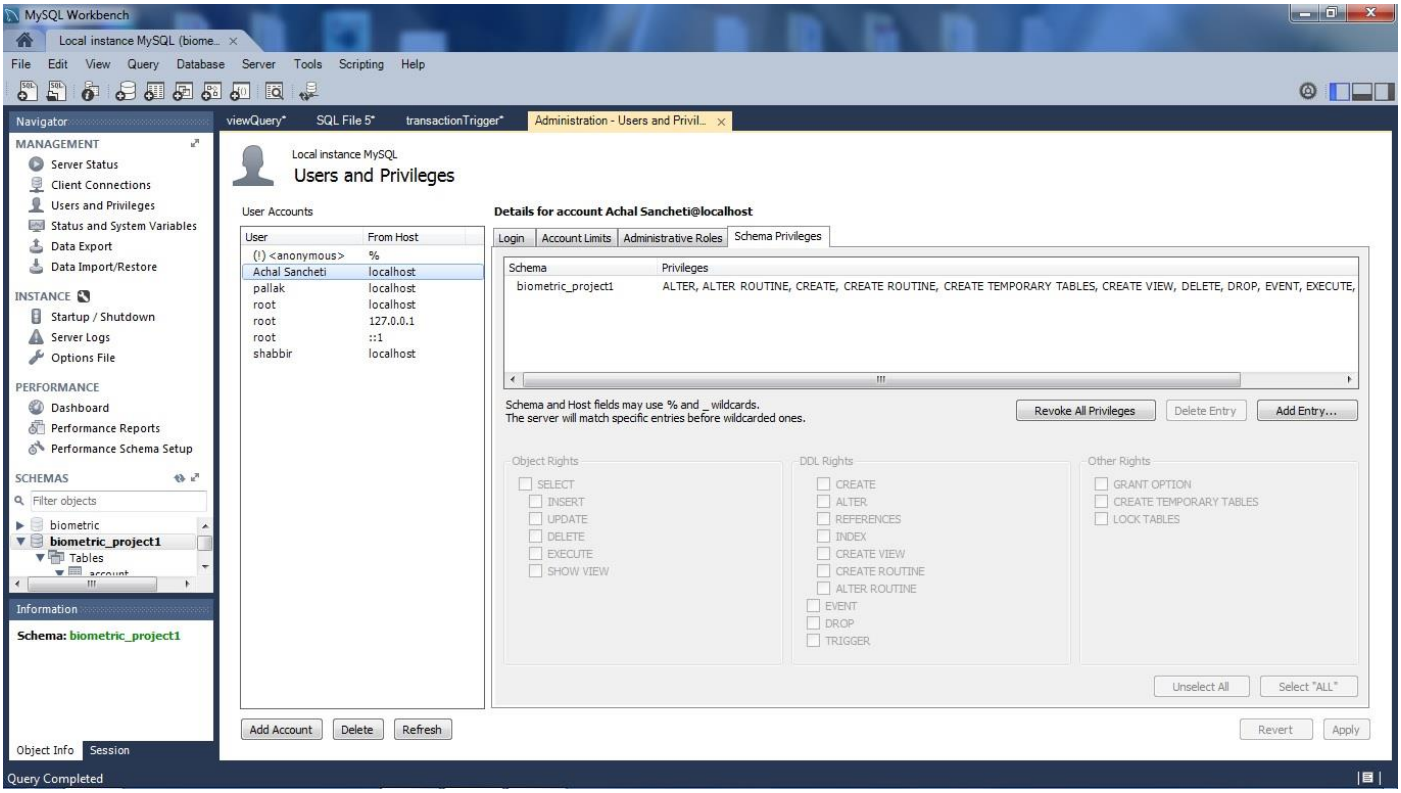


(b) View to show account nominee

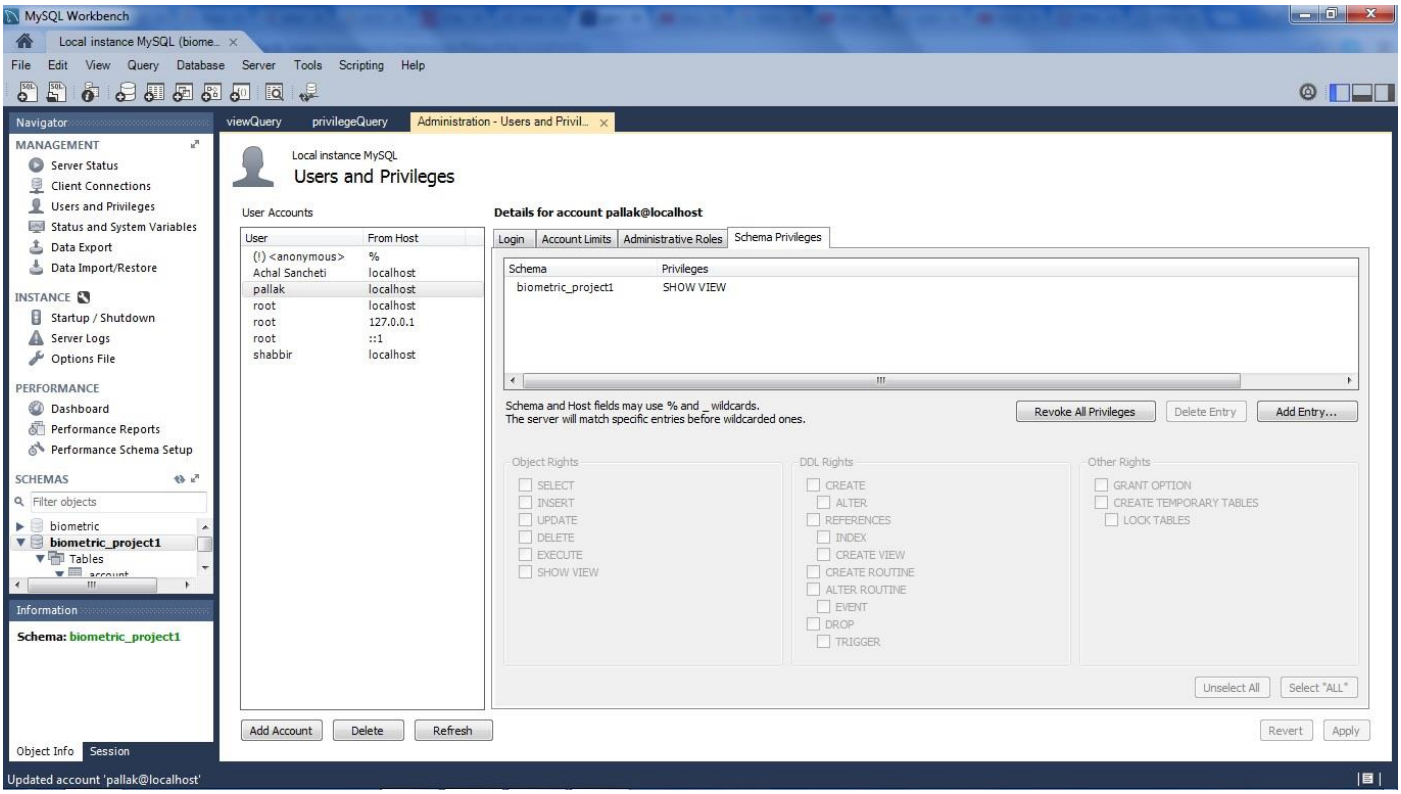


5.3.3 User and Privileges:

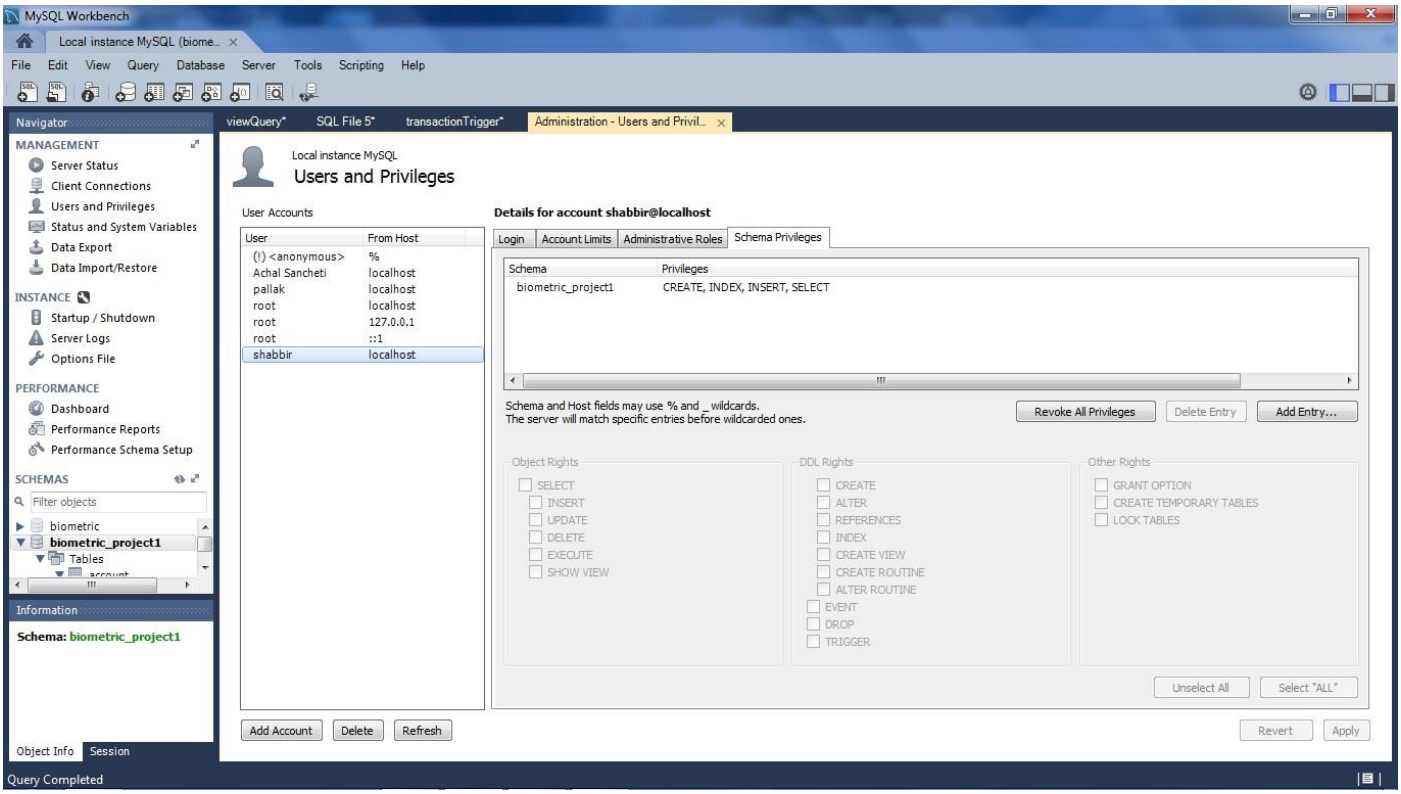
(a) Admin Privilege



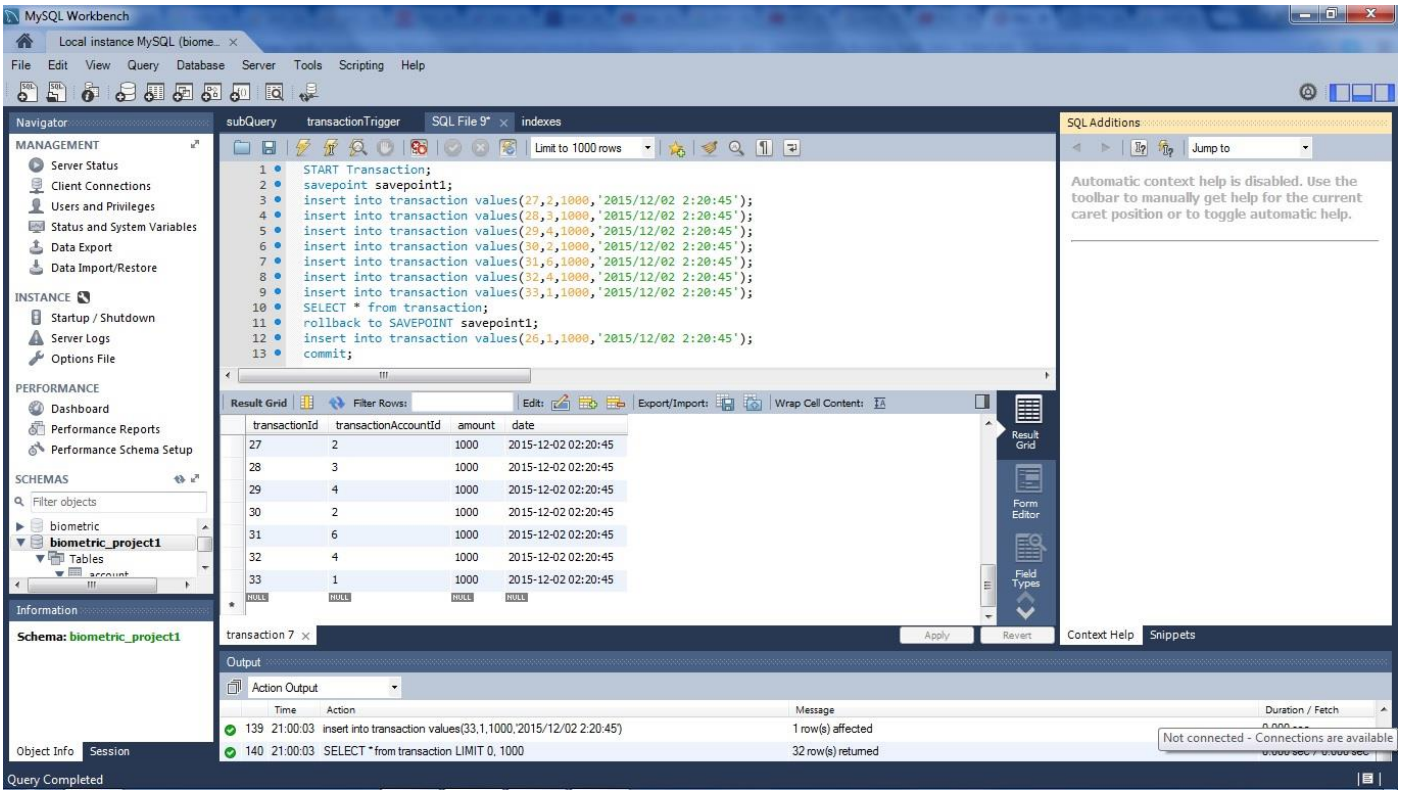
(b) Customer Privilege



(c) Employee Privilege

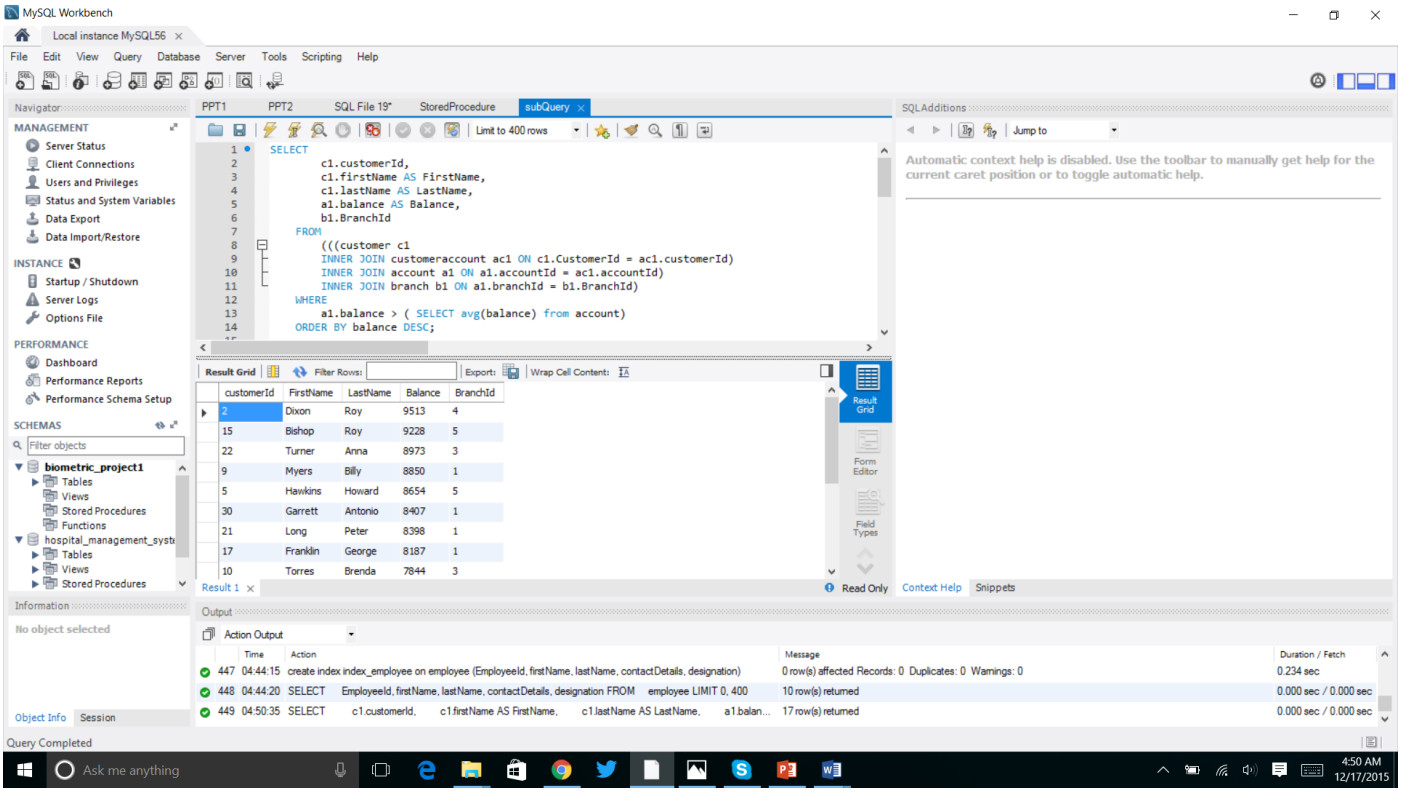


5.3.4 Transaction:



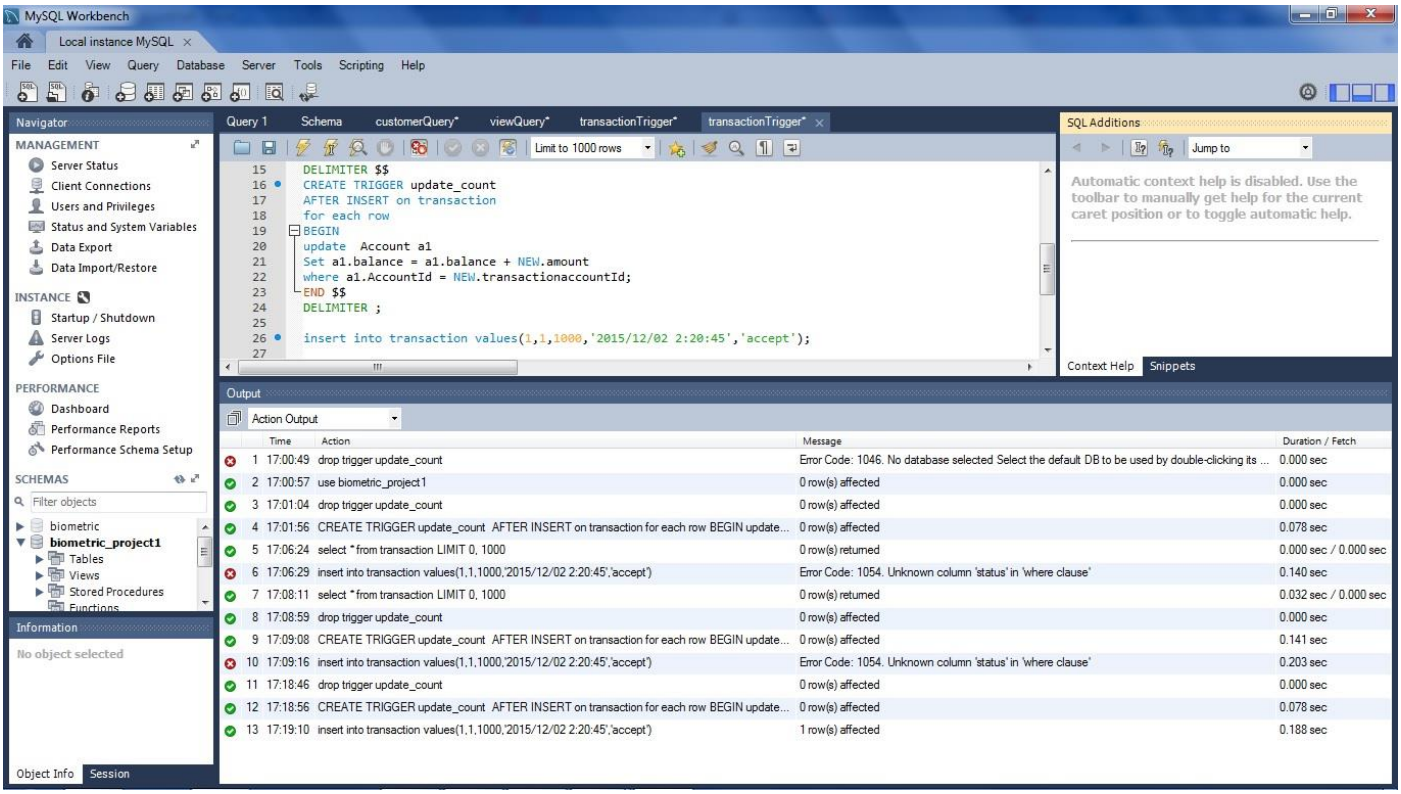
5.3.5 Sub-query:

Sub-query to view customer information

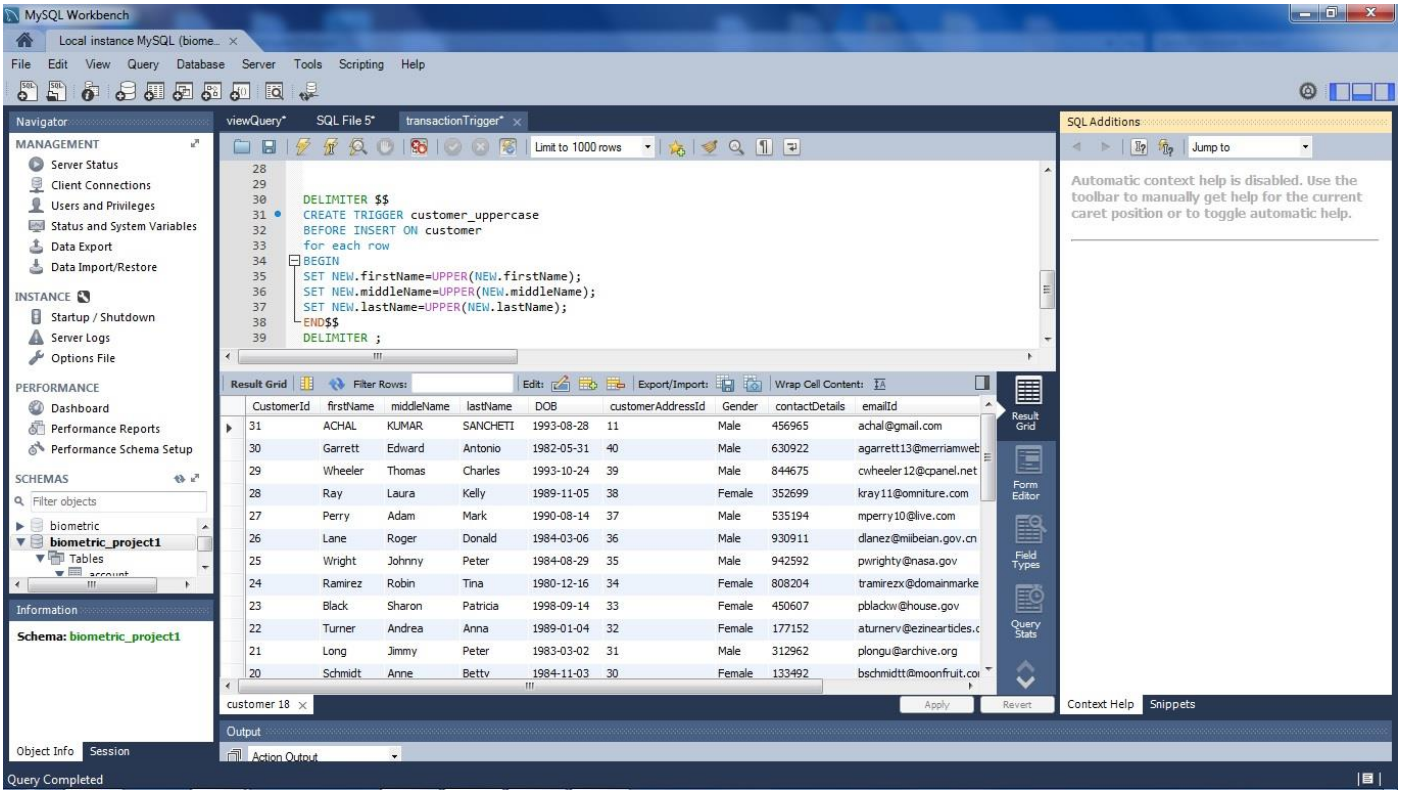


5.3.6 Trigger:

(a) Trigger to update balance for any transaction

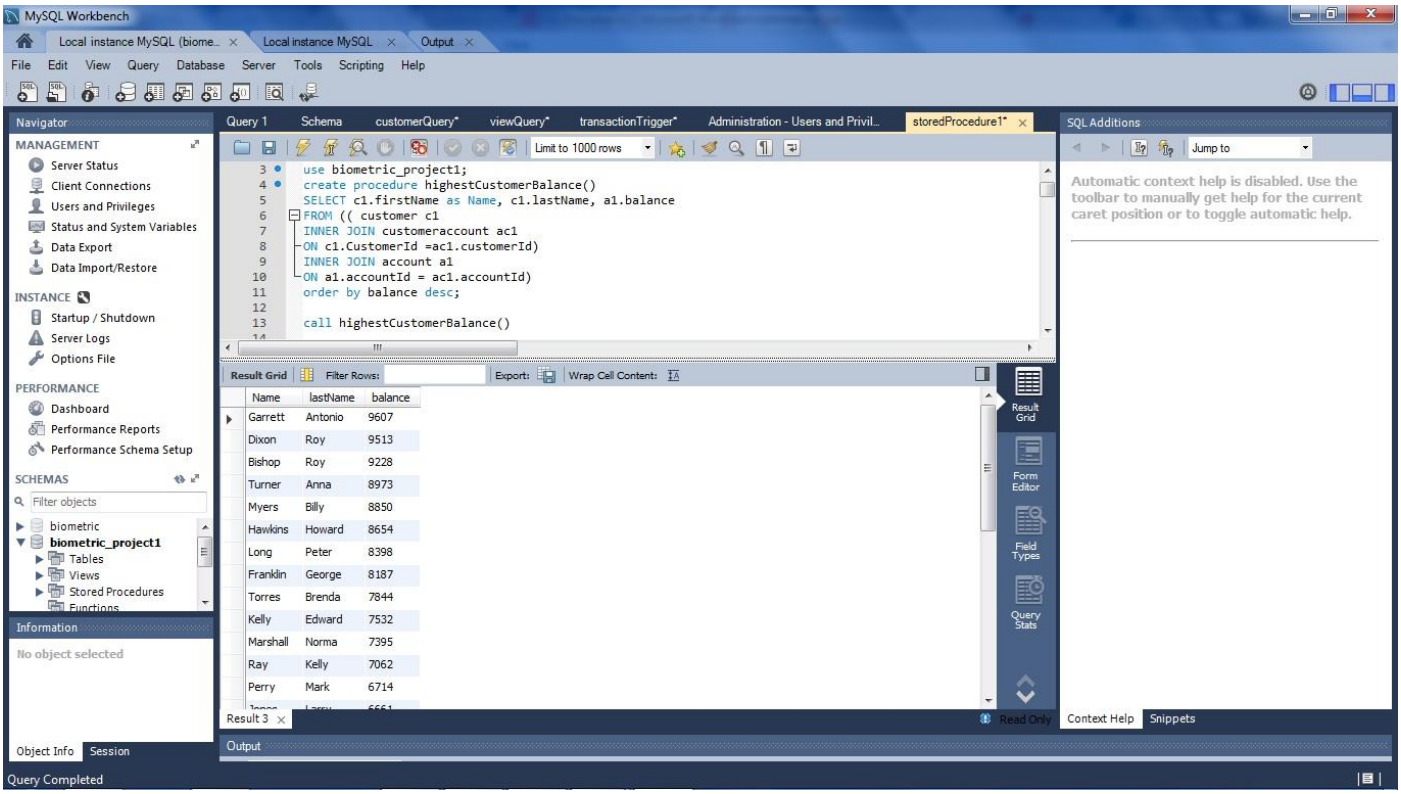


(b) Trigger to change the case of letter on insertion

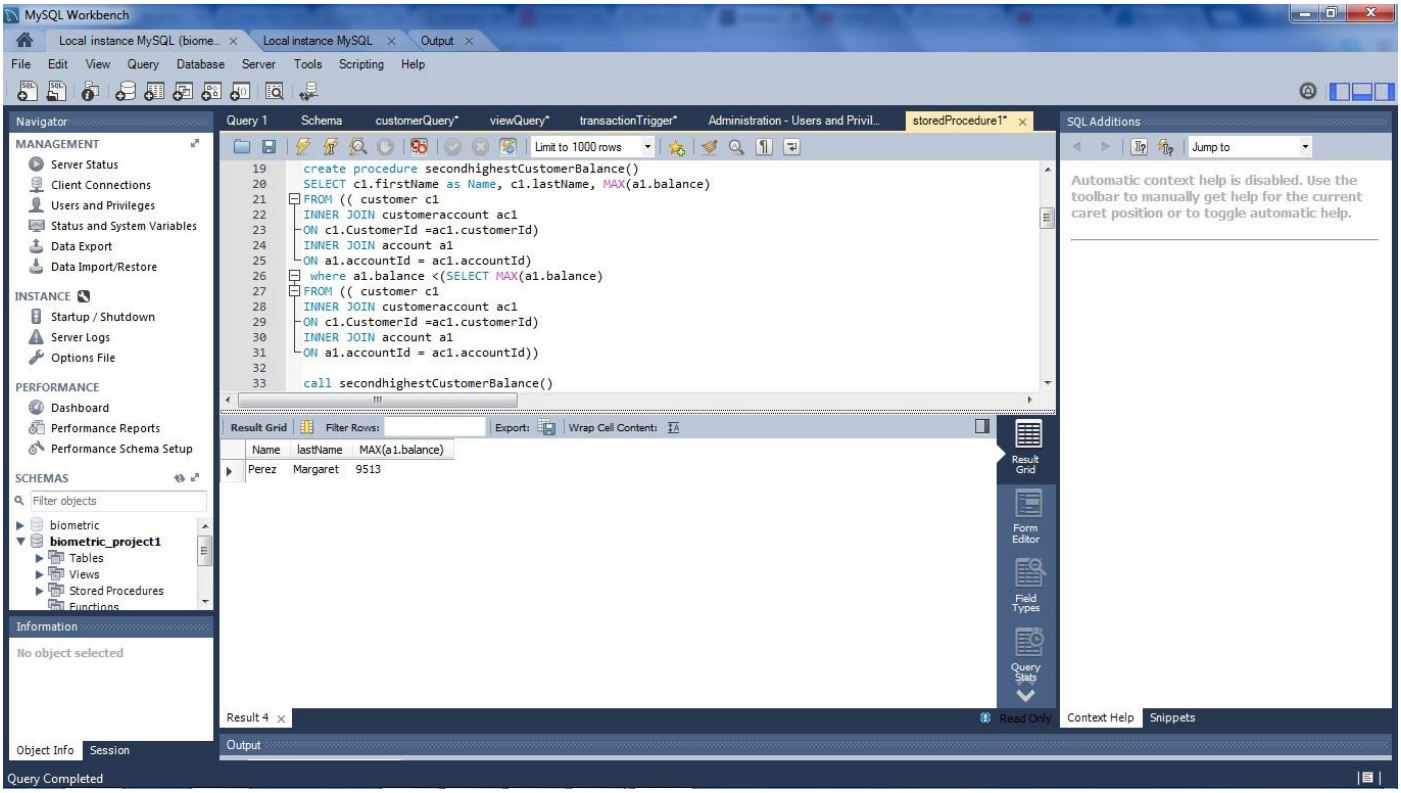


5.3.7 Stored Procedure:

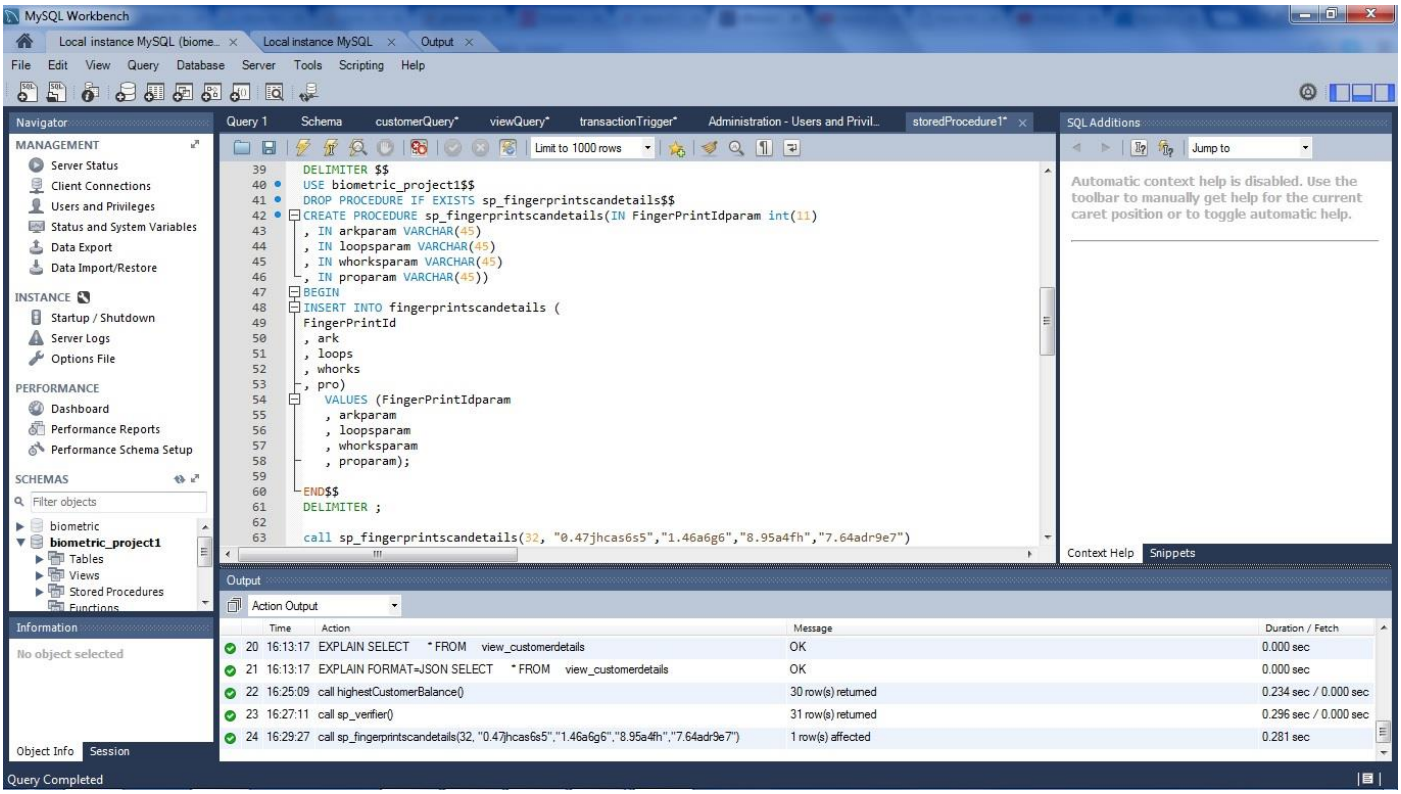
(a) Stored Procedure to find highest balance of customer



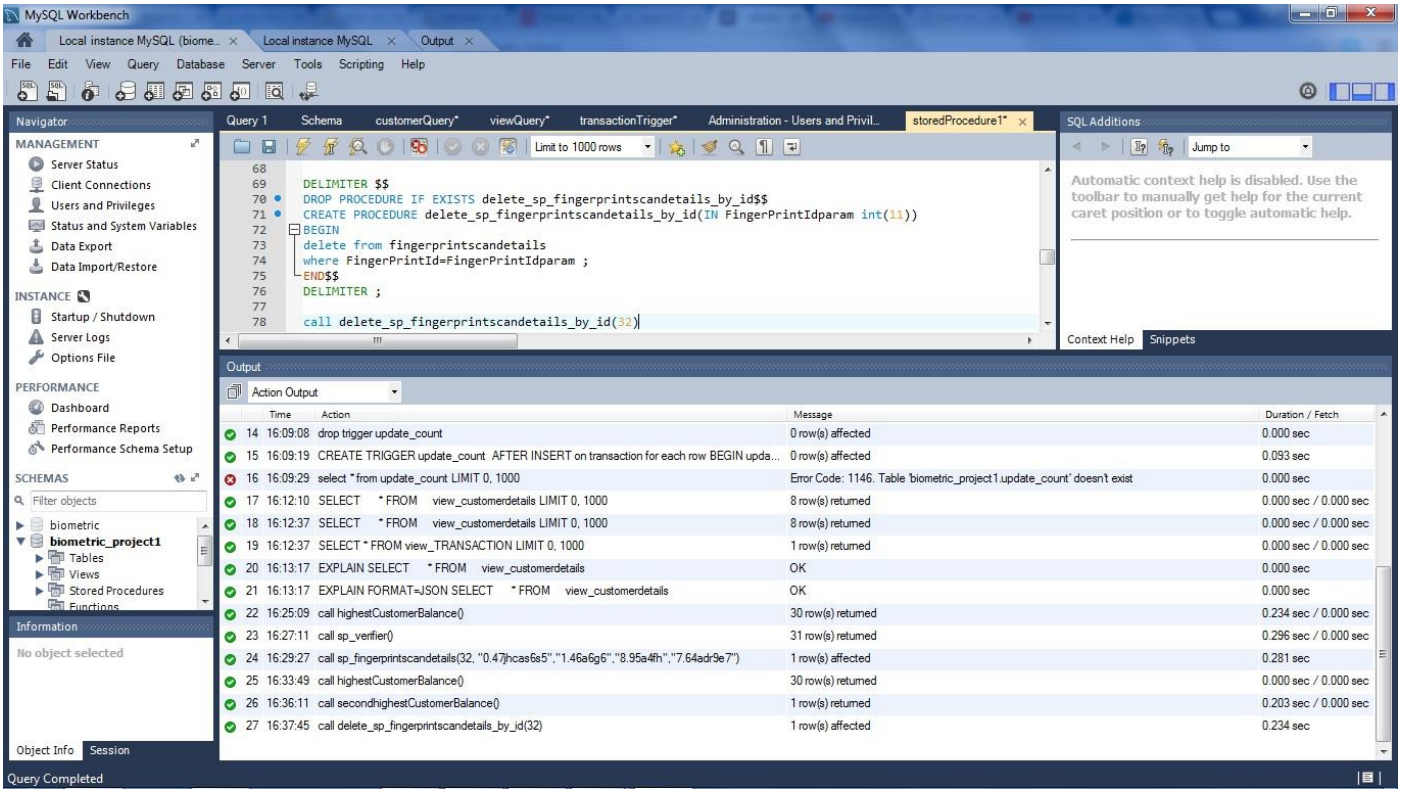
(b) Stored Procedure to find second highest balance of customer



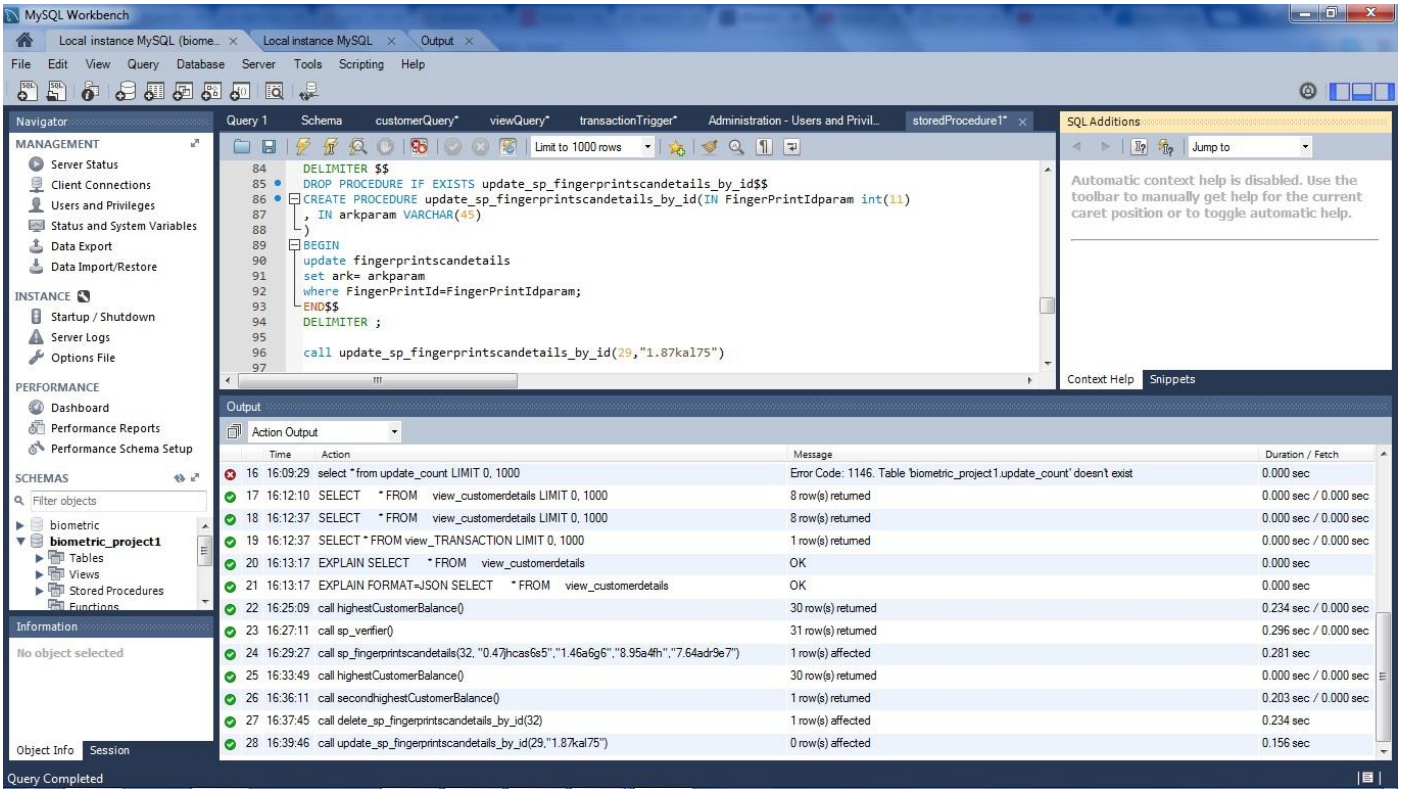
(c) Stored Procedure to insert data in fingureprintscandetails table



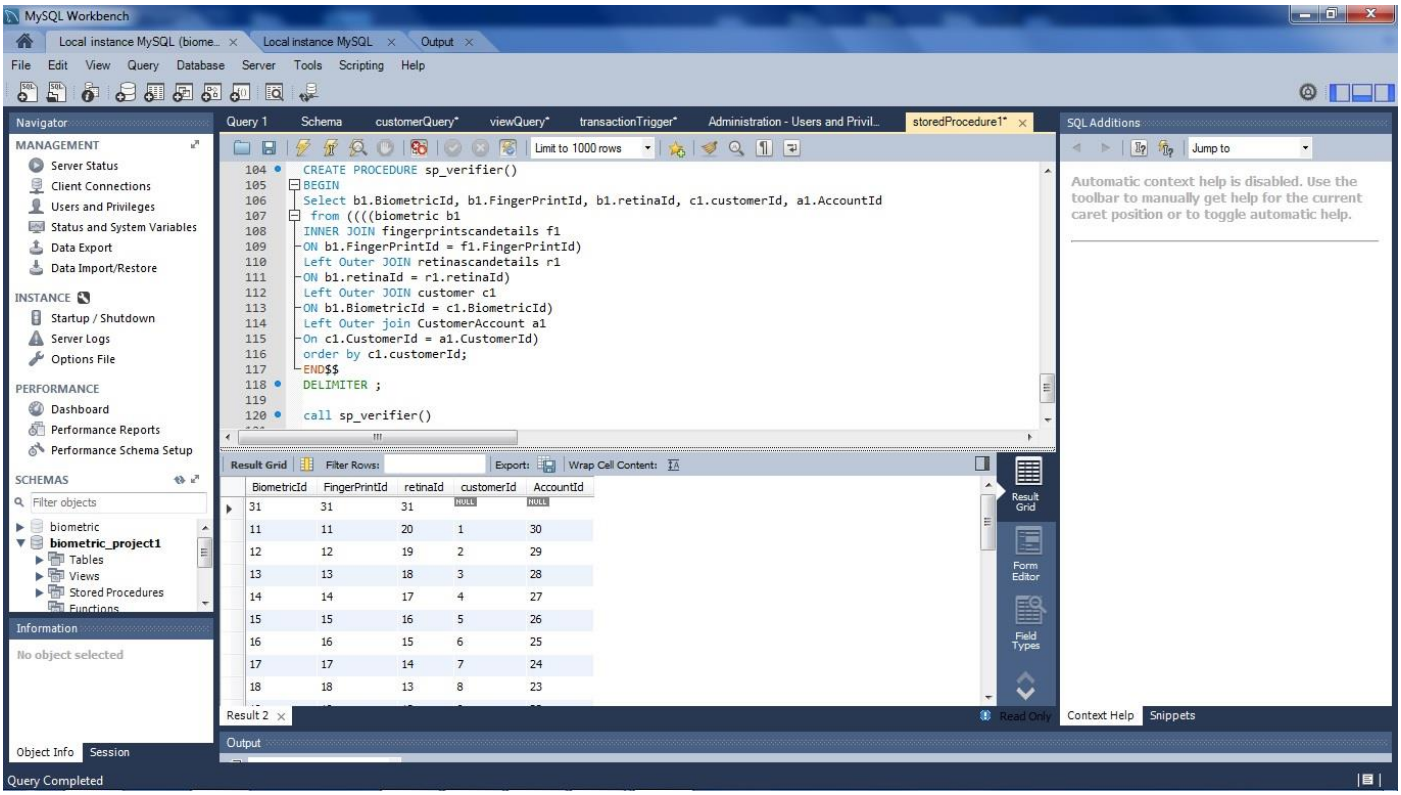
(d) Stored Procedure to delete a row from fingerprintscandetails table



(e) Stored Procedure for update data in fingureprintscandetails table



(f) Stored Procedure to verify customer using two biometrics



CHAPTER – 6

6.1 Backup Strategy:

- Backups can guard against data loss, support compliance and retention needs and protect the business from disaster.
- Back up strategy used for project is RMAN (Recovery Manager/Oracle Database Manager).
- Fast Recovery Area (FRA) – A disk location in which database can store and manage back up & recovery files.
- Strategy: Back up of FRA sized for 7-day retention on disk using a weekly full, daily incremental back-up and archived logs.
- Weekly tape back -up maintained for 90 days.
- Monthly tape back -up for 7 years.
- RMAN back up optimizes disk utilization space.

CHAPTER – 7

7.1 Key Benefits:

- Uniqueness
- Biometrics is the only means of determining “who” is actually using the system.
- High level of security.
- Very high accuracy.
- Minimizing frauds.
- Card-less feature in ATMs.
- Spoof reduction in cash less transactions.
- Ease of access and convince.
- Easier to use verification solutions.
- Most definitive, real time tool today.
- Universality
- Permanence
- Measurability
- User friendliness
- Comfort

CHAPTER – 8

8.1 Assumptions:

- We have assumed that all the customers maintain their account in a single bank.
- Customer's biometrics are stored in database at the time of account creation.
- Biometric data is stored as random strings in database.

8.2 Future Scope:

- Online transaction scenario can be changed using various smart devices in addition to our database.
- Key Stroke Patterning, Fingerprint palettes and other more behavioral biometrics can be implemented.
- Cars, automobiles and other automatic devices can be operated using biometrics.

CHAPTER – 9

9.1 References:

- https://dev.mysql.com/doc/refman/5.7/en/innodb-introduction.html
- https://technet.microsoft.com/en-us/library/aa933055(v=sql.80).aspx
- https://www.daniweb.com/programming/databases/threads/439533/how-to-store-an-image-in-mysql-database
- www.mysqltutorials.org
- www.w3schools.com
- http://dev.mysql.com/doc/refman/5.7/en/commit.html
- http://www.tutorialspoint.com/mysql/mysql-transactions.htm