**Chapter 8 – Team Project - Implementing Security Features for the Team Project**

Read the sample project steps for this chapter and apply the same techniques to the team project that you are developing. Use the normalized purely relational database you created at the end of chapter 6. For the team project, do the following:

**Step 8.1 – Design a value-independent view that hides some sensitive/private information. Then execute the value-independent view in the database.** Show your work by providing screenshots of executing the CREATE VIEW SQL statements in the database.

Ans 1. The LocationandCost view will be of Job1 table, but without employee id(empid) , event, date, or Contract no.

CREATE VIEW LocationandCost AS

SELECT Location, Type, Cost, Duration

FROM Job1;

Table

Description automatically generated

2. Value dependent view

CREATE VIEW EventandCostinfo AS

SELECT \* FROM Job1

WHERE TYPE='wed' AND cost > 120;

Ans : Table

Description automatically generated with medium confidence

**Step 8.2 - Create a user and authorize that person to read the view. Connect to the database as the new user and demonstrate (provide screenshots) that the new user can read the view. Draw an authorization graph by hand or by using a drawing tool, showing the privileges given.**

**Ans. 1. SQL commands:** CREATE USER Gaurav22 IDENTIFIED BY Test123456789;

GRANT SELECT ON EventandCostinfo TO Gaurav22;

Figure 1:A screenshot of a computer

Description automatically generated with medium confidence

Figure 2:

**Table

Description automatically generated**

**Step 8.3 – Create and authorize four other users to access and/or modify various parts of the database. For each new user, connect to the database and demonstrate (provide screenshots) that each new user can access the various parts of the database that you granted. Draw an authorization graph by hand or by using a drawing tool, showing the privileges given.**

**Ans. CREATE USER Sanjay IDENTIFIED BY Test123456789;**

**CREATE USER Samyukta IDENTIFIED BY Test123456789;**

**CREATE USER Sphurti IDENTIFIED BY Test123456789;**

**CREATE USER Omer IDENTIFIED BY Test123456789;**

**GRANT ALL PRIVILEGES ON Payment TO Sanjay;**

**GRANT SELECT,UPDATE ON Payment TO Samyukta;**

**GRANT ALL PRIVILEGES ON Payment TO Sphurti;**

**GRANT SELECT,UPDATE ON Job1 TO Sphurti;**

**GRANT SELECT,UPDATE ON Client TO Omer;**

**GRANT CREATE SESSION TO Sanjay;**

**GRANT CREATE SESSION TO Samyukta;**

**GRANT CREATE SESSION TO Sphurti;**

**GRANT CREATE SESSION TO Omer;**

**Text, letter

Description automatically generatedGraphical user interface, text

Description automatically generated with medium confidenceText, letter

Description automatically generated**

**Table

Description automatically generatedTable

Description automatically generated**

**Table

Description automatically generated with medium confidenceTable

Description automatically generated**

**Step 8.4 - Design an audit trail trigger for updates to a sensitive/private item. Then create the audit trail trigger in the database.** Show your work by providing screenshots of creating the trigger in the database.

**Step 8.5 – Design and execute SQL statements to demonstrate that the trigger is working as expected.** To demonstrate that the trigger is working as expected, provide a screenshot of the data before and after the trigger is executed.