CT069-3-3 - Database Security Assignment

Case Study

APU Sports Equipment Private Limited is an established store selling sports equipments in Bukit Jalil, Kuala Lumpur. It sells various categories of locally produced and imported equipments of high quality. You have been tasked to design and develop a secure database system for APU Sports Equipment Private Limited to securely manage their operations.

Following are details that must be considered to design and develop the database system.

General

1. There are several categories of equipments such as Balls, Rackets, Bats and Nets.

2. For each item, details such as equipment name, price per unit, category it belongs to, quantity in stock, country it was produced are stored.

3. Imported items are taxed at 10% of the item price.

4. Sometimes the store offers discounts on the items it sells. Discounts are based on categories.

5. Members can access the database system to browse and purchase one or more items of the same type or different type. Membership details stored are a unique member id, national registration id or passport number, name, address, phone number, member status (active, expired) and login id. National registration id or passport number must be encrypted.

6. For each transaction, important details such as member id, transaction date, items purchased, quantity purchased.

7. Any purchased items can only be returned within 3 days.

Security

1. Security and permissions must be managed using SQL Roles.

2. Members
   a. must be able to update their own membership details only
   b. must be able to check, add, update and delete their own transactions only
      Note:
      - *Add refers to purchase new items*
      - *Update refers to change item quantity (add/removeNo other details can be updated for that transaction*
      - *Delete represents item return.*

3. Store Clerks
    a. must be able to manage (add, update, remove) all data except membership and transaction details
    b. must be able to view all transaction records (full details) but not modify them
    c. must be able to add new membership data
    d. must be able to view and update non confidential membership data
    e. should not be able to view any member’s confidential data

4. Database Administrators (DBA)
    a. All DDL queries can only be performed by database administrators (DBA). No other users shall be able to run any DDL queries
    b. Should not be able to view any member/user confidential data

5. Management
    a. Management staffs must be able to query all tables but not make any changes to it.
    b. Should not be able to view any member’s confidential data

Note: You are free to make any other logical assumptions to make your solution complete.

General Requirements:

In this assignment you are required to:

- Work in a group of **minimum 2 / maximum 4** members. Provide workload matrix, providing details on the distribution of work amongst group members. For group components, each member is required to participate in all tasks. All work must be equally distributed among team members.
- Design, implement and document the solution based on the case study and any assumptions that you made.
- Submit a written report through Moodle before/on due date and time given by module lecturer.
- **Wherever individual work is mentioned, each member’s contribution/work must be unique / different from other group member**. Any sections not done by an individual member, will not be given marks for that person.
- **Wherever group work is mentioned, each member’s contribution/work must be mentioned as percentage contribution.** Any sections not contributed by an individual member, will not be given marks for that person.

Deliverables

A. Initial Report / Implementation (25%)

B. Final Report (35%)

Initial Report - Implementation (100 marks)

1. **Relational Database Implementation with Integrity and Redundancy Controls**

Deliverables & Break down:

- **Group work – 10 marks**

  Each group must produce a Data dictionary that can be used to implement your solution (data):

  i) All field must be clearly defined (field name, field type, length, default value if any, valid values if any) in the data dictionary.

  ii) Each table must be assigned an owner (team member) who is responsible to create and populate the table, audit the DDL and DML events for that table and secure the table.

  iii) The data dictionary must be accompanied with some explanations.

- **Individual work – part A – 10 marks**

  Each member must produce a set of SQL queries with proper explanations for the tables they own as defined in the data dictionary.

  i) SQL queries that create tables and views.

  ii) SQL queries that populate the tables – must include encryption for the relevant table. Show a maximum of 5 rows for each table. If need to show more, please attach in appendix.

  iii) SQL query/queries that can produce details of transactions that happen in the last *n* days where n = {1,2,…., 7}

  Note: Attach the code as appendix. Give proper naming to it. Use it when explaining you code in the main text.

- **Individual work – part B – 10 marks**

  Each member must produce a set of SQL queries to implement one trigger with proper explanations. The trigger can be a DDL or DML trigger. Examples: trigger to protect a table or column from accidental deletion, trigger to perform some form of validation, trigger to perform some form automation (automatic computation), trigger to automatically create a database user or disable a database user etc.

  Note: Attach the code as appendix. Give proper naming to it. Use it when explaining you code in the main text.

2. **Database Encryption**

<u>Deliverables & Break down:</u>

- **Group work – 20 marks**

  Each group must produce a complete set of steps and SQL queries with proper explanations and outputs to

  i) Create a view that will show member full details including automatically decrypting the encrypted values if run by a user in the Members role. This view should be accessible by Members only. It must also show only the users own details only (implement row level security).

  ii) Create a view that will show member full details and hides any encrypted values. This view can be accessed by Store Clerks and Management only.

  iii) Encrypt a database (TDE) or encrypt the backup (for databases without TDE) from one MS-SQL instance and restore into another MS-SQL instance

  Note: Attach the code as appendix. Give proper naming to it. Use it when explaining you code in the main text.

3. **User Permission Management**

<u>Deliverables & Break down:</u>

- **Group work – 10 marks**

Each group must produce an authorization matrix for all the roles with proper explanations:

i) All permission settings at all levels (database, table & view, column) must be identified and defined in the authorization matrix.

ii) Each authorization must be assigned an owner (team member) who is responsible to write SQL queries to implement the authorization.

- **Individual work– 10 marks**

  i) Each member must own the implementation of a minimum one role - produce a set of steps and SQL queries with proper explanations to completely implement the authorization as defined in the authorization matrix

Note: Attach the code as appendix. Give proper naming to it. Use it when explaining you code in the main text.

4. **Database Auditing**

<u>Deliverables & Break down:</u>

- **Group work – 30 marks**

  Each group must produce a complete set of steps and SQL queries with proper explanations to capture and audit the activities as listed below

  i) Login and logout

  ii) Database structural changes

  iii) Data changes

  iv) User permission changes.

Note: Attach the code as appendix. Give proper naming to it. Use it when explaining you code in the main text.

<u>Demo</u>

Sample scenarios that may be asked of you to demo

1. What happens if a user is returning an item within or after 3 days
2. How the equipment data is protected by accidental deletion by users
3. Who have accessed the Member data and performed what actions to it

Final Report (100 marks)

1. Entity-Relationship Diagram, & Relational Model

Deliverables & Break down:

- **Group work – 30 marks**

Each group must produce:-

i) An ERD that models the business requirements in this case study: All relevant attributes, relationships, cardinality, participation, primary and foreign keys must be identified in the ERD. The ERD must be accompanied with some explanations.

ii) A Relational Model (set of relations) that implements the ERD: All relevant relations and fields including primary and foreign keys must be identified in the Relational model. The relational model must be in 3rd Normal Form (3NF). The list of relations must be accompanied with some explanations.

Note: ERD and Relational model is not the database diagram. No marks will be given if you show DB diagram instead of ERD or a set of relations.

2. Backup and Restore Strategy

Deliverables & Break down:

- **Group work –20 marks**

  Each group must **propose** and justify an effective backup and restore strategy that can be implemented for your solution. You need present at least two options and then choose one and then justify why you chose it instead of the other(s).

3. Confidential & Integrity

Deliverables & Break down:

- **Individual work – 30 marks**

  Each member must discuss & document on how your work contributes to ensure Confidential & Integrity is achieved in your solution as reported in the Initial Report. Discussion must include justifications for the approaches taken. Each member must discuss only their part.

4. Key Learnings

Deliverables & Break down:

- **Individual work – 20 marks**

  Each member must write their **own learnings and experience in their own words**. Discussions should include what they have learned through this course, challenges doing the Database Security assignment/project and research done to address those challenges.