**AYEBARE MOSES**

**A95561**

**S21B23/032**

1. **Define normalization and how it has been applied in my project.**

Normalization is the process of organizing data in a database. It aims at reducing data redundancy and ensuring that only related data is stored in a particular table. This is done by creating tables and creating relationships among those tables according to the way in which the database has been designed. In my database project, I applied this concept by creating Tables for my all data and assigning each of them primary keys for unique identification. Furthermore, I created join tables to establish relationships among my tables and each of these tables had foreign keys referring to primary keys in the tables that they were joining.

1. **Define the different transaction anomalies giving examples from your project and how they can occur.**

Anomalies in general are the result of not normalizing your database. This is because there will be a lot of redundancy in your database as a result.

There are mainly three types of anomalies in databases namely;

**Update anomaly**: This happens when one has to make changes to existing data in the database. If that data is stored redundantly in the database, then the person making changes might end up missing to change an entry. In my database, it can occur when someone wants to change everyone that is flying with Emirates to another airline. Since there are many people using that airline, it is possible that not everyone will get that change.

**Insert anomaly**: This occurs when data cannot be added to a database without other entries of data. In my database, it can occur when someone wants to go to a particular airport without stating what airport they will be departing from.

**Delete anomaly**: This anomaly occurs when deletion of unwanted particular data causes the deletion of other relevant data in the database. In my database it can occur when the airline Emirates is deleted which can cause all the information of those that flew with it to be lost as well.

1. **Suggest ways in which the security of your database is enhanced**.

**Set up an HTTPS proxy server:** A proxy server evaluates requests sent from a workstation before accessing the database server. In a way, this server acts as a gatekeeper that aims to keep out non-authorized requests. The most common proxy servers are based on HTTP. However, if you’re dealing with sensitive information such as passwords, payment information or personal information, set up an HTTPS server. This way, the data traveling through the proxy server is also encrypted, giving you an additional security layer.

**Use real-time database monitoring:** Actively scanning your database for breach attempts increases your security and allows you to counter potential attacks. You can use monitoring software to log all actions taken on the database’s server and alert you of any breaches. Another aspect to consider is regularly auditing your database security and organizing cybersecurity penetration tests. These allow you to discover potential security vulnerabilities and patch them before a potential breach.

**Use database and web application firewalls:** Firewalls are the first layer of defense for keeping out malicious access attempts. On top of protecting your site, you should also install a firewall to protect your database against different attacks.

**Create regular backups of your database:** While it’s common to create backups of your data, it’s essential to create backups for your database regularly, as well. This reduces the risk of losing sensitive information due to malicious attacks or data corruption.

**Separate database servers:** Databases require specialized security measures to keep them safe from cyberattacks. Furthermore, having your data on the same server as your site also exposes it to different attack vectors that target websites. To mitigate security risks, separate your database servers from everything else.

**Use strong passwords/authentication means:** Implementing strong passwords is the first step you can take to strengthen your security in this area. Use reasonably complex passwords and change them at least every 90 days. Don’t ever write down your passwords and leave them on your workstation for other people to find.

**Update your programs regularly:** Make sure your computer is properly patched and updated. This is often the best way to ensure its adequately protected. Security applications are only as good as their most recent update.