Student: Gunay Maharramli

Topic: Data Privacy and Security in Database System

Midterm Paper

Introduction:

This research paper focuses on database privacy and security at the database level, specifically highlighting the PostgreSQL database. PostgreSQL, an open-source relational database management system, has gained popularity due to its robustness and advanced security features. I have chosen PostgreSQL for several reasons. Firstly, it offers comprehensive built-in security mechanisms, including strong authentication methods and access control features. Secondly, PostgreSQL prioritizes data integrity, ensuring reliable and consistent data modifications. Thirdly, an active community continually enhances PostgreSQL's privacy and security features, ensuring prompt bug fixes and updates. By focusing on PostgreSQL, I aim to analyze its security features, access controls, encryption capabilities, and auditing mechanisms. Ultimately, this research aims to provide practical insights for enhancing database security, benefiting practitioners and researchers in the field.

Progress Overview:

In this research, the investigation of database privacy and security at the database level, with a focus on PostgreSQL, involved a series of tasks that provided a comprehensive understanding of the subject matter. Research design was formulated, outlining the objectives, research questions, and methodology that guided the study. Extensive reading of scholarly articles related to database privacy and security was conducted. The methodologies, findings, and recommendations put forth by experts in the field were critically evaluated and analyzed.

Data collection involved gathering relevant information from diverse sources, including scholarly articles, whitepapers, case studies, and technical documentation. These sources provided insights into the challenges, trends, and best practices in securing databases, specifically within the context of PostgreSQL.

An experimental setup was established using a PostgreSQL database. The database was carefully configured to implement appropriate security measures, such as access controls, encryption, and auditing mechanisms.

Security measures, including access controls, encryption techniques, and LDAP integration, were implemented and evaluated within the PostgreSQL database. The effectiveness of these measures in protecting sensitive data and their impact on performance were assessed. It is worth noting that the LDAP integration was not implemented fully, because I just tried some functionalities and set up without active directory configuration. Some are failed; however, future plans include configuring active directory to enhance the authentication and access control capabilities within the PostgreSQL database. This additional configuration will further strengthen the security measures and provide seamless integration with the existing infrastructure. In additional to that, I found out that, Postgresql schema idea is different that other databases like Oracle; therefore, I am planning to give limited access to public schema to the users since public is default schema and all users will have specific access by default. Taking all privileges from public schema can be good option, but this needs further research.