Student: Gunay Maharramli

Topic: Data Privacy and Security in Database System

Selected strategy for the research

Research on data privacy and security in databases requires a mixed-methods approach encompassing qualitative and quantitative methodologies. This strategy involves a literature review, interviews, focus groups, surveys, and data analysis. The qualitative component includes literature review and interviews with stakeholders, providing insights into experiences and perceptions. Focus groups explore diverse perspectives. The quantitative phase involves designing surveys and collecting numerical data from a random sample. Thematic analysis is used for qualitative data, while statistical analysis is conducted for quantitative data. Integration of findings offers a comprehensive understanding. Clear objectives and ethical compliance are emphasized, with pilot testing to ensure validity. Conclusions and recommendations address improvements. The research process is documented in a comprehensive report, ensuring clarity and coherence. This strategy contributes to the field, informing practices and policies related to data privacy and security in databases.

Strategy for the Data Collection

Data privacy and security in databases are critical aspects in today's digital landscape. To conduct research in this field, it is important to define specific research questions and objectives. A comprehensive literature review should be conducted to identify existing knowledge and research gaps. Various data sources can be utilized, such as research papers, government reports, industry surveys, and case studies on data breaches. Data collection methods may include online research, surveys, and interviews with experts. Privacy and security considerations, such as ensuring anonymity, obtaining informed consent, and implementing data protection measures, should be followed throughout the data collection process. Once the data is collected, appropriate analysis methods can be employed to identify patterns and trends related to data privacy and security. The findings should be reported in a comprehensive research paper or report. Sharing the research with the scientific community, policymakers, and relevant stakeholders can contribute to the improvement of data privacy and security in databases. Platforms like Open

Security Data, Kaggle, UC Irvine Machine Learning Repository, and Data.gov provide datasets that can be explored for research purposes.

Data cleansing approaches

Data cleansing approaches in the context of data privacy and security in databases involve techniques such as removing duplicate records to ensure consistency and accuracy. Another important aspect is handling missing values, which can be addressed through various methods like imputation or deletion. Despite having my own data that doesn't require cleaning, it is essential to be aware of the common problems that arise during data cleansing, such as the potential loss of valuable information or introducing bias if not executed carefully.