Student: Gunay Maharramli

Topic: Data Privacy and Security in Database Systems

1. **What are you going to do?**
   The aim of researching data privacy and security in database systems is to address the pressing concerns and challenges surrounding the protection of sensitive information in the digital age. By investigating this topic, the objective is to develop effective techniques, strategies, and best practices that can safeguard personal data stored within databases.
2. **How is it done today? Current Limitations?**
   Data privacy and security in database systems are typically addressed through a combination of measures, including access controls, encryption, and regular security audits. However, limitations persist, such as the potential for insider threats, evolving cybersecurity threats, and the challenge of balancing privacy with data usability.
3. **What is your idea to do something better?**
   Implementing LDAP authentication can bolster data privacy and security in database systems by providing centralized user authentication and access control management. By leveraging LDAP, organizations can streamline user management, enforce strong password policies, and enable secure authentication across multiple systems. Furthermore, implementing additional security measures such as two-factor authentication, role-based access control, and regular security audits can further enhance the overall protection of sensitive data in database systems. These measures collectively contribute to strengthening data privacy and security, mitigating unauthorized access risks, and safeguarding against potential breaches.
4. **Who will benefit from your work? Why?**
   The work on data privacy and security in database systems benefits a wide range of stakeholders. Organizations gain protection against data breaches and regulatory penalties, ensuring business continuity and customer trust. Individuals benefit from increased safeguards on their personal information, protecting their privacy and minimizing the risk of identity theft. Database administrators (DBAs) can also reap several benefits from the work on data privacy and security in database systems. By implementing robust security measures, DBAs can protect databases from unauthorized access and potential data breaches, reducing the risk of data loss and reputational damage.
5. **What risks do you anticipate?**
   Researching data privacy and security in database systems is a complex and challenging task due to multiple factors. Firstly, the dynamic nature of cybersecurity threats necessitates researchers to continuously update their knowledge on evolving attack techniques, vulnerabilities, and mitigation strategies. Secondly, addressing data privacy and security involves a multidisciplinary approach, spanning areas such as cryptography, access control, network security, and legal compliance. Additionally, implementing

effective privacy and security measures requires striking a balance between protecting data and maintaining its usability and functionality. Successfully navigating these intricacies requires a comprehensive understanding of technical and policy aspects, making the work in this field demanding and multifaceted.

6. **Out of pocket costs? Complete within 11 weeks?**
   With dedicated effort and focused work this can be done within 11 weeks.
7. **Midterm results?**
   The midterm results of the research project on data privacy and security in database systems showed promising progress and provided valuable insights for further investigation.
8. **Final Demonstration?**
   The final demonstration showcased the successful implementation and practical application of the research findings on data privacy and security in database systems.