CS850 Database Security - Project Instructions

Objective	The course project is designed to offer you practical exposure to applying theoretical concepts related to database security.
Instructions	In this course, you will work in a team to implement the course project. Groups will consist of 2 members. It is expected that each group will begin their project when topics are approved, then present system components by the scheduled progress reporting dates.
Stages	**I. Develop a proposal for the project**: First, groups should submit for approval their project ideas. Informal discussions with the professor can help to refine the project and proposal. Groups should not continue working on the project unless it has been approved by the course instructor. This proposal should include: 1. A separate cover page indicating the title of your project, the full names of the group members (with e-mail), the course number and course section. 2. A narrative description of the project. This should also include a description of the problem being addressed. 3. Identification of the information needs - what information would help solve the problem. 4. Distribution of duties for the project. List the names of each group member and what their primary role will be. **II. Project Implementation**: Groups should then implement the approved project. Groups will periodically submit status updates. **III. Project Demonstration**: The final step is to prepare a formal demonstration and brief presentation.

Deadlines for different stages	1. Team formation- 15th January 2026
	2. Project proposal submission- 25th January 2026
	3. Midsem evaluation- 10-14th March 2026
	4. Continuous evaluation- 25th March 2026
	5. Endsem evaluation- 10th April - 17th April 2026
Sample Projects (For reference)	Your project can involve implementing something related to database security ideas. Here are a few suggestions – other topics can, of course, be suggested: 1. Context Aware RBAC Model for Wearable Devices. 2. Access Control: Delegation in access control, Access control for Workflow, attribute- based access control, access control/privacy for big data, XACML. 3. Role Engineering. 4. Access Control Systems for Medical Sensor Networks-Secure Aggregation Algorithms. 5. Service-Oriented Architecture Security - Software-level (single service) security, Business-level (service composition) security, Forensics over Web Services - Develop criteria to evaluate correctness of composite application execution, Increase reliability using redundant services, Offer security as service, Develop defense models using distributed and collaborative components (E.g., detect malicious behavior based on collaborative nodes, verify execution correctness by comparing outcome of different services, deploy intelligent software etc.) 6. Security Tool to Detect Vulnerabilities at Application Level (XSS and cross site forgery). 7. Cross-Site Scripting Attack Detection, Content Sniffing Attack Detection, Cross-Site Request Forgery Attack Detection, Phishing Attack Detection. 8. Security as a service for cloud applications, Identification of indicators for insider attacks in the cloud environment is an open area of research. 9. The differentiation between a normal and malicious user within the cloud 10. Security in digital payments. 11. IOT security. 12. SNA security: Protecting user data from the OSN, Mitigating attacks from large- scale crawlers, Mitigating Sybil attacks, Mitigating social spam, Mitigating Distributed Denial-of-service attacks (DDoS) attacks, Spam campaigns detection, understanding the privacy leakage and associated risks when OSNs work as a Web tracker. 13. Outsourcing of database storage and access control/privacy. 14. Privacy preserving data mining, k-anonymity (l-diversity). 15. Integrity enhancing models/provenance. 16. Intrusion detection for databases. 17. Models of security and privacy for graph databases. 18. Writing a tool which can query a MySQL database for a list of dates and times and exporting the resulting list to Google Calendar which will display them in the user's account. 19. Virtual Private Databases.