PROJECT PROPOSAL

Our Group (Group 17) has decided to do a project based on secure password storage using salted hashing.

Description: Our project aims to bolster data privacy in credit card fraud detection by leveraging differential privacy techniques, specifically employing Laplace and Exponential mechanisms. Differential privacy ensures that the analysis of sensitive credit card transaction data does not compromise individual privacy, even in the presence of malicious attacks such as data reconstruction attempts, model inversion attacks, and membership inference attacks. These threats fall under the malicious model, where adversaries actively seek to exploit vulnerabilities in security measures.

Implementation: Developing an advanced credit card fraud detection system featuring differential privacy mechanisms. The system will preprocess transaction data and apply Laplace and Exponential mechanisms to add privacy-preserving noise before analysis. Laplace mechanism will introduce noise proportional to the sensitivity of the data, while Exponential mechanism will select data elements probabilistically based on their scores. This approach will safeguard sensitive information, ensuring that fraudulent patterns are detected without compromising the privacy of individual transactions.

By Group 17-

Iyyapu Lakshmi Apoorva(A20545698)

Buraga Balaji (A20525910)

Hanumegowda Rohith (A20545660)