CS 47206/57206       DATA SECURITY AND PRIVACY       3 credit hours

Instructor’s Name: Kambiz Ghazinour

Online Material

Course Content:
(Slashed with CS 57206) The goal of the course is to familiarize the students with basic concepts of security and privacy, their definitions, applications and current advances in research community and industry. This course addresses the security and privacy issues in legacy systems and also studies security and privacy policies and legislations. This course also reviews current research projects in the area of security and privacy.

Prerequisites or co-requisites: Minimum C grade or better in CS 23001.
Required, elective, or selected elective

Topics to be Covered (45 Hours):
1- Introduction (4 hours)
2- Ethics (4 hours)
3- Defining Privacy (Foundations) (4 hours)
4- Legislative Privacy (4 hours)
5- Privacy and Data Collection (4 hours)
6- Data Privacy Taxonomy and alternative Privacy Frameworks (4 hours)
7- Hippocratic Databases (4 hours)
8- Privacy-aware Access Control (4 hours)
9- Anonymity models (4 hours)
10- Privacy Policies (4 hours)
11- Privacy in Cloud infrastructure and Big Data (5 hours)

Learning Outcomes:
1- Describe the concept of privacy including personally private information, potential violations of privacy due to security mechanisms, and describe how privacy protection mechanisms run in conflict with security mechanisms.
2- Describe how an attacker can infer a secret by interacting with a database.
3- Explain how to set a data backup policy or password refresh policy.
4- Discuss how to set a breach disclosure policy.
5- Describe the consequences of data retention policies.
6- Identify the risks of relying on outsourced manufacturing.
7- Identify the risks and benefits of outsourcing to the cloud.

Assessment of Learning Outcomes:
1- 4 Quizzes through the semester
2- Class Discussion
3- Project writing and implementation
4- Writing critiques on research work