King Fahd University of Petroleum and Minerals

College of Computer Science and Engineering
Computer Engineering Department

COE 526: Data Privacy

Term 201

Course Information

- Lectures: Sunday & Tuesday, 6:45-8:00 PM
- "Virtual" office hours: UT 8:15-9PM for calls on Teams (or send me on Teams and I will try to accommodate your Qs online)
- Web page:
  - Blackboard page
  - https://faculty.kfupm.edu.sa/COE/mfelemban/COE526/201/index.html

Course Description

Data privacy: definition and terminologies. Difference between data security and privacy. Data privacy attacks. Data privacy laws and regulations. Privacy risk and impact assessment. Privacy engineering, management, and evaluation. Data anonymization. Statistical privacy. Differential privacy. Cryptographic privacy. Homomorphic encryption. Secure multi-party computation. Secure data outsourcing. Data hiding and steganography. Anonymous networks. Trusted execution environment. Applications of privacy preserving technologies in computer systems and applications.

Course Objectives

The objective of this course is to

- Introduce students to the theoretical foundations and practical technologies for ensuring data security and privacy while allowing organizations to collect, store, analyze, and share data for worthy purposes.
- Apply and design new privacy-enhancing technologies for emerging systems
- Equip students with skills pertaining to evaluate and criticize computer systems and Infrastructures in terms of preserving the security and privacy of users

Prerequisites Senior Standing

Textbook No Textbook

References

1. Nataraj Venkataramanan, Ashwin Shriram. “Data Privacy: Principles and Practice”. CRC Press, 2016
2. Mark Stamp. “Information Security: Principles and Practice”, Wiley, 2011.
3. Aggarwal, Charu C., Yu, Philip S. “Privacy-Preserving Data Mining Models and Algorithms”. Springer, 2008.
4. Xun Yi, Russell Paulet, Elisa Bertino. “Homomorphic Encryption and Applications”, Springer, 2014
5. Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, Security in Computing, 5th edition, Prentice-Hall, 2015
6. David Salomon. "Data Privacy and Security". Springer , 2003.
7. Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. Found. Trends Theor. Comput. Sci. 9, 3–4 (August 2014), 211-407

Learning Outcomes

After taking this course, students will have the ability to

1. Identify data privacy requirements
2. Explain privacy-related issues
3. Design new solutions to enhance the data privacy in emerging computer systems and applications
4. Analyze the level of data privacy in existing computer systems and applications
5. Enhance and integrate privacy-preserving technologies to achieve information security and privacy
6. Evaluate privacy-preserving technologies

Evaluation

Homework and programming assignments	25%
Short quizzes	10%
Term Project	25%
Major Exams	20%
Final Exam	20%

List of Topics

The following schedule is tentative and subject to changes. More details will be announced in the class and course website/Blackboard.

1. Introduction to Data privacy, difference between data security and data privacy, data privacy attacks
2. Data privacy laws and regulations: GDPR, HIPAA, and CCPA.
3. Privacy impact and risk assessment, evaluation of privacy-preserving systems
4. Privacy engineering and management
5. Data anonymization and statistical privacy
6. Differential privacy
7. Cryptographic Privacy: Homomorphic encryption
8. Secure multi-party computation: Yao's millionaire problem, Garbled circuits
9. Secure data outsourcing: Oblivious transfer
10. Data hiding and steganography
11. Anonymous communication networks: Onion routing, TOR network
12. Trusted Execution Environment
13. Preserving Privacy solution in computer systems and application: AI, Blockchain, and IoT

Course Policies

- **Coursework includes** participation, online/in-class discussions and activities, attendance, homework assignments, and quizzes. Active learning is implemented in this class. Students are expected to be positively engaged in the learning process.

- **Course Website & Participation:** Students are required to periodically check the course website and download course material as needed
  - Blackboard will be used for communication and interaction, posting and submitting assignments, posting grades, posting sample exams, etc.
  - It is expected that you get benefit of the discussion board by raising questions or answering questions put by others.

- **Attendance:** Regular attendance is a university requirement.
  - Attendance will be checked at each lecture.
  - Missing 20% of the classes will result in an automatic DN grade (without warning).
  - Late arrivals will disrupt the class session, and may be counted as a miss if repeated.

  - If you find yourself unable to attend a class, email the instructor ahead of time for better planning and management of the class. If you fail to do so, send your email as soon as you get a chance and provide your excuses if any.
  - Every unexcused absence may lead to a loss of 0.5% of total grade.

- **Late assignments** are subjected to late-penalty.
  - Late submission will result in deducing 10% per day of the assignment grade. For example, the assignment will be graded out of 80% if the assignment is submitted two days after the due date.

- **Re-grading policy:** if you have a complaint about any of your grades, discuss it with the instructor no later than 3 days of distributing the grades (except for the final). Only legitimate concerns on grading should be discussed.

- **Office Hours:**
  - Students are encouraged to use the office hours to clarify and understand the material. Use the Blackboard (Bb) for quick points and homework questions.
  - For urgent issues, use emails instead of Bb-mails, please indicate ICS553 in the "Subject" field of your email (e.g. ICS553: Quiz1 score is missing).

- **Academic honesty:**
  - Students are expected to abide by all the university regulations on academic honesty.
  - Cheating will be reported to the Department Chairman.
  - Although collaboration and sharing knowledge is highly encouraged, copying others' work without proper citation, either in part or full, is considered plagiarism. Whenever in doubt, review the university guidelines or consult the instructor.

- **Courtesy:**
  - Students are expected to be courteous toward their classmates and the instructor throughout the duration of this course (in-class and online).
  - Side-talks and text-messages during the class are prohibited.