Lecture 1

Network Security

Introduction

Chapter 1

Learning Objective

- Introduce the security requirements
  - confidentiality
  - integrity
  - availability
- Describe the X.800 security architecture for OSI

Network Security Requirements

Network Security

- Definition: The protection afforded to an automated information system in order to attain the application objectives to preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

- NIST Computer Security Handbook

Confidentiality

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals;
- **Privacy:** Assures that individual's control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- i.e., student grade information

Integrity

- **Data integrity:** Assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner;
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- i.e., a hospital patient's allergy information

Availability

- **Availability:** Assures that systems work promptly, and service is not denied to authorized users, ensuring timely and reliable access to and use of information
- i.e., denial of service attack

Other security requirements

- **Authenticity**
- **Accountability**
  - tracible data source,
  - fault isolation
  - intrusion detection and prevention,
  - recovery and legal action
  - system must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

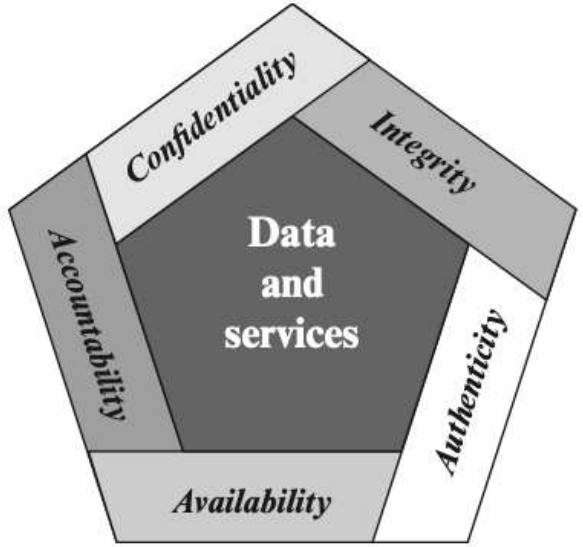

Figure 1.1 Essential Network and Computer Security Requirements

Question

- What security requirements does a blockchain system have achieved?

Project

- **Task1: OnDemand Professor Q&A Bot**
  - Your task is to build a Q&A Bot over private data that answers questions about the network security course using the open-source alternatives to ChatGPT that can be run on your local machine. Data privacy can be compromised when sending data over the internet, so it is mandatory to keep it on your local system.
  - Your Q&A Bot should be able to understand user questions and provide appropriate answers from the local database, then the citations should be added **(must be accomplished)** if the response is from the internet, then the web references should be added.
  - Train your bot using network security lecture slides, network security textbook, and the Internet.
  - By using Wireshark capture data for Step 4's of the LLM workflow shown in Figure 1. Provide detailed explanations of the trace data. Also, Maintain a record of Step 1's prompt and its mapping to the trace data in Step 4's.
- **Task2: Quiz Bot**
  - Your task is to build a quiz bot based on a network security course using the open-source alternatives to ChatGPT that can be run on your local machine. Data privacy can be compromised when sending data over the internet, so it is mandatory to keep it on your local system.
  - Two types of questions should be offered by the bot: randomly generated questions and specific topic questions and the answers should be pulled from the network security database. Train your bot using network security quizzes, lecture slides, network security textbook, and the Internet.
  - The quiz must include multiple-choice questions, true/false questions, and open-ended questions.
  - Finally, the bot should be able to provide feedback on the user's answers.

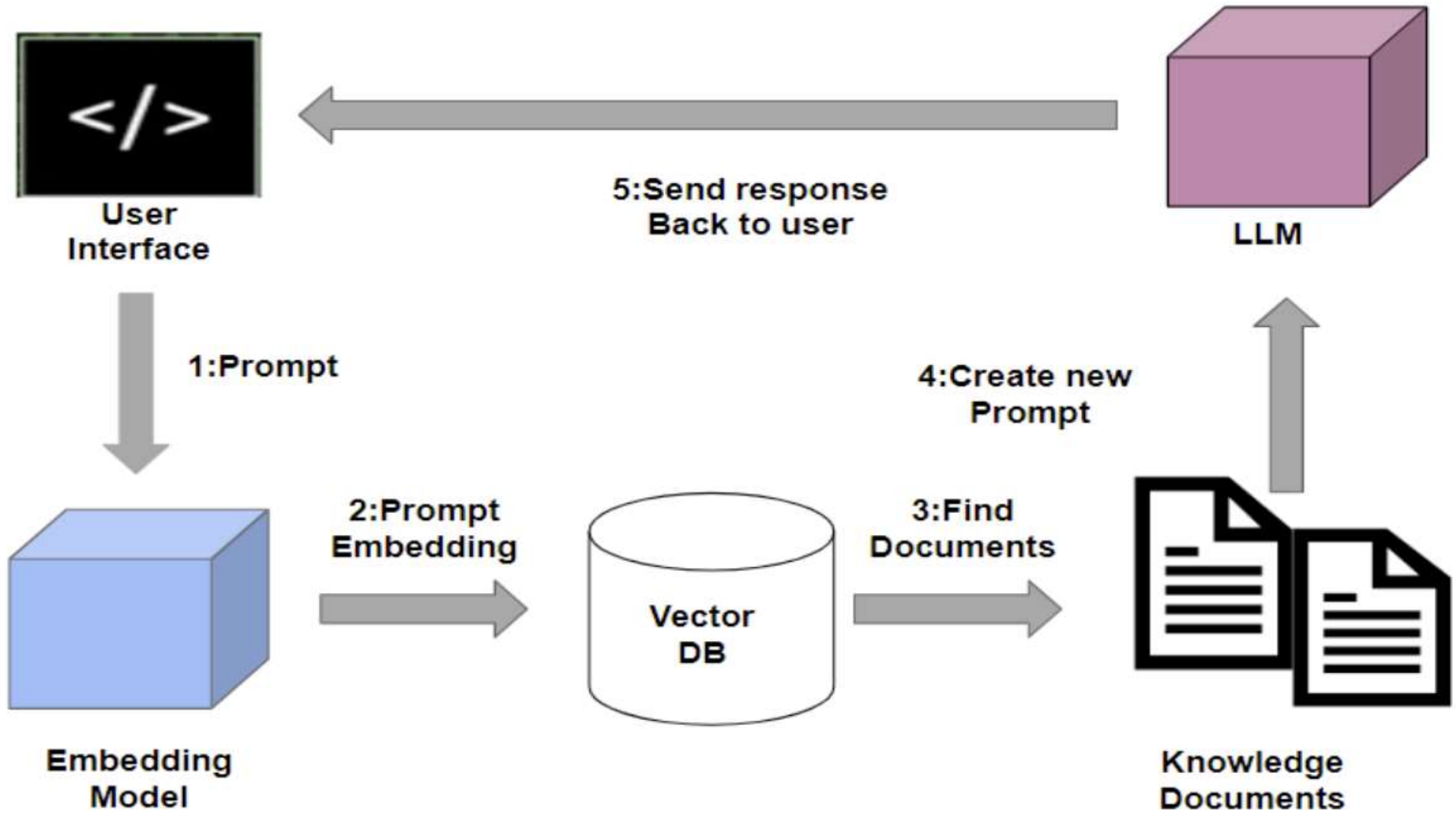

Figure 1: LLM workflow

Form Project Groups

- Form a group **(no submission)**
  - The project will be assigned as a group project. Six students will be considered a group for a project. Here is the link to enter your project group member names.

    FALL 2023 CS5342 PROJECT GROUP NAMES.xlsx
  - It is recommended that one person in the group fills in the form to avoid multiple entries and submits project files on Blackboard. If you cannot get a group, contact to TA.
- Deadline to submit your group members is 11:59PM on Sept 8th, 2023

Email communication

- Email subject: course# _course name_reason
  - such as “CS 5342_network security_late submission”