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.

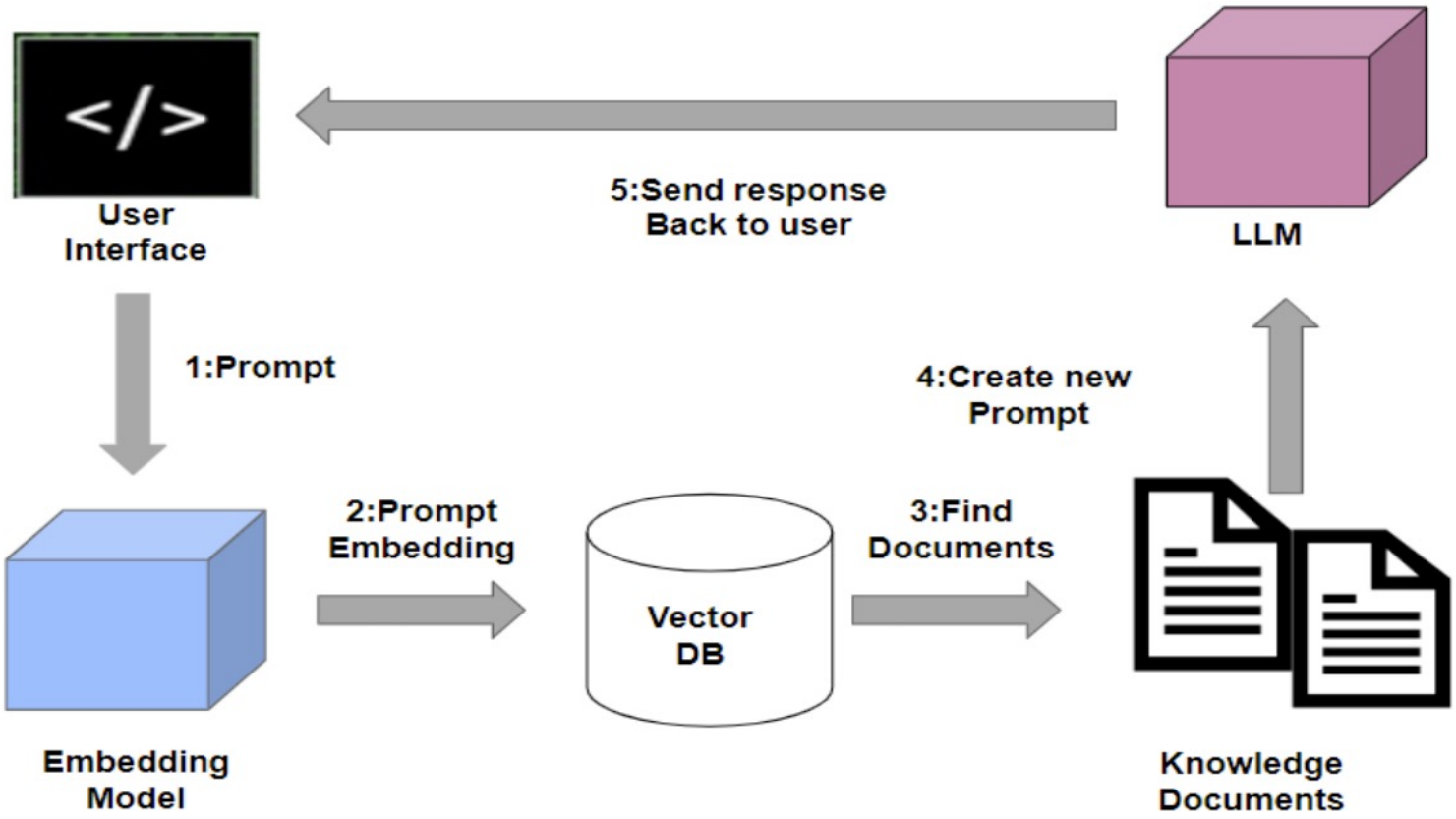


Figure 1: LLM workflow

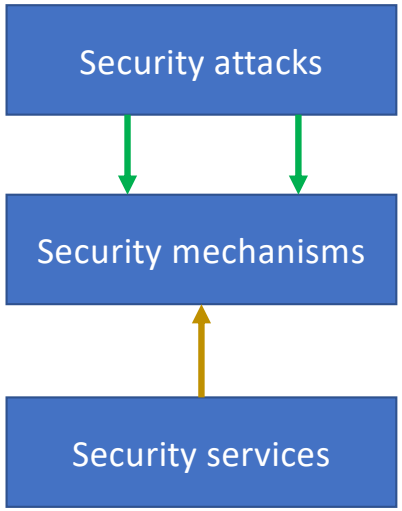
Outline

- Review
- OSI Security Architecture
  - Attack model

OSI Security Architecture

OSI Security Architecture

- International Telecommunication Union – Telecommunication (ITU-T) recommends X.800
- Security Architecture for Open Systems Interconnection (OSI)
  - Defines a systematic way of defining and providing security requirements
  - Used by IT managers and vendors in their products



a process (or a device incorporating such a process) to detect, prevent, or recover from an attack

enhances the security of the data processing systems and the information transfers, such as policies

Other Security Architectures

- NIST, Cybersecurity Framework (CSF)
  - https://www.nist.gov/cyberframework
  - VIRTUAL WORKSHOP #2 | February 15, 2023 (9:00 AM – 5:30 PM EST). Discuss potential significant updates to the CSF
  - https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2
- OWASP - Open Web Application Security Project
  - Web application security
  - OWASP Application Security Verification Standard (ASVS) - https://owasp.org/www-project-application-security-verification-standard/
  - OWASP Web Security Testing - https://owasp.org/www-project-web-security-testing-guide/
  - OWASP foundation

Security attack

- **Definition**: any action that compromises the security of information owned by an organization
- Two types of security attacks
  - Passive attack
  - Active attack