ÇANKAYA ÜNİVERSİTESİ

1997

CRYPTOSEARCH

Faik Doruk Akgüney 202371202

The CryptoSearch project is a platform designed to securely store and access sensitive data using homomorphic encryption, allowing users to perform data search and computation operations while maintaining privacy and security. This project serves as a bridge for encrypted data sharing and operations between data owners and users.

Objectives:

- Data Security and Privacy: Enable data owners to encrypt their sensitive data using homomorphic encryption for secure storage and processing.
- User-Friendly Interface: Provide a Command-Line Interface (CLI) for users to easily conduct data search and computation operations.
- Data Search and Computation: Allow users to search encrypted data based on specific keywords or filters and perform computations on the encrypted data.

User Roles:

1. Data Owner:

    - Data owners upload their sensitive data using the CLI interface.
    - The program encrypts the data using homomorphic encryption libraries like PySeal and securely stores it.

2. User:

    - Users log in to the program with their credentials via the CLI.
    - Users initiate search operations on encrypted data by specifying keywords or filters.

Workflow:

1. Data Encryption and Upload:

    - Data owners start the program and upload their sensitive data via the CLI.
    - The program uses homomorphic encryption libraries (e.g. PySeal) to encrypt the data and store it securely.

2. User Login and Search Operations:

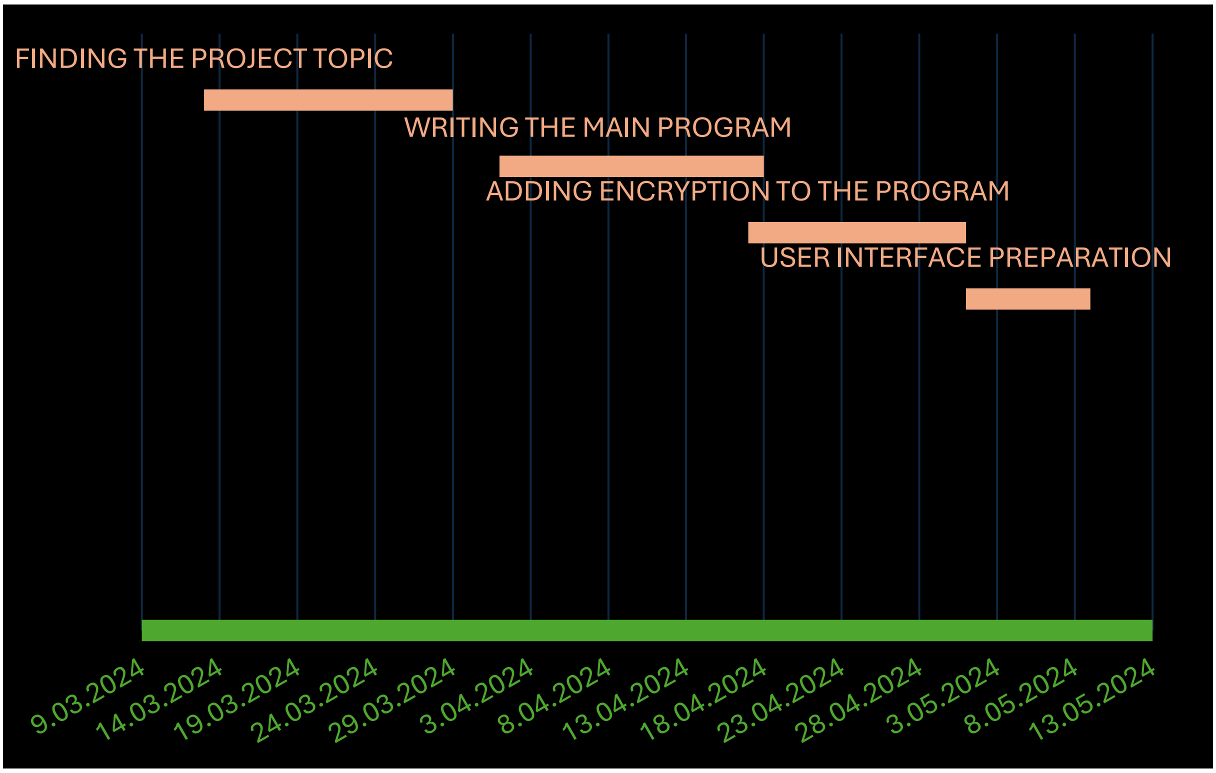
    - Users launch the program, log in with their credentials, and specify keywords or filters for search operations.

- The program performs homomorphic encryption-based search operations on the encrypted data using the specified criteria.

3. Homomorphic Encryption Operations:
   - The program conducts search and computation operations on the encrypted data based on user-defined keywords or filters.
   - Operations are performed securely without revealing the full contents of the encrypted data.

4. Result Display:

   - Search and computation results are displayed in a formatted manner based on user preferences.
   - Users can access processed results without viewing the plaintext contents of the encrypted data.


FINDING THE PROJECT TOPIC
WRITING THE MAIN PROGRAM
ADDING ENCRYPTION TO THE PROGRAM
USER INTERFACE PREPARATION