SYNOPSIS OF

MINOR PROJECT ON

CyberHUB: An Innovative Web App for Real-Time Data Protection and Breach Prevention

SUBMITTED BY

SUPRIYO PURKAIT: TNU2021020100021

SAJAL PAUL: TNU2021020100016

SOUMYA SAMANTA: TNU2021020100015

SUBHASHIS MONDAL: TNU2021020100009

FOR

THE PARTIAL FULFILLMENT OF B. Tech DEGREE

IN

CSE (CYBER SECURITY)

UNDER THE SUPERVISION OF

Bilas Haldar, Assistant Professor Adhoc (Grade - 1) in the Department of Computer Science and Engineering

2021-2025

SCHOOL OF SCIENCE AND TECHNOLOGY

THE NEOTIA UNIVERSITY

Bilas Haldar 2/4/24

Signature

Project Name:

CyberHUB: An Innovative Web App for Real-Time Data Protection and Breach Prevention

Abstraction:

In the digital age, where data security is very important, CyberHUB emerges as an innovative solution to contemporary challenges. By leveraging advanced technologies, CyberHUB addresses data protection concerns with the help of hash identification, real-time email and password breach checking via external APIs, and a secure message encryption/decryption mechanism. The project focuses on empowering users with a simple user interfaces and collaborative backend processing, offering robust tools for identifying and mitigating security risks. With a commitment to innovation in multidimensional data security, CyberHUB stands as a pivotal contribution to cybersecurity, addressing the evolving landscape of information technology with a user-centric and forward-thinking approach.

Introduction:

In the rapidly growing technological era, the significance of data security and integrity measures cannot be underestimated. As cyber threats evolve and increase, individuals and organizations facing in safeguarding sensitive information. CyberHUB, an innovative initiative engineered to reinforce data security in this dynamic landscape. This project uses advanced technologies to implement a multifaceted approach to cybersecurity, effectively addressing the urgent need for heightened protection against data breaches and cyber-attacks.

CyberHUB distinguishes itself by integrating cutting-edge solutions such as hash identification for data integrity verification, real-time monitoring of email and password security breaches through external APIs, and a sophisticated mechanism for secure message encryption and decryption. These features are meticulously designed to shield users from the myriad of threats in the digital world, ensuring their data remains safe and secure.

CyberHUB is a project that focuses on making cybersecurity tools easy to use and encouraging people to work together smoothly. The design is so simple that for anyone can use and understand, even if they're not experts in technology. Which implies that everyone, no matter their level of technical skill, can easily use the tools effectively.

Behind the scenes, there's a lot of teamwork going on. The system is set up so that different parts can work together efficiently. This teamwork helps CyberHUB provide security solutions quickly and effectively when they're needed.

Background:

In today's digital world, cyber threats are increasing, making it tough for individual and orgination to keep their data safe. These threats can cause financial losses and damage reputations. That's why there's a big need for better ways to safeguard data from hackers and cyber-attacks.

Because cyber threats are getting more complex, traditional security measures aren't enough anymore. We need new and smarter solutions that use advanced technology to stay ahead of these threats.

In response to the growing need for enhanced data security, CyberHUB emerges as a groundbreaking initiative designed to address the evolving challenges of cybersecurity. By harnessing advanced technologies and adopting a comprehensive approach, CyberHUB aims to provide users with effective tools and strategies to defend against cyber threats and safeguard sensitive information. Through its user-friendly interface and collaborative backend processing, CyberHUB empowers individuals and organizations of varying technical expertise to navigate the complexities of cybersecurity and ensure the integrity of their digital assets.

Problem Statement:

The project addresses the following key challenges:

- Lack of efficient hash identification tools.
- Limited resources for checking email and password breaches.
- Inadequate message encryption and decryption mechanisms.

Objective and Scope:

Objectives:

- Develop a robust hash identifier.
- Implement an email breach checker utilizing external APIs for real-time analysis.
- Create a password breach detection system.
- Design a secure message encryption and decryption mechanism

Scope:

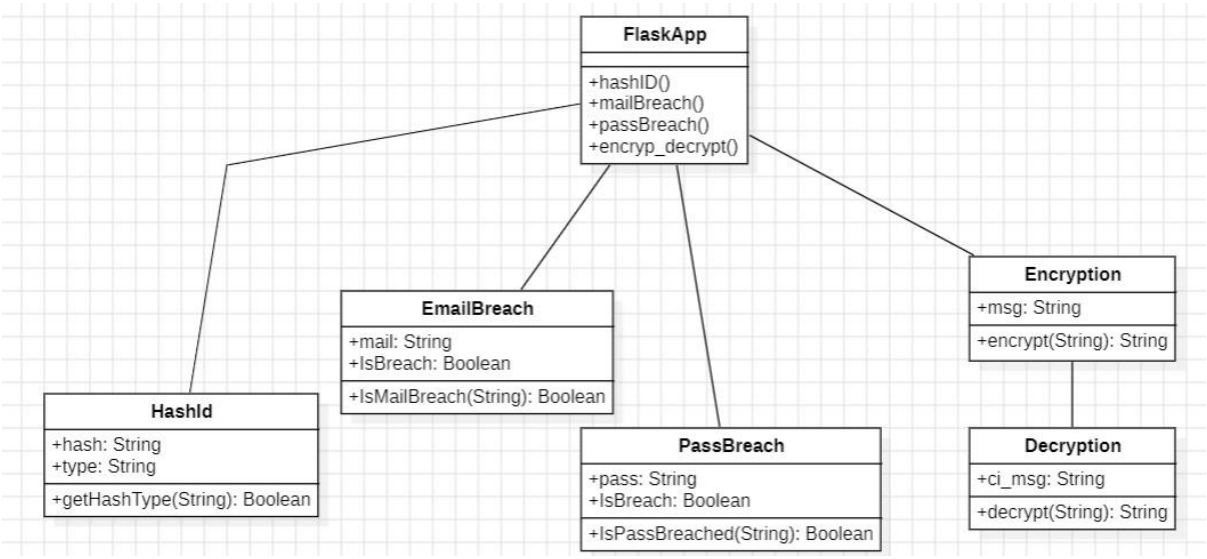
- The project focuses on providing user-friendly interfaces for hash identification, email breach checking, password breach analysis, and message encryption/decryption.
- Emphasis on backend processing to ensure data integrity and security.

Methodology:

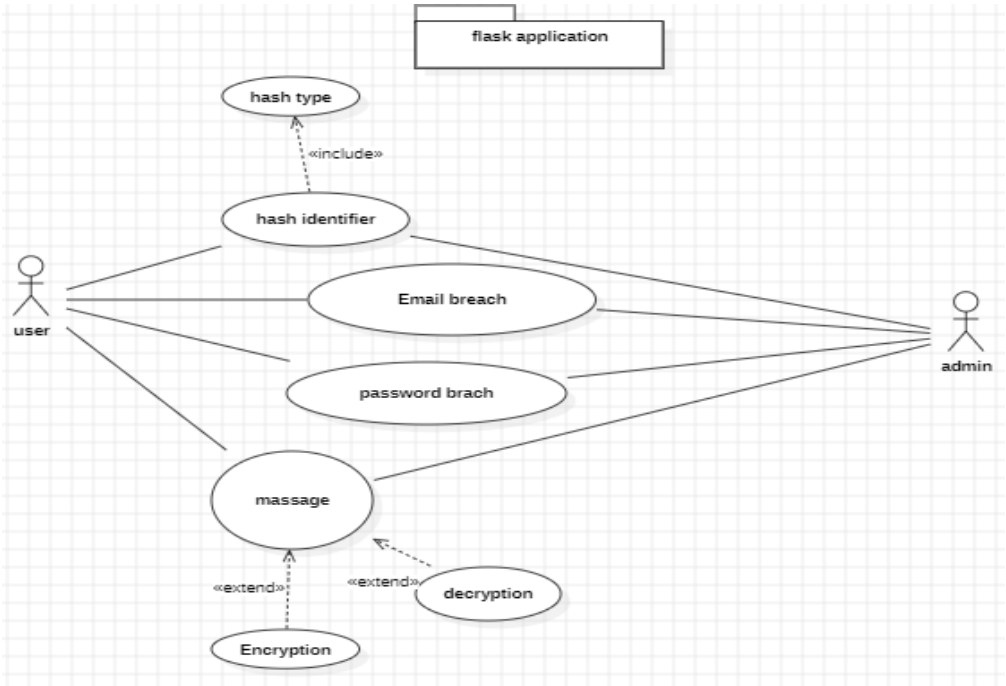
The project will be implemented using a combination of frontend and backend technologies. The backend will involve processing algorithms, external API integrations, and database management. The frontend will provide a user interface for seamless interaction.

UML Diagram:

Class diagram:

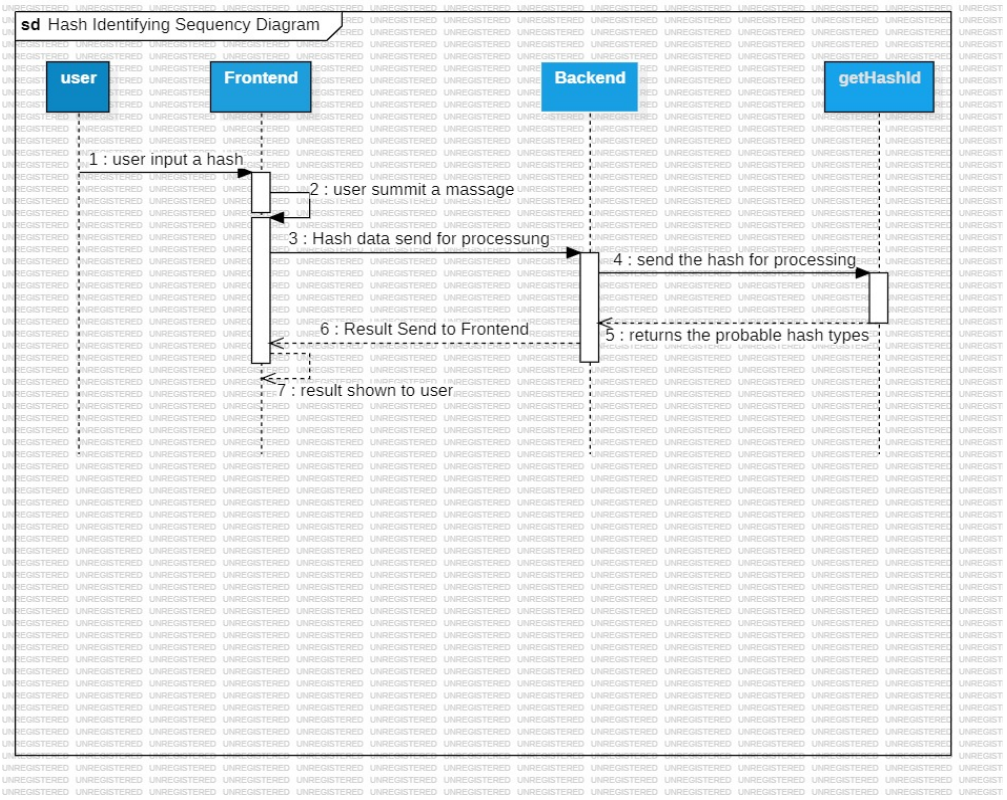


Use case diagram:

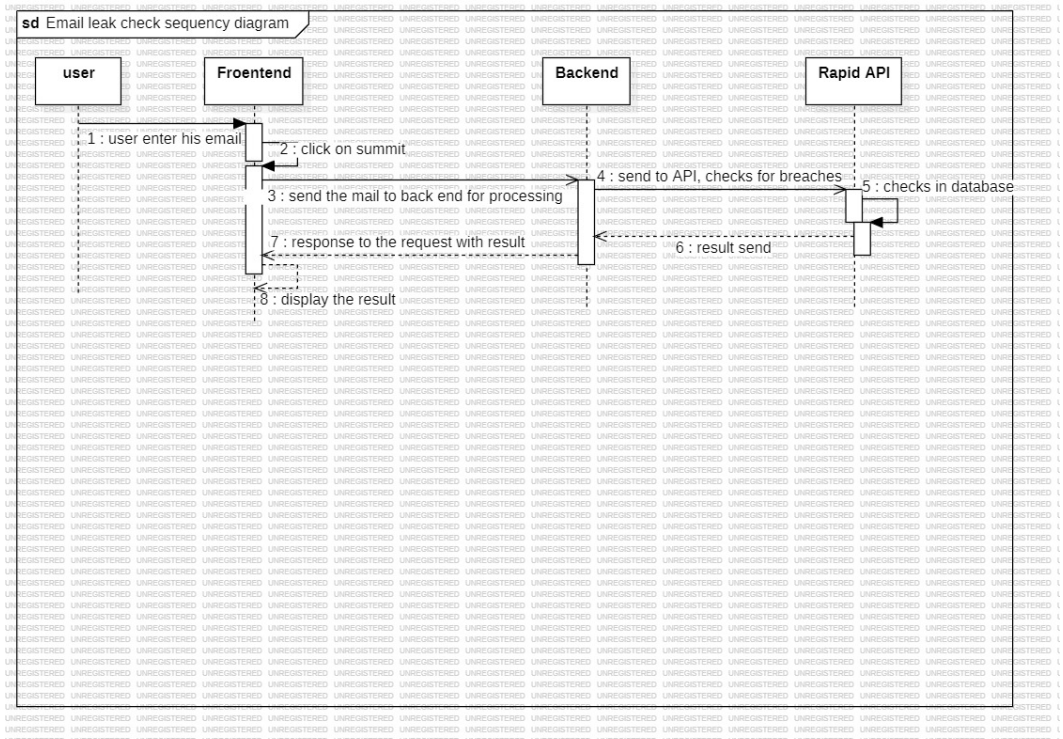


Sequency diagram:

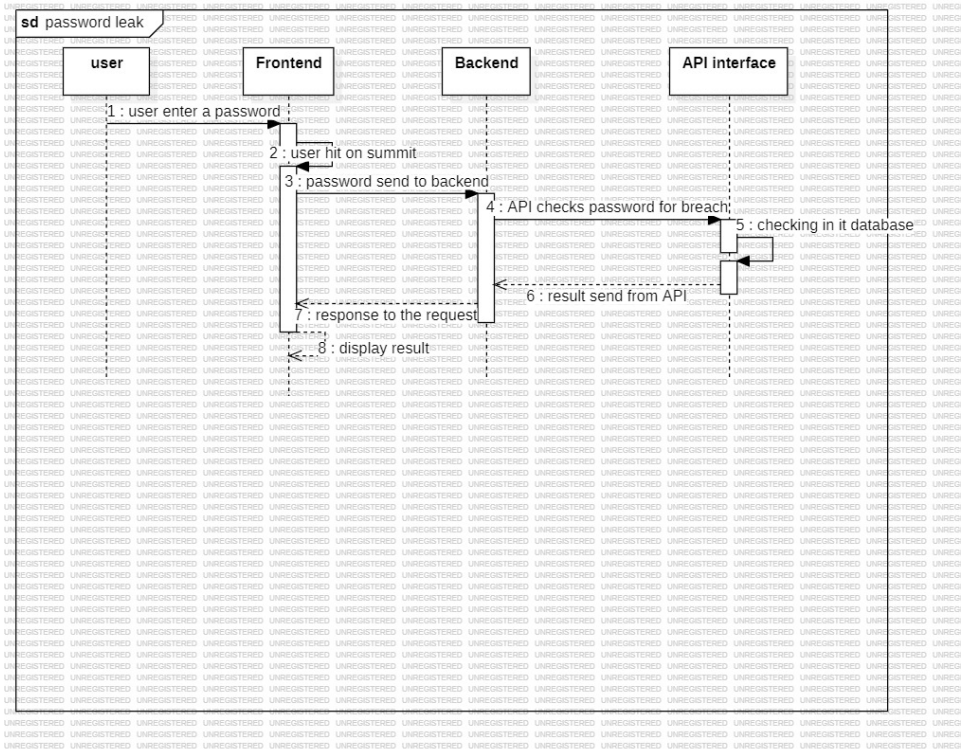
1.



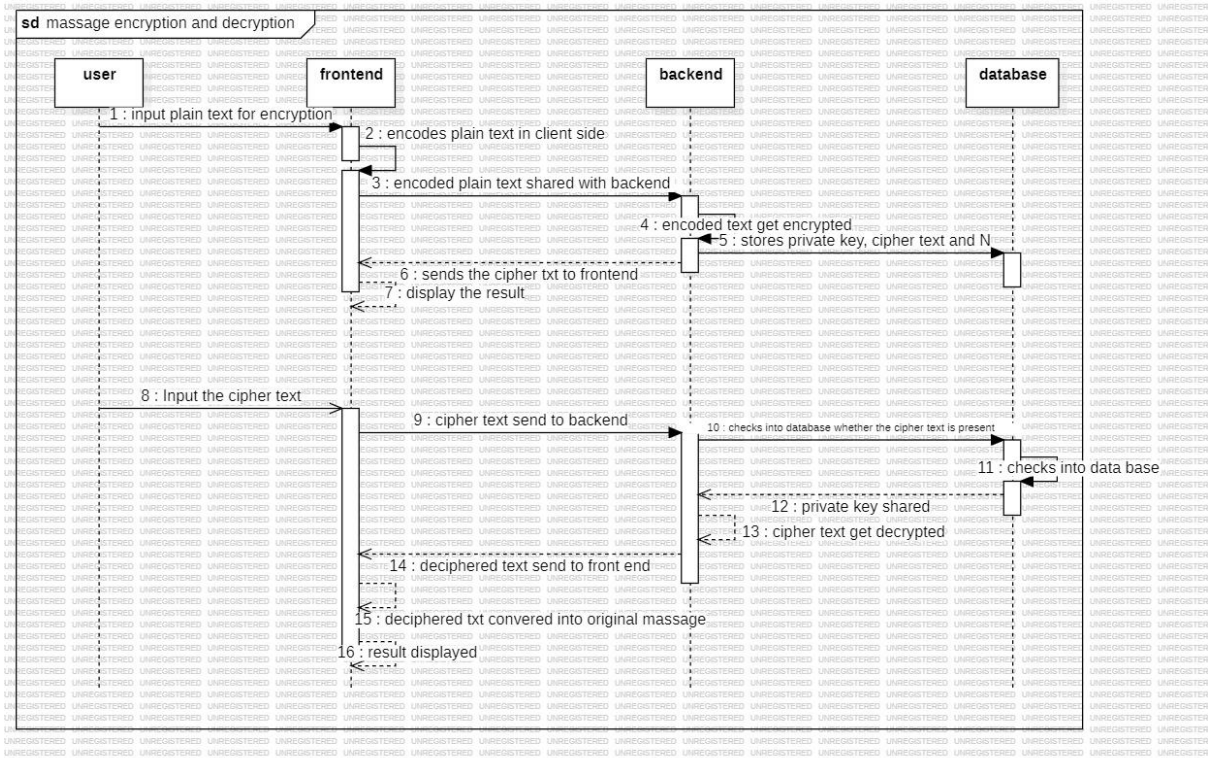
2.



3.


sd password leak
user
Frontend
Backend
API interface
1 : user enter a password
2 : user hit on summit
3 : password send to backend
4 : API checks password for breach
5 : checking in it database
6 : result send from API
7 : response to the request
8 : display result

4.


sd massage encryption and decryption
user
frontend
backend
database
1 : input plain text for encryption
2 : encodes plain text in client side
3 : encoded plain text shared with backend
4 : encoded text get encrypted
5 : stores private key, cipher text and N
6 : sends the cipher txt to frontend
7 : display the result
8 : Input the cipher text
9 : cipher text send to backend
10 : checks into database whether the cipher text is present
11 : checks into data base
12 : private key shared
13 : cipher text get decrypted
14 : deciphered text send to front end
15 : deciphered txt convered into original massage
16 : result displayed

Hardware & Software:

Hardware:

- Server infrastructure for backend processing.
- Database server.

Software:

- Programming languages: Python
- Database management system: MySQL
- External APIs: haveibeenpwned APIv2, RapidAPI

Contribution:

Each team member will play a crucial role in the development of specific components:

- **Subhashish Mondal**: Designing the frontend for seamless interaction
- **Sajal Paul**: Email breach checker and Password breach checker integration with external APIs.
- **Supriyo Purkait**: Creating and managing the backend using Python and connection between frontend and the backend
- **Soumya Samanta**: Message encryption and decryption and implementation of this in backend.

References:

1) **JavaScript Guide by MDN:** [https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide]
2) **Flask's Documentation:** [https://flask.palletsprojects.com/en/3.0.x/]
3) **Have I Been Pwned API:** [https://haveibeenpwned.com/API/v3]
4) **W3Schools**: [https://www.w3schools.com/]