**Project Name:** CyberHUB (A webapp for data security)

**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:**

The **CyberHUB** is a comprehensive solution designed to address the growing concerns surrounding data security. With a focus on email breach checking, password breach checking, secure message encryption/decryption, and hash identification, this project aims to provide users with robust tools to safeguard their sensitive information.

**Background:**

In the era of increasing cyber threats and data breaches, it has become necessary to implement advanced security measures. This project stems from the need to empower users with effective tools to identify potential vulnerabilities and protect their data.

**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:**

<>

**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.