**DESCRIPTION**

**Project Description: Quantum-Safe Messaging Application**

**The Quantum-Safe Messaging Application is a secure web-based messaging platform designed to withstand the cryptographic threats posed by quantum computers. This project leverages quantum-safe cryptographic algorithms to ensure end-to-end security for communication, authentication, and data storage. By integrating cutting-edge technologies such as the Open Quantum Safe (OQS) project, Flask for backend logic, HAProxy for SSL/TLS termination, and MySQL for database management, this application demonstrates how modern web applications can be made resilient against quantum attacks.**

**Objective**

**The goal of this project is to build a secure messaging platform that uses quantum-safe cryptography to protect user data and communications. The application ensures:**

1. **Secure communication between clients and servers using quantum-safe encryption.**
2. **Robust session management and authentication mechanisms.**
3. **Encrypted storage of sensitive data in the database using quantum-safe algorithms.**
4. **A scalable architecture capable of handling real-time messaging securely.**

**Key Components**

**1. Quantum-Safe Cryptography**

* **The project adopts quantum-safe algorithms from the CRYSTALS suite , including:**
  + **CRYSTALS-Kyber : A Key Encapsulation Mechanism (KEM) for secure key exchange.**
  + **CRYSTALS-Dilithium : A digital signature algorithm for authentication and integrity.**
* **These algorithms are integrated into the system using the Open Quantum Safe (OQS) project's libraries (liboqs and oqs-provider) and a custom-built, quantum-safe version of OpenSSL.**

**2. HAProxy for SSL/TLS Termination**

* **HAProxy acts as a reverse proxy to terminate SSL/TLS connections securely using quantum-safe algorithms.**
* **It ensures that all communication between the client and server is encrypted with quantum-safe protocols, protecting against both classical and quantum attacks.**
* **HAProxy forwards unencrypted traffic to the Flask backend after terminating TLS connections.**

**3. Flask Backend**

* **The Python Flask server serves as the core backend for the application, replacing the traditional Apache HTTPD server.**
* **Flask handles:**
  + **Authentication : Using session-based authentication with quantum-safe encryption for session data.**
  + **Business Logic : Managing user interactions, message processing, and database operations.**
  + **API Endpoints : Providing RESTful APIs for the React.js frontend to interact with the backend.**
* **Flask integrates with the quantum-safe OpenSSL library to encrypt sensitive data before storing it in the database or transmitting it over the network.**

**4. React.js Frontend**

* **The frontend is built using React.js , providing a user-friendly interface for messaging and user management.**
* **Users can log in, register, send messages, and view their message history through an intuitive UI.**
* **Communication between the frontend and backend is secured using quantum-safe encryption via HAProxy.**

**5. MySQL Database**

* **MySQL is used as the database to store user credentials, session data, and messages.**
* **Sensitive data stored in the database is encrypted using quantum-safe algorithms (e.g., Kyber for key exchange and AES for symmetric encryption).**
* **The database schema includes tables for users, sessions, and messages, ensuring efficient data management.**

**Workflow**

1. **Client ↔ HAProxy :**
   * **The client communicates with HAProxy over HTTPS using quantum-safe algorithms (e.g., Kyber for key exchange, Dilithium for signatures).**
   * **HAProxy terminates the TLS connection, decrypting the traffic before forwarding it to the Flask backend.**
2. **HAProxy ↔ Flask Backend :**
   * **HAProxy forwards unencrypted HTTP traffic to the Flask backend.**
   * **Flask processes requests, interacts with the MySQL database, and returns responses to HAProxy.**
3. **Database Encryption :**
   * **Before storing sensitive data in the MySQL database, Flask encrypts it using quantum-safe algorithms.**
   * **For example:**
     + **Session Data : Encrypted using Kyber for key exchange and AES for symmetric encryption.**
     + **Messages : Signed with Dilithium to ensure integrity and authenticity.**
4. **User Authentication :**
   * **Users authenticate via Flask using session-based authentication.**
   * **Session data is encrypted with quantum-safe algorithms to prevent unauthorized access.**
5. **Real-Time Messaging :**
   * **The Flask backend supports real-time messaging using WebSockets or similar technologies.**
   * **Messages are encrypted end-to-end using quantum-safe algorithms to ensure confidentiality.**

**Security Features**

1. **Quantum-Safe Encryption :**
   * **All communication between the client and server is secured using quantum-safe algorithms.**
   * **Sensitive data stored in the database is encrypted with quantum-safe protocols.**
2. **End-to-End Security :**
   * **Messages are encrypted on the client side, decrypted only by the intended recipient.**
   * **Digital signatures ensure the authenticity and integrity of messages.**
3. **Secure Session Management :**
   * **Flask uses quantum-safe encryption to secure session data, preventing session hijacking and replay attacks.**
4. **Scalability :**
   * **HAProxy provides load balancing and SSL termination, making the system scalable for multiple users and high traffic.**

**Technologies Used**

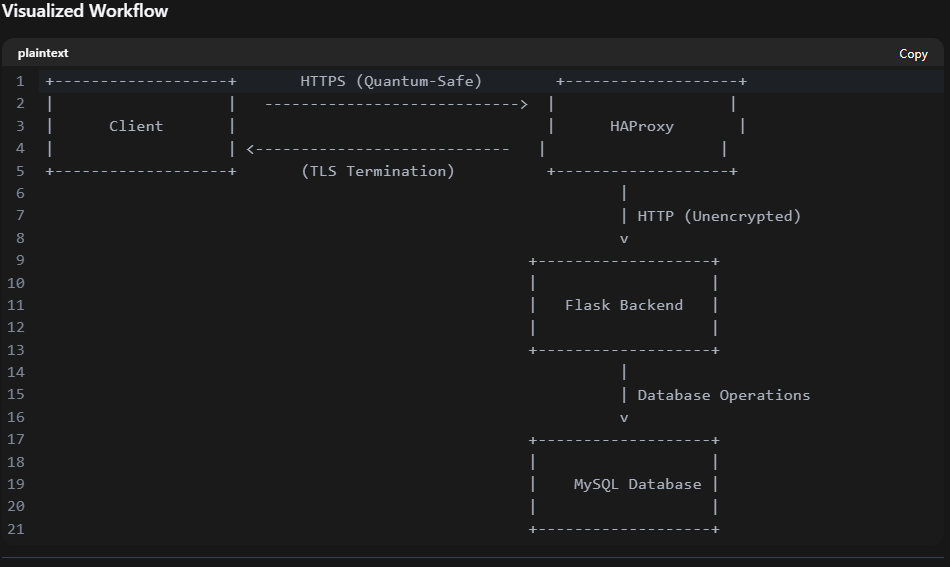
* **Frontend :**
  + **React.js for building the user interface.**
  + **CSS for styling the application.**
* **Backend :**
  + **Python Flask for handling business logic, authentication, and API endpoints.**
  + **Quantum-safe OpenSSL for encryption and decryption.**
* **Reverse Proxy :**
  + **HAProxy for SSL/TLS termination using quantum-safe algorithms.**
* **Database :**
  + **MySQL for storing user credentials, session data, and messages.**
* **Quantum-Safe Libraries :**
  + **liboqs and oqs-provider for implementing quantum-safe algorithms.**

**Development Environment**

* **Operating System : Ubuntu 22.04 LTS**
* **Dependencies :**
  + **Quantum-safe OpenSSL**
  + **HAProxy**
  + **Flask**
  + **MySQL**
  + **React.js**
* **Certificates :**
  + **Self-signed certificates created using quantum-safe algorithms (e.g., Dilithium for signatures, Kyber for key exchange).**

**WORKFLOW**

Below is a visualized workflow of the project based on the description you provided. It outlines how data flows from the client, through HAProxy, to the Flask backend, and finally to the MySQL database, and back. This flow ensures quantum-safe encryption at every step.



**Detailed Step-by-Step Workflow**

**1. Client ↔ HAProxy**

* Client Sends Request : The client communicates with HAProxy over HTTPS using quantum-safe algorithms :
  + Key Exchange : Uses Kyber for secure key exchange.
  + Signatures : Uses Dilithium for authentication and integrity.
* HAProxy Terminates TLS : HAProxy terminates the TLS connection, decrypting the traffic using quantum-safe algorithms.
* Forwarding Traffic : HAProxy forwards the decrypted (unencrypted) HTTP traffic to the Flask backend.

**2. HAProxy ↔ Flask Backend**

* HTTP Traffic : HAProxy sends unencrypted HTTP requests to the Flask backend.
* Flask Processes Requests :
  + Handles user authentication.
  + Interacts with the MySQL database.
  + Encrypts sensitive data before storing it in the database.
* Response : Flask sends responses back to HAProxy, which re-encrypts them using quantum-safe algorithms before forwarding them to the client.

**3. Flask Backend ↔ MySQL Database**

* Data Encryption :
  + Before storing sensitive data in the MySQL database, Flask encrypts it using quantum-safe algorithms :
    - Session Data : Encrypted using Kyber for key exchange and AES for symmetric encryption.
    - Messages : Signed with Dilithium to ensure integrity and authenticity.
* Database Interaction :
  + Flask queries the database for user sessions, messages, or other data.
  + All sensitive data retrieved from the database is decrypted by Flask before being processed.

**4. Real-Time Messaging**

* WebSockets : Flask supports real-time messaging using WebSockets or similar technologies.
* End-to-End Encryption :
  + Messages are encrypted end-to-end using quantum-safe algorithms:
    - Key Exchange : Kyber ensures secure key exchange between users.
    - Signatures : Dilithium ensures message integrity and authenticity.
* Real-Time Updates : Encrypted messages are sent and received in real time between clients via Flask.

**5. User Authentication**

* Session-Based Authentication :
  + Users authenticate via Flask using session-based authentication.
  + Session data is encrypted with quantum-safe algorithms to prevent unauthorized access.
* Session Management :
  + Encrypted session data is stored securely in the MySQL database.
  + Flask validates sessions for each request.

**SSL/TLS TERMINATION MEANING**

"Terminates SSL/TLS connections" refers to the process where HAProxy (or any reverse proxy/load balancer) handles the decryption of incoming encrypted traffic from clients. Here's a detailed breakdown of what this means:

**1. What Happens During SSL/TLS Termination?**

* SSL/TLS Encryption : When a client (e.g., a browser or React.js frontend) sends a request to the server, the communication is encrypted using SSL/TLS to ensure security.
* Decryption at HAProxy : Instead of forwarding the encrypted traffic directly to the backend servers (e.g., Flask or Apache HTTPD), HAProxy decrypts the traffic by performing the SSL/TLS handshake with the client. This process is called SSL/TLS termination because the encryption "ends" at HAProxy.
* Unencrypted Traffic to Backend : After decrypting the traffic, HAProxy forwards the unencrypted HTTP requests to the backend server (e.g., Flask or Apache HTTPD).

**2. Why Terminate SSL/TLS Connections?**

There are several reasons why SSL/TLS termination is commonly used in web architectures:

**a. Offload Encryption/Decryption Work**

* Encrypting and decrypting SSL/TLS traffic is computationally expensive. By handling this at HAProxy, the backend servers (e.g., Flask or Apache HTTPD) are relieved of this workload, improving their performance.

**b. Simplify Backend Configuration**

* The backend servers do not need to handle SSL/TLS certificates or encryption. They can focus solely on processing HTTP requests.

**c. Enable Traffic Inspection**

* Since HAProxy decrypts the traffic, it can inspect, modify, or route requests based on their content. For example:
  + Redirect HTTP to HTTPS.
  + Modify headers (e.g., adding **X-Forwarded-For**).
  + Route traffic to different backend servers based on URL paths or other criteria.

**d. Centralize Certificate Management**

* HAProxy manages all SSL/TLS certificates in one place, making it easier to update or renew certificates without affecting the backend servers.

**3. How Does SSL/TLS Termination Work?**

Here’s a step-by-step explanation of how SSL/TLS termination works in your setup:

1. Client Sends Encrypted Request :
   * A client (e.g., React.js frontend) sends an HTTPS request to HAProxy using quantum-safe algorithms like Kyber for key exchange and Dilithium for signatures.
2. HAProxy Handles SSL/TLS Handshake :
   * HAProxy performs the SSL/TLS handshake with the client, verifying the client's identity (if mutual TLS is enabled) and decrypting the traffic using the configured quantum-safe algorithms.
3. HAProxy Decrypts the Traffic :
   * Once the handshake is complete, HAProxy decrypts the encrypted traffic into plain HTTP.
4. HAProxy Routes Unencrypted Traffic :
   * HAProxy forwards the decrypted HTTP request to the appropriate backend server (e.g., Flask or Apache HTTPD).
5. Backend Server Processes the Request :
   * The backend server processes the unencrypted HTTP request and sends back an unencrypted HTTP response to HAProxy.
6. HAProxy Re-Encrypts the Response (Optional) :
   * If needed, HAProxy can re-encrypt the response before sending it back to the client. This is known as SSL/TLS re-encryption .

**4. Example in Your Setup**

In your environment:

* HAProxy acts as the reverse proxy that terminates SSL/TLS connections.
* The Flask backend or Apache HTTPD server receives unencrypted HTTP traffic from HAProxy.
* The quantum-safe OpenSSL library ensures that the SSL/TLS termination uses quantum-safe algorithms like Kyber and Dilithium.

**5. Security Implications**

While SSL/TLS termination simplifies the architecture, it introduces some security considerations:

* Traffic Between HAProxy and Backend : The communication between HAProxy and the backend server is unencrypted. To mitigate this risk:
  + Use a private network or VLAN to isolate HAProxy and the backend server.
  + Alternatively, enable SSL/TLS re-encryption so that HAProxy re-encrypts traffic before forwarding it to the backend.
* Central Point of Failure : HAProxy becomes a critical component in the system. Ensure it is highly available and secure.

**6. Summary**

"Terminates SSL/TLS connections" means that HAProxy handles the decryption of incoming encrypted traffic from clients, allowing it to forward unencrypted HTTP requests to the backend servers. This approach simplifies backend configuration, improves performance, and enables advanced traffic management features like routing and inspection. However, it also requires careful consideration of security to protect unencrypted traffic between HAProxy and the backend.

**WHAT TO USE FOR AUTHENTICATION**

**4. Best Way to Implement Authentication for Your Quantum-Safe Messaging App**

**Recommendation: Use Session-Based Authentication**

For your quantum-safe messaging app , session-based authentication is the better choice because:

1. Security : Sessions are more secure when implemented with **HttpOnly**, **Secure**, and **SameSite** cookies, protecting against common vulnerabilities like XSS and CSRF.
2. Simplicity : Managing sessions is straightforward for a small-scale project like a graduation project.
3. Revocation : You can easily invalidate sessions if needed (e.g., during logout or account suspension).
4. Quantum Safety : Since your app already uses quantum-safe algorithms for encryption, you can ensure that session data is stored securely on the server using quantum-safe encryption.