Mục lục

[1. Mô tả bài toán 2](#_Toc61104590)

[2. Giải pháp và kiến trúc hệ thống 2](#_Toc61104591)

[*2.1* *Cơ sở giải pháp bảo mật* 2](#_Toc61104592)

[*2.2* *Kiến trúc hệ thống và luồng xử lý* 2](#_Toc61104593)

[Diagram

Description automatically generated 2](#_Toc61104594)

[Luồng kết nối client-server: 2](#_Toc61104595)

[Luồng chứng thực client: 2](#_Toc61104596)

[3. Cài đặt 3](#_Toc61104597)

[*3.1* *Server* 3](#_Toc61104598)

[*3.2* *Client* 3](#_Toc61104599)

1. ***Mô tả bài toán***

Xây dựng hệ thống chat peer to peer bao gồm hệ thống server và phần mềm trên máy pc cho người dùng. Yêu cầu bảo mật dữ liệu của người dùng được lưu trữ trên hệ thống và bảo mật dữ liệu truyền nhận trong hệ thống tránh bị nghe lén hay thay đổi; nội dung trò chuyện giữa người dùng là riêng tư với tất cả các bên khác.

Các chức năng của hệ thống server:

* Cho phép đăng ký tài khoản trên hệ thống và đăng nhập.
* Quản lý các user đang online trên hệ thống
* Chứng thực tài khoản khi các user muốn kết nối để chat với nhau.

Các chức năng của phần mềm pc:

* Giao diện để người dùng đăng ký và đăng nhập hệ thống.
* Hiển thị danh sách người dùng trên hệ thống.
* Kết nối đến người dùng khác và giao diện chat.

1. ***Giải pháp và kiến trúc hệ thống***
2. ***Cơ sở giải pháp bảo mật***

Bảo mật trong quá trình lưu trữ: bảo vệ mật khẩu của người dùng bằng cách băm mật khẩu bằng hàm băm ***PBKDF2*** trước khi ghi xuống cơ sở dữ liệu để tránh lộ thông tin kể cả khi cơ sở dữ liệu bị rò rỉ.

Bảo mật trong quá trình truyền nhận dữ liệu:

* Bảo vệ dữ liệu giao tiếp giữa client-server và client-client bằng thuật toán mã hóa khối ***AES*** bảo đảm mức độ bảo mật và vẫn giữ tốc độ xử lý của hệ thống.
* Khóa bí mật AES của phiên giao tiếp được mã hóa bằng ***RSA*** trước khi client gửi cho server để tránh bị nghe lén và mạo danh khi bắt đầu phiên.

Chứng thực: khóa công khai RSA của các client được chứng thực bằng chữ ký của server dùng thuật toán ***SHA256withRSA*** nhằm bảo đảm client kết nối đến đúng tài khoản mong muốn.

1. ***Kiến trúc hệ thống và luồng xử lý***

Diagram

Description automatically generated with medium confidence

Luồng kết nối client-server:

Luồng chứng thực client:

1. ***Cài đặt***
2. ***Server***
3. ***Client***