**Project Report: Secure Chat Application**

**.1 Introduction:**

This project makes a secure chat app using Python. It has a server and a client. The goal is to let people chat safely using encryption.

**.2 System Architecture:**

The app uses a client-server setup:

* **Server:** Manages connections, shares messages, and keeps things secure.
* **Client:** Lets users connect to the server to send and get messages.

**.3 Features:**

* **Secure Communication:** Uses AES-256 encryption to keep chats safe.
* **Key Exchange:** The server gives each client a secret key when they connect.
* **Multi-Client Support:** Many clients can chat at the same time.
* **Message Broadcasting:** The server sends messages from one client to all the others.
* **Client Disconnection Handling:** The server handles it when someone leaves a chat.
* **Server-Side Chat:** The server operator can also send messages.

**.4 Implementation Details:**

* **Language:** Python
* **Libraries:** socket, threading, cryptography, json, os
* **Encryption:** AES-256
* **Mode**: CBC
* **Padding**: PKCS7
* **Key Exchange:** The server creates a secret key and sends it to the client.
* **Message Format:** Messages are encoded as UTF-8, encrypted, and sent with an IV.

**.5 Code Explanation:**

* Server (SecureChatServer): Handles connections, sends keys, processes messages, and broadcasts.
* Client (SecureChatClient): Connects, sends/receives encrypted messages, and decrypts them.

**.6 Security:**

* **Encryption:** AES-256
* **CBC Mode:** Secure with unique IV for each message.
* **PKCS7 Padding:** Makes sure messages are the right size.
* **IV Generation:** Random using os.urandom().
* **Key Exchange:** Server sends the key when a client connects.
* **Vulnerabilities:** Shared key, no user verification, error handling could be better.

**.7 Improvements:**

* Better key exchange (like Diffie-Hellman or RSA)
* User login
* Message buffering
* Better error handling
* SSL/TLS
* GUI interface
* Logging

**.8 Conclusion:**

This project makes a basic secure chat app with AES-256 encryption. It could be improved with things like better key exchange and user login.