Peer Review – Yihui He

Manual Code Review

The provided code is relatively well organised and spaced out and did include a well-documented README file. However, the instructions provided are not very helpful and naïve to the system using executing the code.

When looking over the code it appears that the encryption section for AES and RSA are missing in the client-side code. There is commented out code that would serve this function but is not included in the provided build. This poses a serious risk to users sending private messages as it allows for interception of messages, MITM attacks, impersonation and more attacks on the system. However, it would appear that the build works as intended and all functions described in the README work as intended, minus the encryption.

Static Analysis

The static analysis I performed used a tool called HCL AppScan CodeSweep that sweeps through many source code languages, finding and highlighting areas of vulnerability or issues within the code. This tool could not find any vulnerabilities within the provided build after scanning through the given files.

A further analysis using ChatGPT's coding assistant finds the same risk outlined in the manual review, finding that the lack of encryption for both file uploads and chat messages is dangerous and should be implemented as it is outlined in the README file. ChatGPT also suggests that there are concerns around the input validation and sanitisation which if not properly implemented can leave the system vulnerable to XSS attacks. Similarly, file upload validation is also a concern. To mitigate this, it is recommended that restrictions are put in place for what files can be uploaded such as restricting to only .txt or .pdf as well as enforcing file encryption.