Instituto Tecnológico de Costa Rica

Área Académica de Ingeniería en Computadores

Algoritmos y Estructuras de Datos II (CE 2103)

Informe Ejecutivo

Tercer proyecto: Criptografía

Profesor:

Jose Isaac Ramírez Herrera

Estudiantes:

Jestim Felix Espinoza Morales

Introducción:

En la era digital actual, la comunicación fluida y eficiente es esencial. Este proyecto aborda la necesidad de una herramienta de comunicación versátil que combine el chat en tiempo real con la transferencia de archivos, utilizando C++ y la biblioteca SFML. El objetivo principal es desarrollar un sistema de chat cliente-servidor robusto y eficiente que permita a los usuarios intercambiar mensajes de texto y transferir archivos de diferentes tipos.

Este informe ejecutivo detalla la ejecución de la propuesta de investigación, incluyendo la metodología empleada, los resultados obtenidos y las conclusiones derivadas del proceso.

Desarrollo de la metodología:

La metodología empleada se dividió en tres etapas principales:

Etapa 1: Implementación de la Comunicación Cliente-Servidor (Semana 1-2)

- **Actividades:**
  - Implementar la conexión TCP para establecer una comunicación confiable entre el cliente y el servidor.
  - Desarrollar la lógica para el envío y recepción de mensajes de texto en tiempo real.
  - Utilizar la biblioteca SFML para la gestión de la red y el manejo de eventos.
- **Evidencias:**

Etapa 2: Implementación de la Transferencia de Archivos (Semana 3-4)

- **Actividades:**
  - Implementar la funcionalidad para la selección y transferencia de archivos de diferentes tipos.
  - Diseñar un mecanismo para la segmentación de archivos grandes en bloques para una transferencia eficiente.
  - Implementar la lógica para el envío y recepción de bloques de archivos, asegurando la integridad de los datos.
- **Evidencias:**

Etapa 3: Investigación de Seguridad (Semana 5)

- **Actividades:**
  - Investigar algoritmos de criptografía simétrica (AES) para el cifrado de mensajes y archivos.
  - Investigar algoritmos de criptografía asimétrica (RSA) para el intercambio seguro de claves y la autenticación de usuarios.
  - Investigar funciones hash (SHA-256) para la verificación de la integridad de los mensajes.
  - Analizar la viabilidad de la implementación de protocolos de comunicación segura como TLS/SSL.
- **Evidencias:**

Conclusiones:

El desarrollo del sistema de chat cliente-servidor con transferencia de archivos se ha llevado a cabo con éxito, cumpliendo con los objetivos planteados en la propuesta de investigación. La elección de C++ y SFML ha demostrado ser adecuada, permitiendo la creación de un sistema robusto, eficiente y escalable.

La implementación de la comunicación cliente-servidor y la transferencia de archivos se realizó de manera efectiva, permitiendo a los usuarios intercambiar mensajes y archivos de forma confiable. La investigación de

seguridad ha sentado las bases para una futura implementación que garantice la confidencialidad e integridad de la información intercambiada.

Posibles Mejoras y Cambios:

- Implementar la funcionalidad de cifrado de mensajes y archivos utilizando los algoritmos de criptografía investigados.
- Integrar un sistema de autenticación de usuarios para asegurar la identidad de los participantes en el chat.
- Implementar la funcionalidad de chat grupal para permitir la comunicación entre múltiples usuarios.
- Optimizar el rendimiento del sistema para manejar un mayor número de usuarios concurrentes.
- Desarrollar una interfaz gráfica de usuario más intuitiva y amigable.