Characterization Document

for

Workshop: Network Applications

Application: Decentralized P2P Messaging application

Submitted by: Shai Michaeli – 316221019

CONTENTS

INTRODUCTION

PROJECT OVERVIEW

In an era where digital communication has become indispensable, concerns over privacy and data security are more pronounced. My project introduces a peer-to-peer (P2P) messaging mobile app designed to address these concerns by facilitating direct, encrypted communication between users without relying on centralized servers for message relay.

PROJECT OBJECTIVES

Enhance Privacy

To provide a good level of privacy by ensuring that messages are only accessible to the intended recipients, with no intermediaries having access to the content.

Promote Data Security

To implement robust end-to-end encryption, safeguarding users' messages from potential sniffing or data breaches.

Improve Reliability and Speed

To offer a more reliable and faster messaging experience by reducing dependence on centralized servers that can be bottlenecks or single points of failure.

CHARACTERIZATION

PRODUCT OVERVIEW

Solution Description

This application enables users to exchange messages directly with one another without the messages passing through a central server. The app is designed to support text messages, images, and videos, ensuring that communication remains between the sender and the receiver only.

Target Audience

The primary users of this app are individuals who prioritize the confidentiality of their communications and are looking for alternatives to traditional messaging apps that rely on centralized servers for data transmission.

KEY FEATURES

Direct Messaging

Users can send and receive text, images, and videos directly to and from other users without intermediary storage or processing.

Discovery Mechanism

A service like Firebase is used initially for peer discovery. This mechanism assists users in finding and connecting with other users by registering their presence and facilitating the exchange of necessary information for establishing a P2P connection.

End-to-End Encryption

All messages are encrypted from the moment they are sent until received, ensuring that only the sender and intended recipient can read them.

FLOW AND SCENARIOS

User Registration

Upon launching the app for the first time, users are prompted to register. This process includes the device registering with the discovery service, facilitating the initial connection setup with other users.

Finding Peers

The app uses the registered information in the discovery service to notify users about the presence of new peers and enables the establishment of a direct connection for messaging.

Sending and Receiving Messages

Once a direct connection is established, users can exchange messages in real-time. If the recipient is not online, the sender's app stores the message and attempts to send it when the recipient is available.

HIGH-LEVEL DESIGN

ARCHITECTURE OVERVIEW

The app's architecture is divided into two main components: the client application, which runs on the user's mobile device, and a server-based discovery service. The client application handles direct messaging, messaging, encryption, and local storage of messages. The discovery service facilitates the initial connection between users.

COMPONENTS

Mobile App (Client)

- User Interface:
  Provides functionalities for sending and receiving messages and managing contacts.
- Local Data Storage:
  Stores messages and contacts information locally on the device, ensuring data remains accessible even when offline.
- Networking Capabilities:
  Manages direct P2P connections for message exchange and interacts with the discovery service for peer discovery.
- Encryption Module:
  Responsible for encrypting and decrypting messages to ensure privacy and security.

Discovery Service (Server)

- User Registry:
  Maintains a list of active users and their associated information necessary for establishing P2P connections, such as public keys and, if necessary, last known IP addresses.
- Notification Mechanism:
  Utilizes Firebase Cloud Messaging (or a similar service) to notify clients about new users joining the network or updates required for maintaining active connections.

EXTERNAL TOOLS AND LIBRARIES:

Firebase Cloud Messaging (FCM)

Used for sending notifications to clients about peer discovery and other relevant updates.

WebRTC

Facilitates real-time P2P communication between devices, including handling NAT traversal issues.

Encryption Libraries

Libraries such as 'OpenSSL' or 'libsodium' are used for implementing end-to-end encryption of messages.

DATA MANAGEMENT

User Information

- Table Structure:
  Includes columns for user ID, public encryption keys, and other relevant information like device identifiers or last known IP addresses for initiating direct connections.

Message Storage

- Local Storage:
  Messages are stored locally on the device in an encrypted format. The storage structure ensures that messages are only accessible by the app and are protected against unauthorized access.