

PriviChat: A Secure P2P Communication App

Project Number: 15004114

Team Members: Shai Michaeli

Lecturer: Amir Kirsh

Workshop: Network Applications



The Privacy Problem in Modern Chat Apps



End-to-End Encryption Issues: Many chat apps store backups on cloud servers that are often not encrypted, leaving them vulnerable.



Metadata Collection: Even if messages are encrypted, metadata can reveal communication patterns.



Data Selling: User data is often sold to third parties, compromising privacy.



Target Audience: Privacy-conscious users, activists, journalists, and professionals handling sensitive information.

PriviChat: The Secure Alternative



Peer-to-Peer (P2P)
Communication: PriviChat uses a decentralized architecture for direct communication.



End-to-End Encryption: Every message, file, and call is encrypted from sender to recipient.

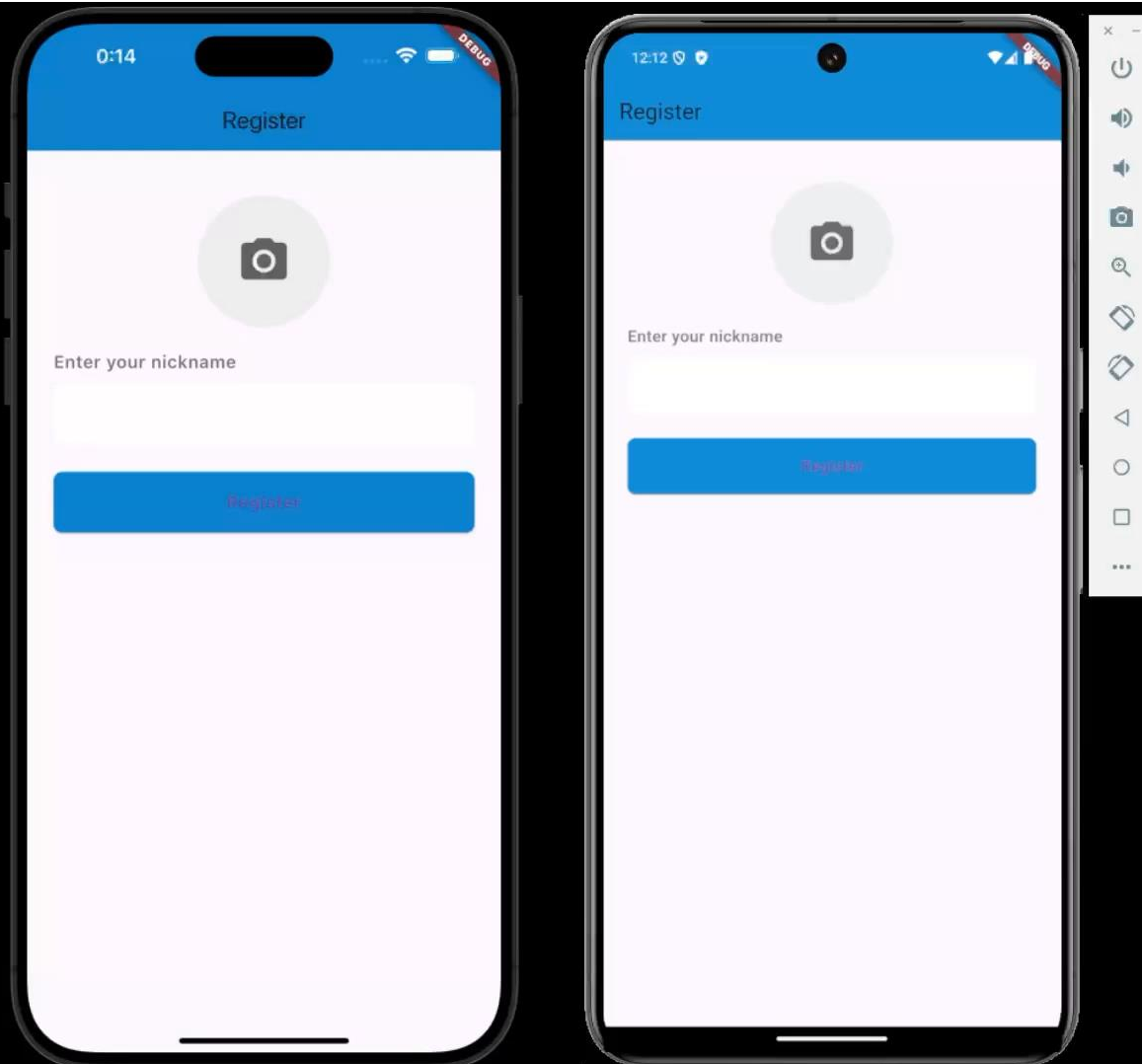


Local Data Storage: All data is stored locally on the user's device.



Transparency and Control: Users have full control over their data with no hidden backdoors.

PriviChat Demo Video



Technologies and Data Flow in PriviChat

Technologies Used:

- Flutter for cross-platform development.
- Firebase Firestore for P2P discovery.
- WebRTC for secure P2P communication.
- Kotlin and Swift for OS-specific adjustments.



Technologies and Data Flow in PriviChat

Data Flow:

Client 'A' initiates communication and discovers Client 'B' using Firebase Firestore.

WebRTC initiates a handshake for a direct P2P connection.

Secure data transmission occurs directly between devices.

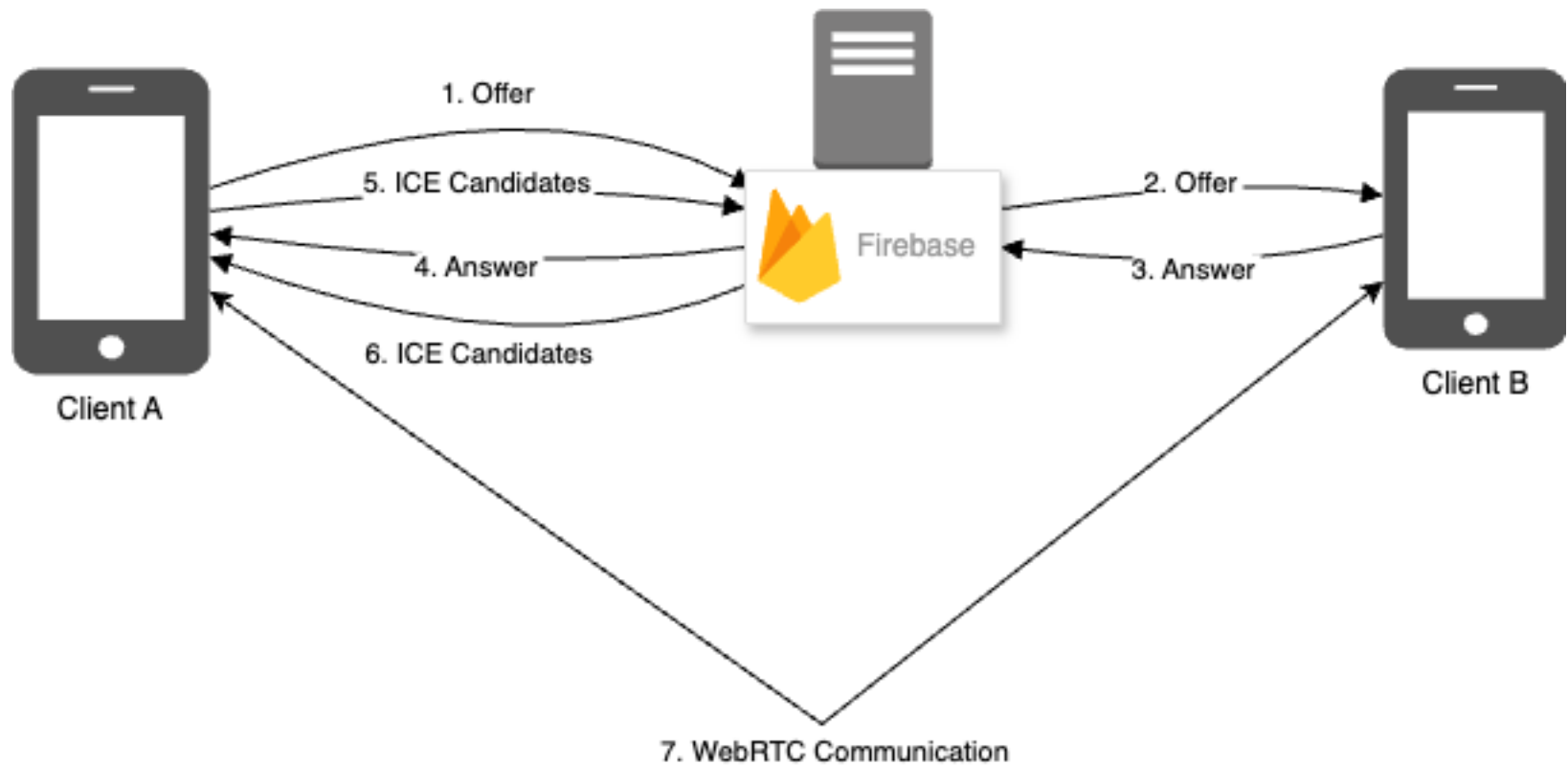
WebRTC Handshake:

ICE Candidates are used to find the best path for P2P connection.

DTLS-SRTP Encryption secures the connection.

Once the handshake is complete, secure P2P communication is established.

Technologies and Data Flow in PriviChat



Alternatives to PriviChat's Approach



Signal: Secure messaging app using end-to-end encryption but relies on centralized servers.



Briar: P2P messaging app using Bluetooth or Wi-Fi for communication.



Server-Based Encryption Models: Apps like WhatsApp offer strong encryption but involve cloud backups and metadata collection.



Drawbacks Compared to PriviChat: Centralized servers, metadata collection, reliance on cloud backups, and less user control.

PriviChat: Secure Communication for the Modern Age

Summary:

- PriviChat addresses critical privacy issues using a decentralized P2P approach, end-to-end encryption, and local data storage.

Impact:

- PriviChat's architecture ensures users have complete control over their data and communications.