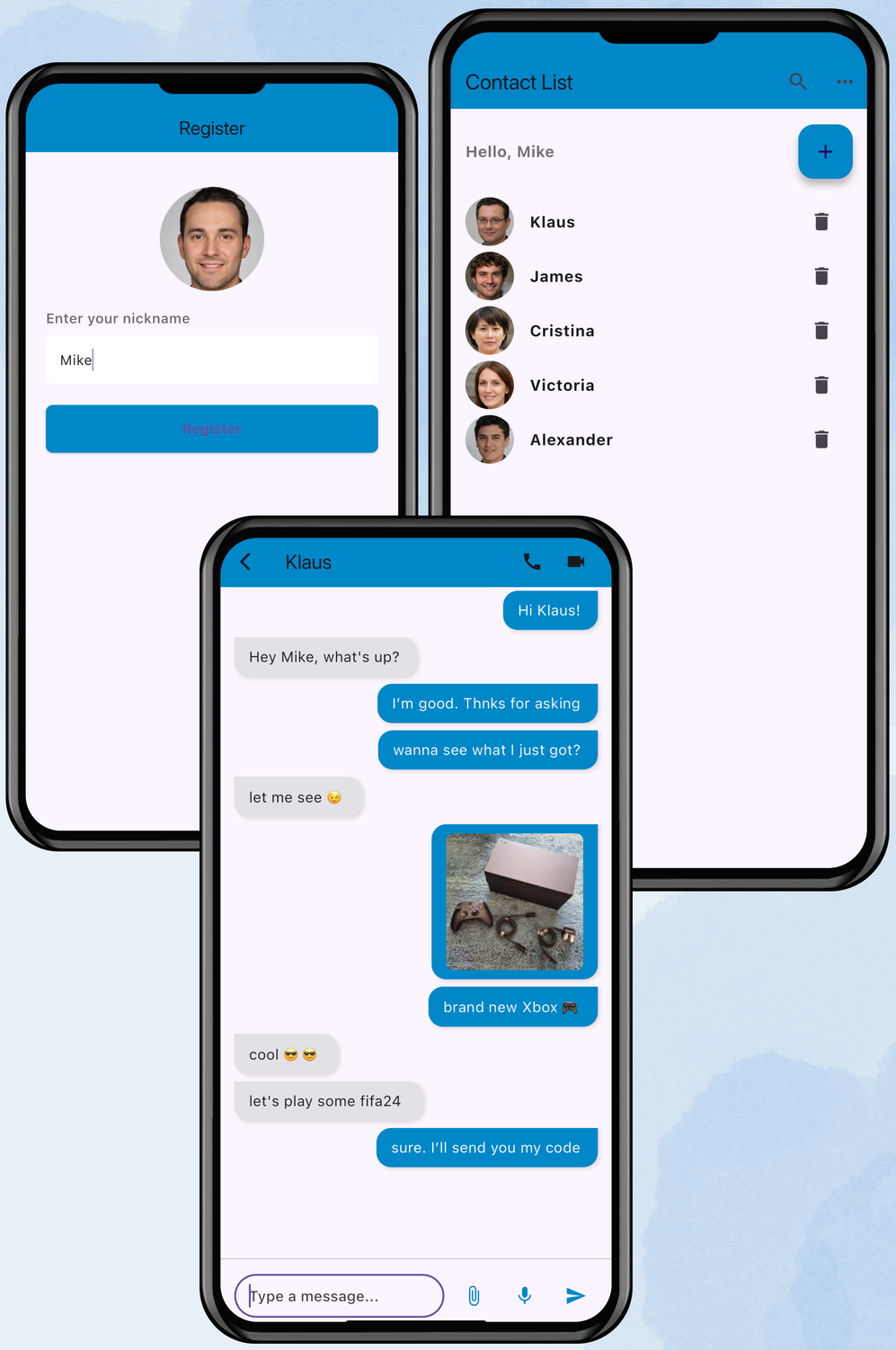
Project Number:
15004114

Project Name: PriviChat
Submitter: Shai Michaeli
Lecturer: Dr. Amir Kirsh

PriviChat



Introduction

In today's chat apps, the main issues are the potential disadvantages of end-to-end encryption and the collection of metadata. These problems can compromise user privacy, as encrypted messages stored on cloud servers may not be secure, and metadata can reveal patterns of communication. Additionally, user data is often sold to third parties, further eroding trust and privacy.
PriviChat solves these problems by utilizing a peer-to-peer (P2P) approach, eliminating the need for centralized servers. This ensures that your messages stay private, no metadata is collected, and your data isn't sold, providing a truly secure and private communication experience.

Goals & Objectives

- **Keep Users' Privacy:** Prioritizing the protection of user data and ensuring confidential communication.
- **Maintain End-to-End Encryption:** Ensuring that all messages and calls are securely encrypted from sender to recipient.
- **Implement Peer-to-Peer (P2P) Communication:** Eliminating the need for central servers by using WebRTC for secure text, media, and call transmission.
- **Store Data Exclusively on Devices**: Ensuring that all data remains on the user's device, with no external storage or access.

Technologies

- **Developed in Flutter:** Ensures a cross-platform experience, allowing PriviChat to run seamlessly on both Android and iOS devices.
- **Utilizing Firebase Firestore:** Employed for the P2P discovery process, enabling efficient and secure user connection.
- **WebRTC:** Used for the peer-to-peer (P2P) communication, facilitating secure text, media, and voice/video calls without the need for centralized servers.
- **Kotlin and Swift:** Implemented for specific OS adjustments, ensuring optimal performance and integration on Android and iOS platforms, respectively.