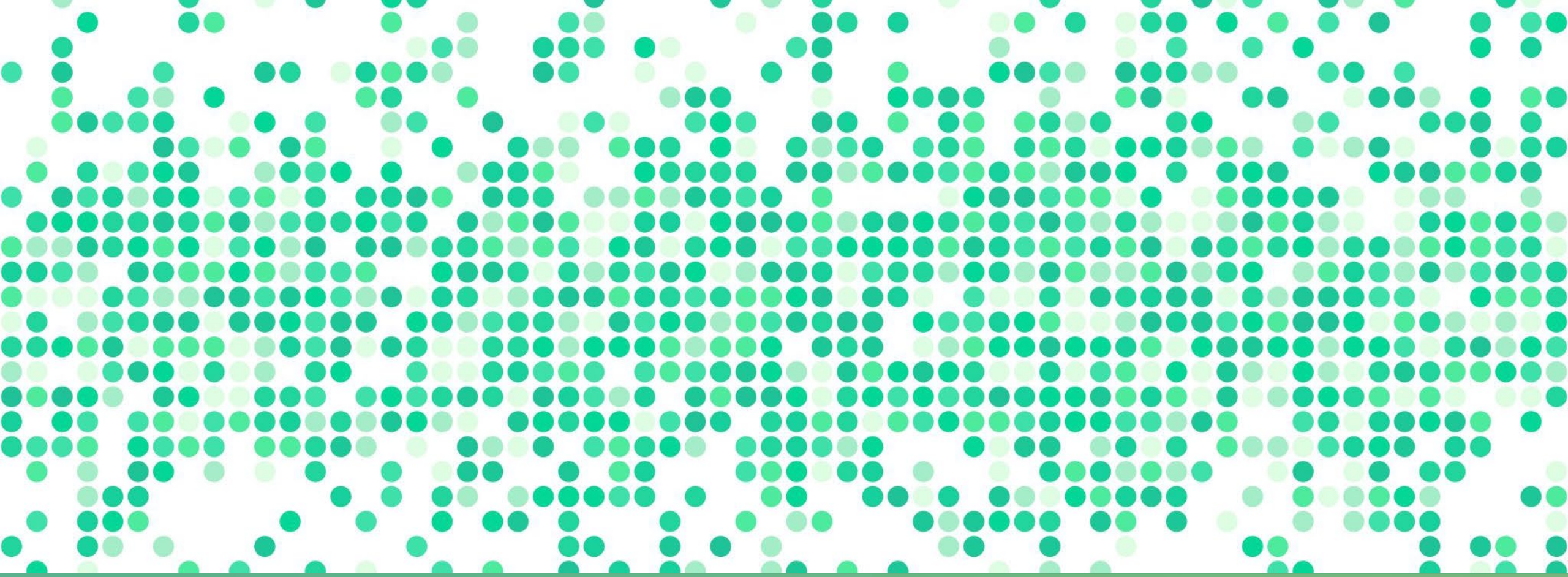


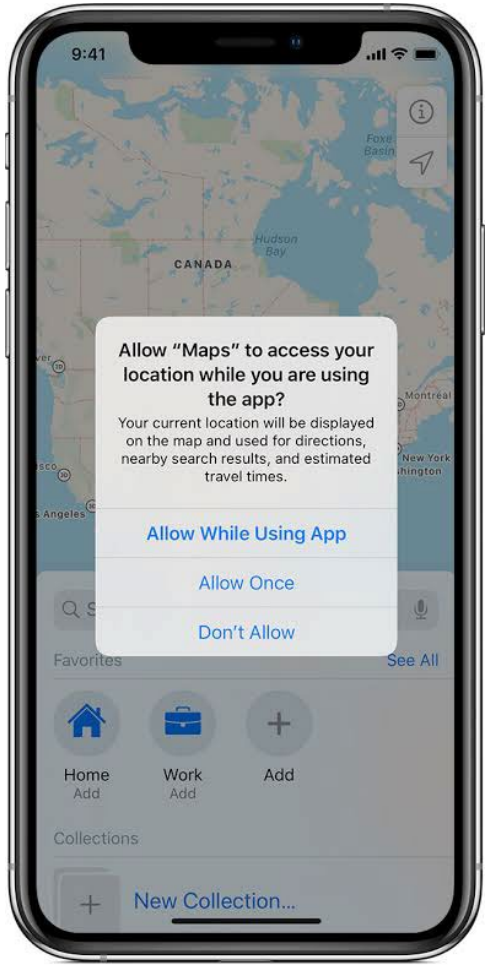
PAIRLOSH - PRIVACY PRESERVING PAIRED LOCATION SHARING CROWDSENSING MECHANISM

PRESENTED BY DOMINIC ADAMS AND MEHUL SEN

MOTIVATION

Location data is extensively shared with wide range of individuals.

- Ride-Hailing Apps (Uber, Lyft)
- Social Media Platforms (Instagram, Snapchat)
- Navigation Apps (Google Maps, Waze)
- Fitness Apps (Fitbit, Strava)
- Delivery Apps (UberEats, Doordash)



It is essential to preserve location privacy.

- Protect personal information
- Preserve anonymity in public spaces
- Avoid targeted advertising

There are risks associated with sharing location data.

- Surveillance and tracking by government or companies.
- Privacy breaches, and identity thefts
- Stalking or harassment by individuals

PROBLEM

Insert limitations of existing solution here

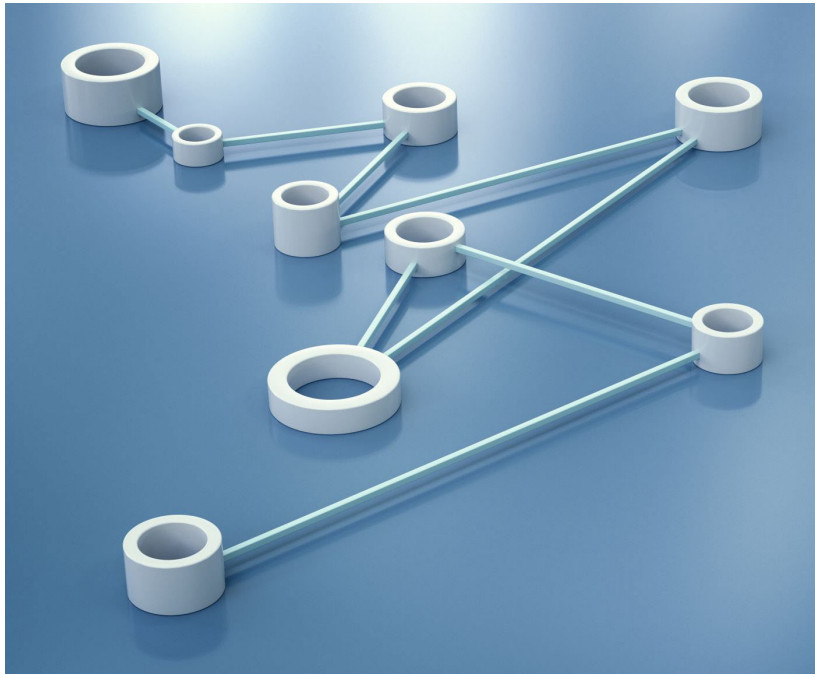
SOLUTION

PairLoSh – Privacy preserving paired location sharing crowdsensing mechanism.

Processes: Pairing, Obfuscation, Aggregation, Encryption

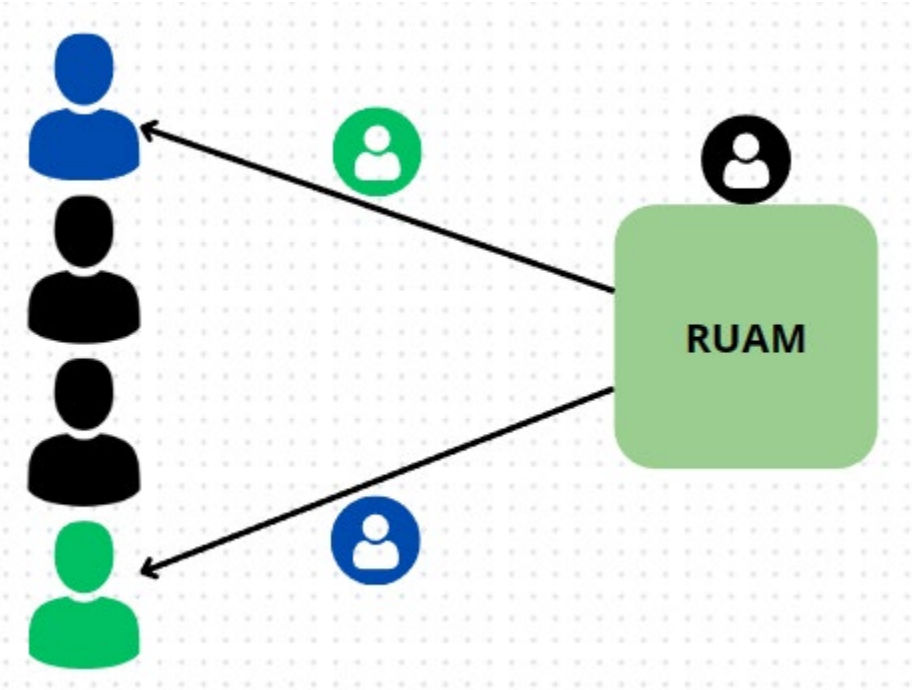
Components: Users, Server, Agent

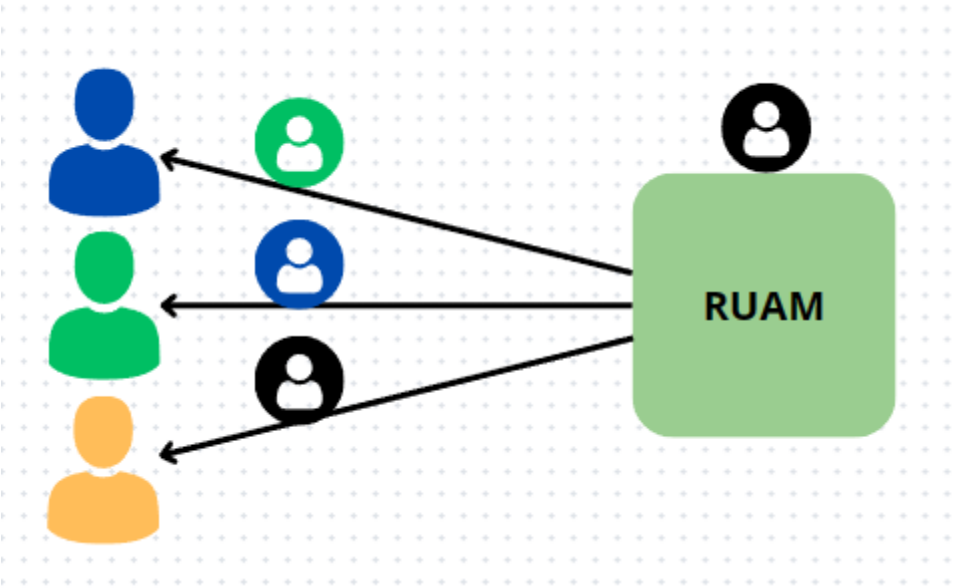
Modules: Obfuscated Data Aggregation Module (ODAM), Random User Allocation Module (RUAM)



RANDOM USER ALLOCATION MODULE(RUAM)

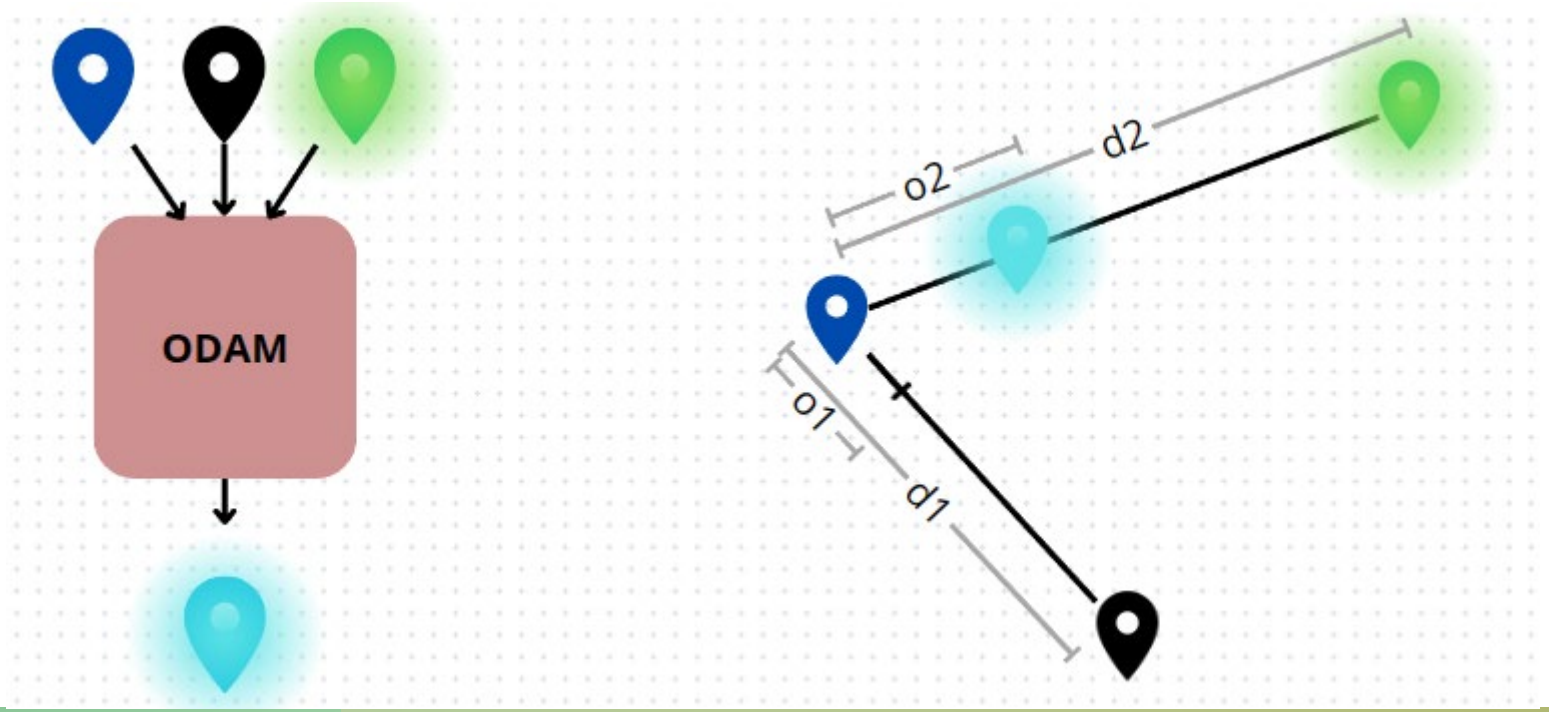
Link two random users within the system and share their pairings.



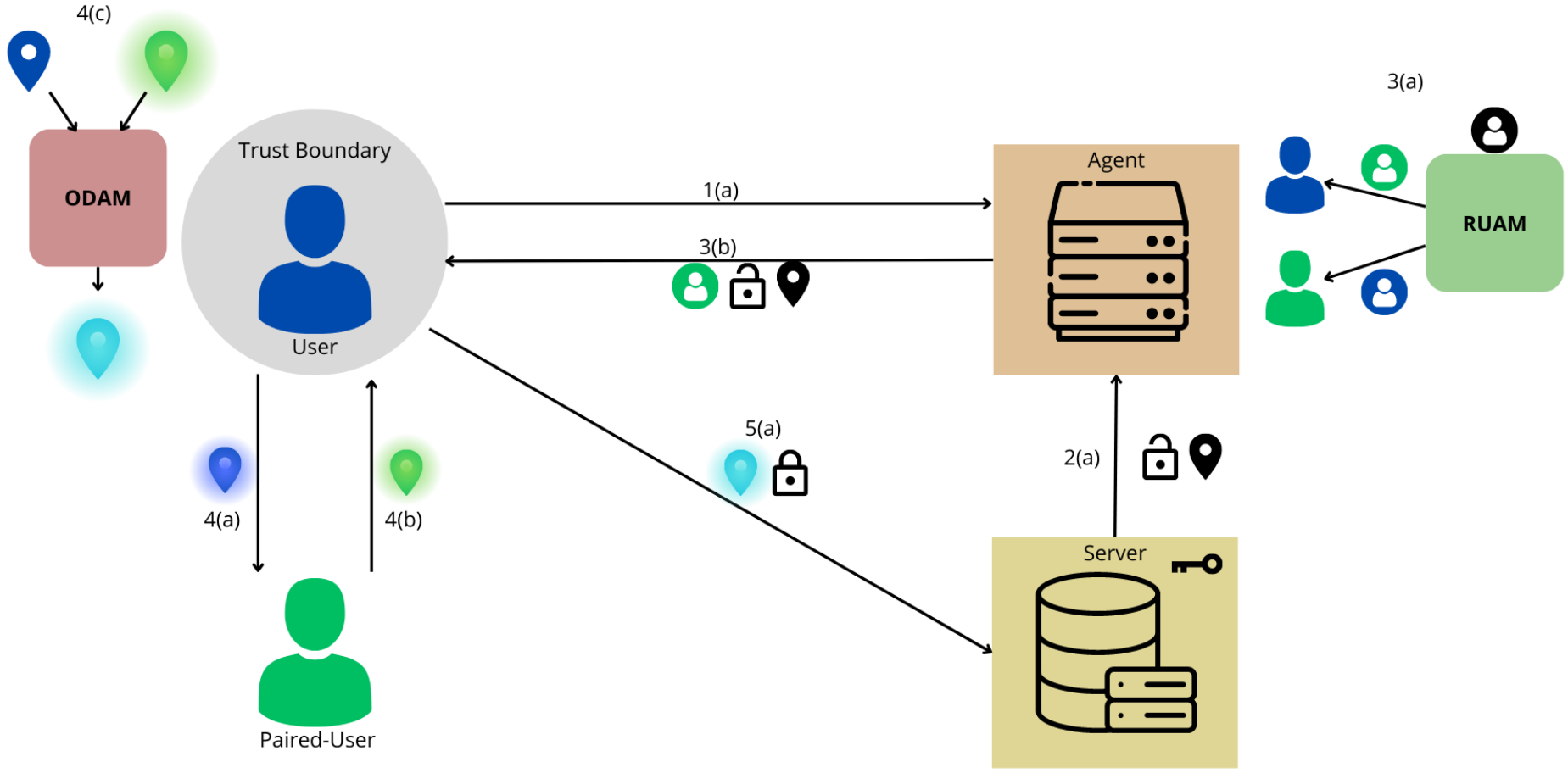


OBFUSCATED DATA AGGREGATION MODULE (ODAM)

Generate the shared obfuscated location using True User location, Obfuscated Paired-User Location, Server Location



PAIRLOSH ARCHITECTURE



PERFORMANCE EVALUATION

FUTURE WORK

CONCLUSION