

**School of Computer Science and Engineering**  
**CSE4003 – Cyber Security**  
**WIN 2021-2022**

**Problem Statement**

With increase in demand for the online ride hailing services, The number of security attacks on the customers also increased. So the need to preserve customer security became imminent in the online ride hailing, The use of third trusted parties was able to preserve the privacy up to a certain extent but it couldn't completely address the issue.

**Privacy-Preserving Online Ride-Hailing System Without Involving a Third Trusted Server**

Ayush Tiwary [19BCE2049], Alokam Nikhitha [19BCE2555], and Galla Kiran [19BCE2583]

**Domain Introduction**

Many ORH services have started which help the riders to easily book a ride on their phone. It was great until people started to realize the privacy concerns, It is then that the use of a third trusted server came into play but this couldn't fully address the privacy concerns. So techniques like Road Network Embedding (RNE) are used for distance calculation and this is uniquely bridged with cryptographic primitives like Property-preserving Hash (PPH) to safeguard the riders privacy.

**Techniques & its Related Challenges**

The main issue with the ORH services is regarding privacy of both Rider and Driver. Techniques like Homomorphic Encryption can perform computations on the data which is encrypted. But this technique can only give the Euclidean distance between the rider and driver which is not viable for ORH in road networks as vehicles are obliged to go along the streets, where in Property-Preserving Hash can calculate the distance by using Road Network Embedding which estimate the distance with Road networks and do the ride-matching, but matching performance may get affected as it doesn't have advanced road network to support dynamic road weights and some malicious riders/drivers intentionally leak the private keys which leads to privacy issues.

**Research Findings**

Conventionally an attacker who tries to steal the sensitive information from the ORH server can monitor the encrypted RNE vectors and the ride-matching data but the results obtained through this paper are pertaining to maintain the privacy of the customer in the online ride-hailing system, without involving a third trusted party and match the nearest driver for each rider while preserving both driver privacy and rider privacy.

**Statement of Purpose**

We are going to proceed with Review based approach . The reason for opting this approach is to provide information on various techniques which are used for preserving privacy in ORH services and to find the best technique which provides the maximum privacy with high ride-matching accuracy.