VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

**School of Computer Science and Engineering**

**CSE4003 – Cyber Security**

**WIN 2021-2022**

**Course Slot : A2 SLOT**

**Course Instructor : Dr. B. D. DEEBAK / SCOPE**

**Project Associates:**

**1. Ayush Tiwary [Reg. No. 19BCE2049]**

**2. Alokam Nikitha [Reg. No. 19BCE2555]**

**3. Galla Kiran [Reg. No. 19BCE2583]**

**PROJECT TITLE**

# Privacy in Online Ride-Hailing Servers

# Table of Contents

## Objective

The growing popularity of online ride-hailing (ORH) services has made our daily travel much easier. It enables a rider to quickly and easily request the nearest driver via mobile devices. Existing ORH systems, on the other hand, necessitate the collection of users' location data, raising serious privacy concerns. While several privacy-preserving ORH service solutions have been proposed, the majority of existing schemes rely on a third trusted party to compute the distance between a rider and a driver. For practical deployment, such a security assumption cannot fully address privacy concerns. We present a new ride-matching scheme for ORH systems that allows for privacy-preserving and effective distance calculation without the use of a third-party server in this paper.

## Background and Motivation

Our proposed scheme allows ORH systems to securely compute the user distance while protecting both riders' and drivers' location privacy. In particular, we employ cutting-edge distance calculation techniques based on Road Network Embedding (RNE) and demonstrate how to uniquely bridge cryptographic primitives such as Property-preserving Hash (PPH) with RNE in depth to support privacy-preserving ride-matching services. Furthermore, we propose an optimised design to improve matching efficiency. We conduct a formal analysis of the security strengths and put the system prototype into action. The evaluation results show that our design is safe and efficient for ORH systems.

# LITERATURE REVIEW

| S.No: | Title | Citation | Abstract |
|---|---|---|---|
| 1. | Quantifying the Tradeoff Between Cyber-security and Location Privacy | Dajiang Suo, M. Elena Renda, and Jinhua Zhao | Increasing location privacy in Location Based Services could protect users' data in case of breaches, it could also lead to security issues for users. In this paper they  examined the impact of location data privacy-preservation on the performance of the anomaly detectors. A Density-based Spatial Clustering of Applications with Noise (DBSCAN) and a Recurrent Neural Network (RNN) framework are used to match the trip and  two dimensional Laplace noise is used to preserve the location privacy of the users. The investigation results clearly show that while the level of privacy increases, by increasing the perturbation noise, the capacity for the system to identify anomalies could decrease quite sensibly, especially when using the clustering. |
| 2. | pShare: Privacy-Preserving Ride-Sharing System with Minimum-Detouring Route | Junxin Huang , Yuchuan Luo , Ming Xu, Bowen Hu and Jian Long | They primarily investigate the privacy and utility of the ride-sharing system, which allows multiple riders to share one driver, in this paper. They proposed pShare, a privacy-preserving ride-sharing system, to solve the privacy problem and reduce ride-sharing detouring waste. They used a zone-based travel time estimation approach to privately compute over sensitive data while cloaking each rider's location in a zone area to hide users' precise locations from the service provider. To compute the matching results, as well as the least-detouring route, the service provider first computes the shortest path for each eligible rider combination, then |

| | | | |
|---|---|---|---|
| | | | compares the additional travelling time (ATT) of all combinations, and finally chooses the combination with the lowest ATT. |
| 3. | SRide: A Privacy-Preserving Ridesharing System | Ulrich Matchi Aïvodji,Kévin Huguenin , Marie-José Huguet, Marc-Olivier Killijian | Modern ridesharing systems, which have been enhanced with location-based features, have improved user experience by allowing drivers and riders to plan trips in near real time. The fine-grained nature of location data collected by service providers and exchanged between users, on the other hand, raises privacy concerns that could stymie the adoption of such systems. They presented SRide: a privacy-preserving ridesharing protocol that addresses the matching problem for dynamic ridesharing systems in this paper. They designed and build an SRide prototype that works in four steps. Firstly, it generalises user spatiotemporal data. Then, to compute feasible matches, it employs a privacy preserving protocol. . Then, for each feasible pair, it computes a ridesharing score using an improved version of Priv-2SP-SP, a privacy-preserving protocol for computing meeting points for ridesharing. Finally, based on their ridesharing scores, it computes the optimal assignment of drivers and riders. To demonstrate the proposed scheme's practical feasibility, we conduct an experimental trace-driven evaluation. |
| 4. | HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System | Iraklis Symeonidis , Dragos Rotaru, Mustafa A. Mustafa , Bart Mennink, Bart Preneel, and Panos Papadimitratos | In this paper, They propose HERMES, a scalable, secure, and privacy-enhancing vehicle sharing and access system.<br>HERMES securely outsources vehicle access token (AT) generation operations to a group of untrusted servers. It extends the system design of |

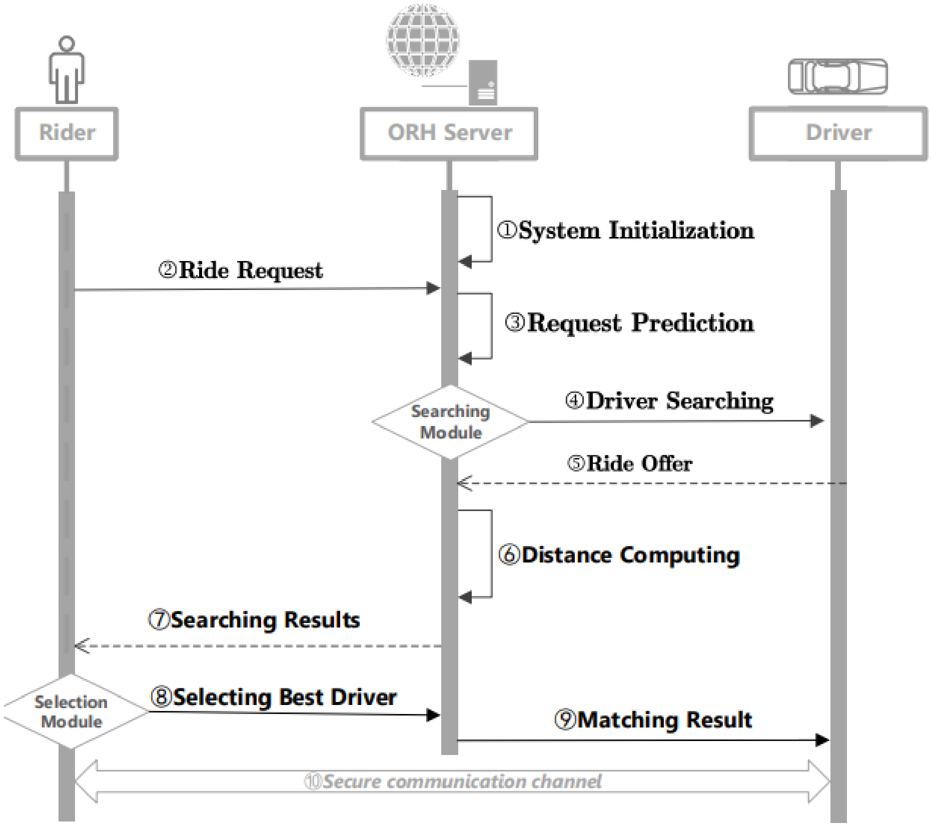
|  |  |  |  |
|---|---|---|---|
|  |  |  | an earlier proposal, SePCAR, for improved efficiency and scalability. HERMES efficiently employs and combines several cryptographic primitives with secure multiparty computation (MPC) to meet system and user needs for secure and private computations. It hides vehicle secret keys and transaction details from servers, such as vehicle booking details, AT information, and user and vehicle identities. It also ensures user accountability in the event of a dispute. Furthermore, they provide semantic security analysis and demonstrate that HERMES satisfies its security and privacy requirements. |
| 5. | Location privacy-preserving in online taxi-hailing services | Xiaoying Shen1 · Licheng Wang1 · Qingqi Pei2 · Yuan Liu1 · Miaomiao Li | Because of its convenience and low cost, online cab hailing has become the most common means of transportation. However, because online taxi-hailing service providers can track their specific movement trajectories, it creates a privacy risk to consumers and drivers. Furthermore, with the existing online taxi-hailing system, there is a time delay between the time a passenger makes a request and the time the driver arrives at the passenger's boarding point. They provided a new and efficient location privacy protection approach based on the MinHash algorithm to address these two issues (LPPM). The LPPM converts the precise positions of passengers and drivers into a set of points of interest surrounding them, and the distance between them into the similarity between the two sets. Using the MinHash technique, a service provider can efficiently match passengers and drivers without giving their particular location information. To overcome the second obstacle, they |

| | | | |
|---|---|---|---|
| | | | deploy mobile edge computing technologies in an online taxi-hailing system in this work. It can speed up data processing, allow drivers to plan ahead of time, and lessen the likelihood of traffic gridlock. LPPM has a high level of security, according to the security study, and the final experimental findings indicated that LPPM is effective. |

## Methodology

The conventional methodology was to use a third party server to address the customers privacy but this did not completely solve the issues as the key was still in the third persons hand, Hence the methodology followed in this paper is as follows:

- Homomorphic Encryption to perform computations on encrypted data. So that the data can be computed without the access to the secret key.But in this method we can only calculate the euclidean distance i.e: the displacement between two points which is not useful to the online ride hailing system.
- Property preserving hash which can use Road network Embedding to calculate the distance between the driver and the rider with the streets taken into account, but the matching performance may get affected as it doesn’t have advanced road network to support dynamic road weights.
- For secure distance calculation, trusted hardware technologies (e.g., Intel SGX). However, the security of their architecture is contingent on the presence of trusted server hardware.
- Bit-block encryption and a Property-preserving Hash (PPH)-based difference evaluation algorithm can be used. Here the main idea is to use bilinear mapping to encrypt RNE vectors into bit-blocks, then incorporate the bit weight with random masks in each block cypher.



## SECURITY ASPECTS:

### CONFIDENTIALITY

Confidentiality refers to protecting information from being accessed by unauthorized parties. Homomorphic encryption is being used for encrypting data. The data includes the location coordinates of the user and the driver. Even when the transmission or storage medium has been compromised, the encrypted information is practically useless to unauthorized persons without the proper keys for decryption. If intercepted, the interceptor will not be able to crack unless they know the key.

**ACCESS CONTROL**

Users and drivers are provided with passcodes and usernames to grant access for the information that is actually useful for them. It ensures that only the people eligible to be the part of a particular resource are granted permission and able to log in to the chat room created.

**NON-REPUDIATION:**

Non repudiation ensures that the user cannot deny sending something. The location coordinates once posted cannot be deleted and users cannot deny sending their location to the server and it will be stored once the session between the user and the driver in a group is terminated/ended. In the online ride hailing application non-repudiation is ensured so that the user cannot delete his location or change it abruptly.

**AUTHENTICATION:**

User ID and password can be used for authenticating that the user belongs to a registered set of people who can access the online ride hailing application. All the passwords are encrypted, So there won't be any compromise with the users safety and only the authorized users can access the app.

## Tools Description

# User Interface

The user can protect his secrets with help of SGX, secrets may contain Personal ID info
Bank Details
Biometric Factors
Passwords
Encryption Keys
Intellectual Property

Secrets of this nature must be secured in order to protect the privacy financial interest and even the safety of both individuals and businesses

## Features

The various features of the Online Raid Hailing System without a third party are to use Encrypted Locations for Ride-Matching which is safe, the secure value comparison which is based on PPH. Building a Safe Ride-Matching Scheme so that the Original location is not being leaked. And also for the improvement of ride-matching performance.

## Specifications

- We will be using Homomorphic Encryption to perform computations on encrypted data.

- As we need the distance and not the displacement we will use road network embedding to effectively calculate the distance between the rider and the driver.

- We will then bridge itb with the cryptographic primitives like property preserving hash to safeguard the users privacy.