Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

ICAR: AN INNOVATIVE APPLICATION FOR FACILITATING CARPOOLING

[1] **B.V.S. Uma Prathyusha,** Assistant Professor, [2] **M. Kotamma,** Assistant Professor,
[3] **R. Kalyan Chakravarthi,** Assistant Professor, [4] **A.V. Karthik Kumar**, Assistant Professor
[1234]Audisankara College of Engineering & Technology (AUTONOMOUS), Gudur (M), Tirupati (D), A.P, India-524101

ABSTRACT - Due to poor traffic conditions and the high costs of travelling byprivate cars, ride sharing has become a popular means to trip. In view of the securitythreats and centralization existing in the current ride-sharing service, we propose asecure ride-sharing scheme based on a consortium, which can guarantee the security, confidentiality and privacy of data interaction via attribute-based proxy re- encryption algorithm [1]. First, the passenger presets the access structure and encrypts the data using attribute-based encryption. The ciphertext is then sent to the roadside unit (RSU), which broadcasts the carpooling request to the driver. After receiving the request, the driver sends the itinerary attribute to RSU, which performs carpool matching according to received ciphertext and itinerary attributes, then the ciphertext isre-encrypted and sent to the matched driver. Second, the master node uses an improved DPoS (Delegated Proof of Stake) consensus to verify the carpool record, which is stored on the after the verification is successful. In case of disputes, block data can be utilized for traceability. Third, drivers and passengers use the credibility mechanism to score each other after ride sharing. In addition, trusted authority can reveal the real identity of malicious users [2]. Finally, we conduct securityanalysis and performance evaluation for our proposed scheme. The results manifest that our scheme not only meets the security and privacy requirements of ridesharing services,but also effectively resists potential security risks. Therefore, our scheme is feasible, efficient and suitable for ride-sharing services [3].

Index Terms— Car-Pooling, Smart contract, Data privacy, Costs

I. INTRODUCTION

With the development of the sharing economy and vehicular ad hoc networks (VANETs), ride sharing (carpooling) and ride hailing are increasingly becoming a significant mode of travel [4]. On the one hand ride sharing alleviates traffic congestionduring rush hour, solves the shortage of

taxi in bad weather. On the other hand, although the number of private cars is increasing year by year, the actual utilization rate is not very high so that private cars are often idle. At thesame time, regular maintenance and car insurance are needed for these vehicles, which will increase people's economic burden [5]. However, ride sharing is very convenient, low cost, and can reduce energy consumption as well as pollution (e.g. exhaust emissions). In view of above benefits, some ride-sharing services provider such as Uber and Lyft have recently providedservices to millions of users in hundreds of cities. Didi, the largest ride-sharing service provider in China, has 450 million users and provides 20 million ride-sharing services for users every day [6]. To carpool passengers and drivers publish their itineraries (e.g. starting point, departure time, and destination) on the application (app). Theridesharing service provider matches supply and demand based on the information provided by passengers and drivers. Relevantinformation about the driver is sent to the mobile device of the successfully matchedpassenger and the passenger's itineraries are sent to the successfully matched driver, thereby facilitating the driver providing the passenger with ride-sharing services. Along with the convenience of ride-sharing services, numerous security threats have also emerged. Consequently, many academics attach great attentions to researching and improving the ride-sharing service. Ni et al. proposed an anonymous two-way authentication scheme based on BBS+ signature, which is used for registration ofthe identity of passengers and drivers andthen authentication of their identities when they use the system [7]. The ride-sharing service system matches the authenticated passengers and drivers to achieve the shared ride mutually. The ride-sharing system provides plaintext information, such as the identity and location of passengers, potentially compromising the privacy and safety of the people in the carpool [8]. Sherif et al. used groupsignatures to protect user's privacy. The server used similarity measurement techniques to detect the similarity of travel data and searched for the driver that best matched the passengers. A ride-sharing platform based on trust level was used toimprove the security of the system and the trust between users. The platform relies on the cloud server to provide users with a reliable measurement of whether to trust another user or not. Hallgren et al. achieved ride-sharing matching based on the similarity of departure and destination and used the Shamir secret sharing scheme to protect the privacy of the user's route. The aboveschemes have achieved rideshare, they meanwhile bring about some risks and challenges, one of which is that security and privacy are threatened. It is easy for an attacker to eavesdrop, tamper with, or forge trip information sent by users (passengers and drivers) on an open wireless communication network. Unsurprisingly,

Hackers can infer users' privacy information, such as work unit and home address from theobtained information. The issue is deteriorated by the case that attackers misuseusers' privacy information. For example, an attacker burgles users' homes once they haveleft. Besides, systems used by most existing ride-sharing services have a centralized structure, which depends on a trusted third party to store and process travel information sent by users. Once the central node is hacked, it can no longer be considered tocontain trusted data as the basis for dispute arbitration [9]. What's more, the single point attack can be used to easily threaten the security of the entire system. Worse still, the centralized structure is prone to information monopoly or information islands. As a result,the ride-sharing service providers may abuse data or sell users' data to other organizations.

For instance, Uber used the cloud platform toleak users' data to other organizations. Last but not least, existing ride-sharing schemes have large computational costs and communication overheads, which give rise tothe poor performance and affect thematching efficiency in ride-sharing systems [10].

Inspired by the above challenges, it is of vitalimportance to propose a secure, decentralized, data traceable and efficient ride-sharing service. As an emerging technology with the features of secure, credibility, tamper resistance as well astraceability, has set off a research boom all over the world [11]. Without authorization, any node in the public can join or leave the network freely, resulting in all nodes having read and write permissions for data. It is an arduous task for the public to reach aconsensus quickly among nodes. Moreover, an attacker can easily forge a large number of fake nodes. Therefore, the public is not suitable for ride-sharing services [12]. On the contrary, a private is only open to individual organizations or institutions. Furthermore, data read as well as write permissions are strictly controlled by a few trusted nodes, which is no distinguished from the centralized database. Thereby, theconsortium blockchain is preferable for ridesharing services.

II. LITERATURE SURVEY

A) Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing

Carpooling enables passengers to share a vehicle to reduce traveling time, vehicle carbon emissions, and traffic congestion. However, the majority of passengers lean to find local drivers, but querying

a remote cloud server leads to an unnecessary communication overhead and an increasedresponse delay. Recently, fog computing is introduced to provide local data processing with low latency, but it also raises new security and privacy concerns because users' private information (e.g., identity and location) could be disclosed when this information are shared during carpooling [13]. While they can be encrypted before transmission, it makes user matching a challenging task and malicious users can upload false locations. Moreover, carpooling records should be kept in a distributed manner to guarantee reliable data auditability. To address these problems, we propose an efficient and privacy-preserving carpooling scheme using blockchain-assisted vehicular fog computing to supportconditional privacy, one-to-many matching, destination matching, and data auditability. Specifically, we authenticate users in a conditionally anonymous way [14]. Also, weadopt private proximity test to achieve one- to-many proximity matching and extend it to efficiently establish a secret communication key between a passenger and a driver. We store all location grids into a tree and achieveget-off location matching using a rangequery technique. A private blockchain is built to store carpooling records. Finally, we analyze the security and privacy properties ofthe proposed scheme and evaluate its performance in terms of computational costs and communication overhead.

B) Privacy-Preserving Partner Selection for Ride-Sharing Services

in this paper, we propose a privacy- preserving ride-matching scheme for selecting feasible ride-share partners in RSSs. First, we design a spatial region-based selection mechanism, which allows the Ride-Sharing server (RS-server) to prechooseriders in the matched regions with drivers, without exposing their accurate sources and destinations. Second, with the encrypteditineraries of drivers and riders, the RS- server further selects potential ride-share partners according to the travel time saving (TTS) and the feasibility of time schedules. Third, the RS server determines proper ride-share partners with the objective of maximizing the system-wide TTS. With the three-step partner selection, suitable riders can be discovered for the drivers to sharevacant seats, resulting in the saving of total travel time and expenditure for riders anddrivers. Finally, we demonstrate that the proposed scheme offers strong privacy guarantees to both riders and drivers, while maintaining the efficiency and practicality of RSSs.

C) Efficient and Privacy-preserving Dynamic Spatial Query Scheme for Ride-hailing Services

With the prosperity of mobile internet andthe pervasiveness of location-aware mobile terminals, online ride-hailing, a high-level location-based service (LBS) which relies on dynamic spatial

query, has made our life more convenient. However, the flourish of ride-hailing service still faces many severe challenges since users' location privacy and service provider's data security. In this paper,we present an efficient and privacy-preserving dynamic spatial query scheme (TRACE) for ride-hailing service. With TRACE, users (i.e., consumers and vehicles) can access ride-hailing service without divulging their sensitive location information, meanwhile, the ride-hailing server can achieve the necessary commercial operating information while keeping its sensitive data (i.e., the space division information) confidential. Specifically, with two proposed efficient and secure spatial query algorithms, named FSSQ and ESVQ, all location-related data are encrypted by its owner before being sent out, and are calculated without decryption during the spatial query process. Therefore, consumers, vehicles, and service provider cannot obtain each other's sensitive information. Detailed security analysis shows that TRACE can resist various known security threats.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

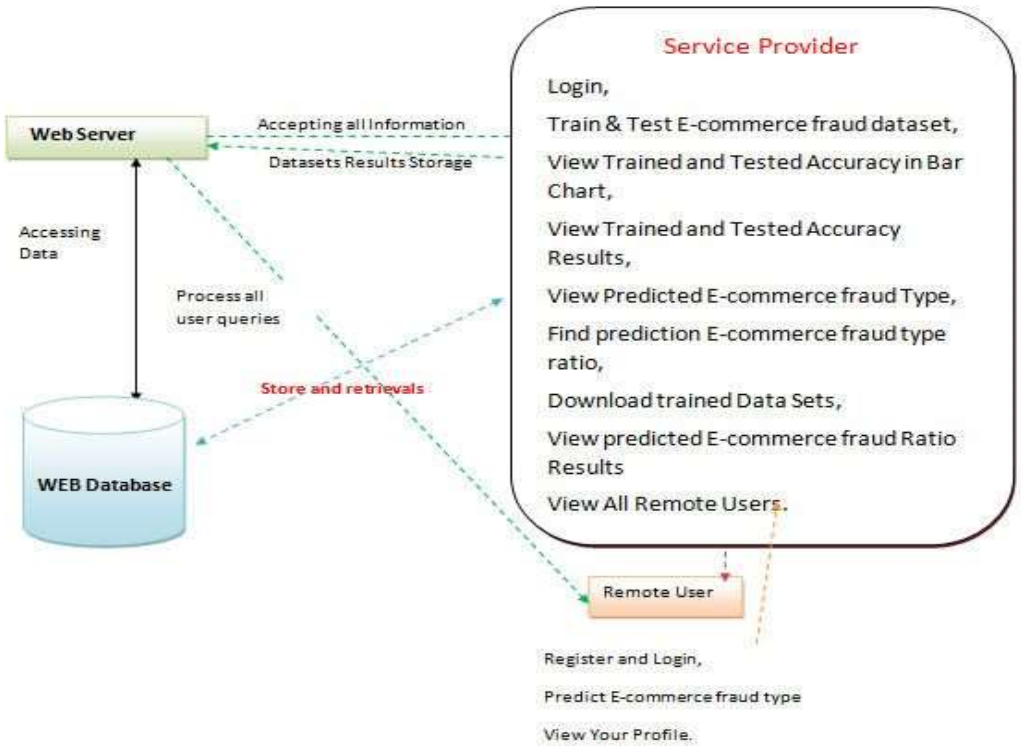

Fig. 1: System Overview

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

Implementation Modules

Passengers

To enjoy a comfortable and fast ride- sharing service, passengers use a mobile application to enter their travel data, which includes not only their place of departure, their earliest andlatest departure time, and destination, but also the latest time by which they must have arrived at their destination. The passenger defines the access structure of the travel data. The travel data and access structure are encryptedto generate the ciphertext that is sent tothe roadside unit. The roadside unit will provide the ride-sharing matching result to the passenger.

Drivers

- The commuter who provides ride-sharing services is referred to as the driver. The driver uses the mobile application to

generate their travel attributes, whichinclude their place of departure, departure time, destination and their latest time of arrival at the destination. The driverencrypts the service information to generate the ciphertext and sends it to the roadside unit. The roadside unit realizes ride-sharing matching by detecting whether the driver's travel attributes meet the access structure of the passenger's travel data. The roadside unit re-encrypts the passenger's ciphertext to generate the re-encrypted ciphertext, which is sent to the matching driver. After receiving the re-encrypted ciphertext, the driver decrypts it to obtain the passenger's itinerary

Implementation Algorithms

Support Vector Machine

- In machine learning, support-vector machines (SVMs, also support-vector networks) are supervised learning models with associated learning algorithms that analyze data for classification and regression analysis. An SVM training algorithm builds a model that assigns newexamples to one category or the other, making it a non-probabilistic binary linearclassifier.

Logistic Regression

- Logistic regression is one of the mostpopular Machine Learning algorithms, which comes under theSupervised Learning technique. It is used for predicting the categorical dependent variable using

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

a given set of independent variables.

- Logistic regression predicts the output of a categorical dependent variable. Therefore, the outcome mustbe a categorical or discrete value. It can be either Yes or No, 0 or 1, true or False, etc. but instead of giving theexact value as 0 and 1, **it gives the probabilistic values which lie between 0 and 1**.

IV. Results

Fig 2: Home Page

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

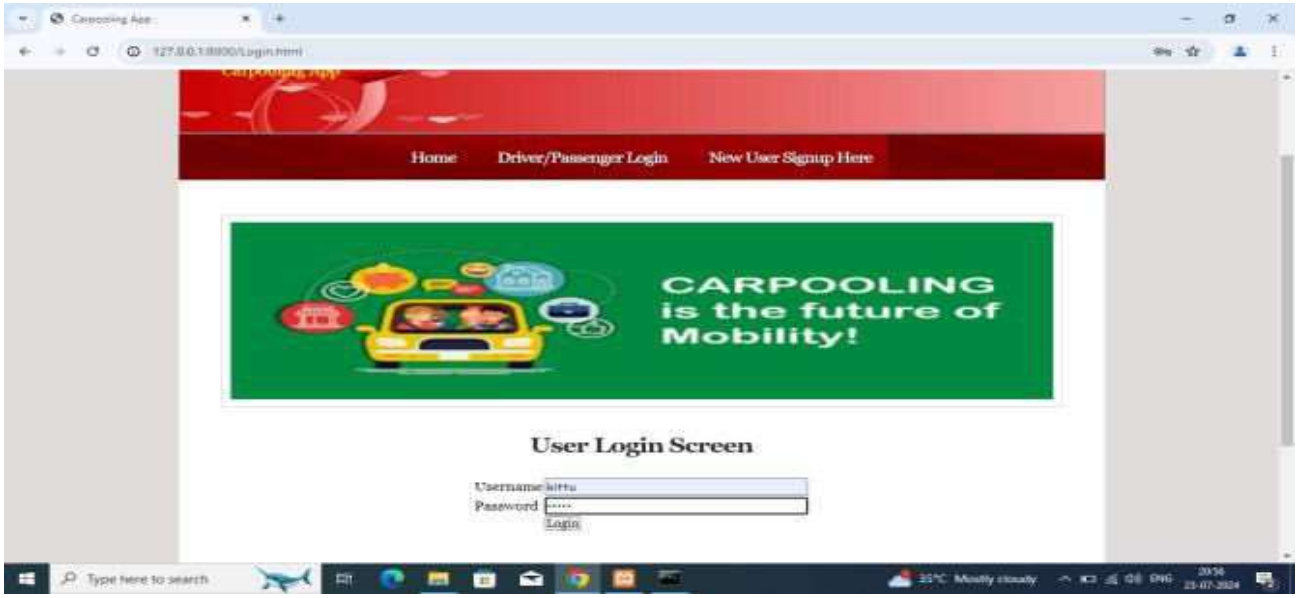

Fig. 3: User Login

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

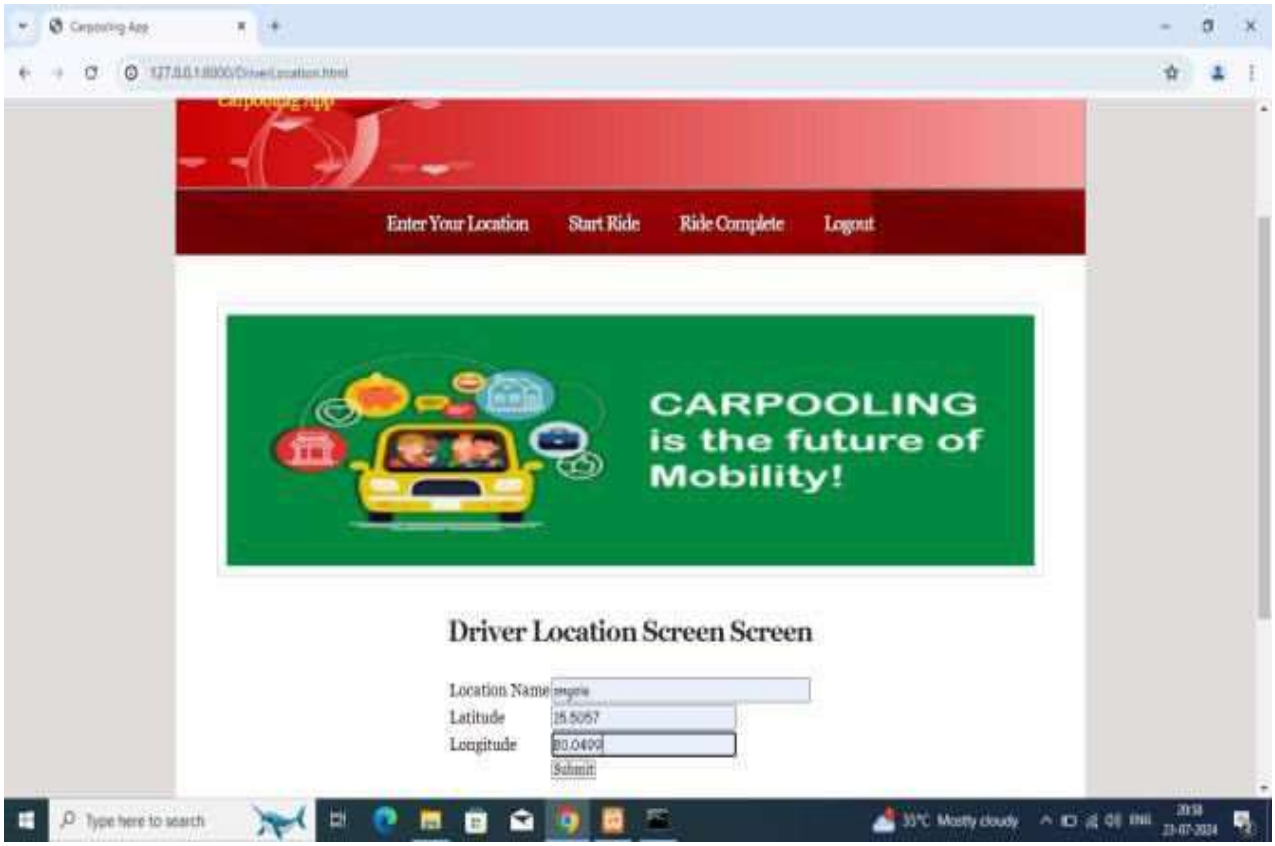

Fig. 4: Add Driver Location

Fig. 5: Add User Location

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 11, November : 2024

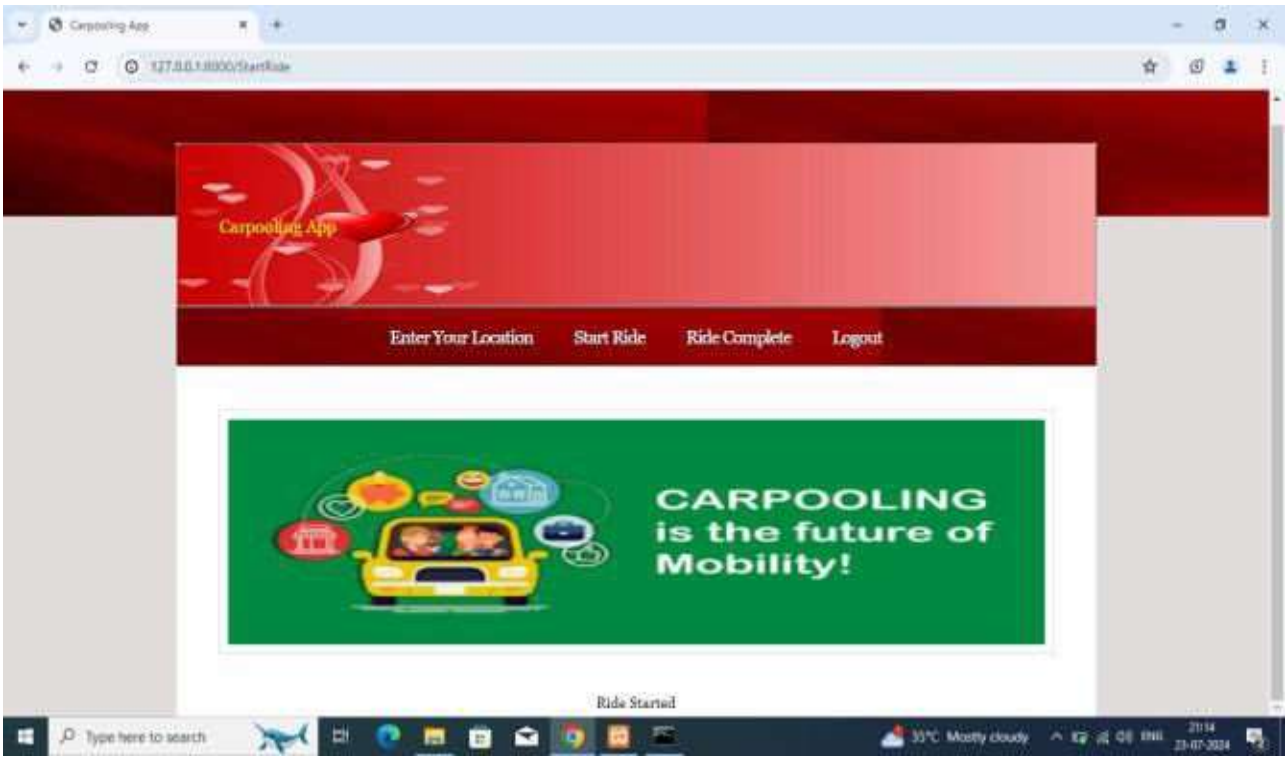

Fig. 6: Start Ride

V. CONCLUSION

In this project not only ensures the confidentiality, security and privacy of information interaction process, but alsochanges the centralized structure of existing ride-sharing systems, which prevents single point collapse and information monopoly leading to malicious abuse or illegal selling of user data. The roadside unit uses attribute-based proxy re-encryption algorithm to match the appropriate driver for the passenger based on the driver's attribute set as well as the access structure.

Attribute- based proxy re-encryption algorithm we proposed meets requirements of uni directionality, and confidentiality. It can prevent roadside unis from colluding with drivers satisfying the access structure, to avoid the leakage ofpassengers' privacy data. The improved DPoS consensus mechanism validates ride- sharing records stored in the block, which ensures data integrity and tamper resistance. The data stored on the can be used as the basis for arbitration in the event of a dispute. The credibility mechanism we designing improves the credibility of the passengers and drivers, which provides a reliable andsecure information interaction environment. Security analysis and performance evaluationindicate that our scheme is more secure and efficient

than existing schemes. Therefore,our scheme provides a certain theoretical basis and research value for ride-sharing services, which is beneficial to enhance privacy protection and data security, such that the service quality of ridesharing can beimproved.

REFERENCES

1. Y. Wang, J. B. Gu, S. Y. Wang, and J. Wang, "Understanding consumers'willingness to use ride-sharing services: The roles of perceived value and perceived risk," Transp. Res. Part C Emerg. Technol., vol. 15, pp. 504-519, Aug. 2019.
2. https://rideshareapps.com/2015-rideshare-infographic/.
3. S. Li, H. Tavafoghi, K. Poolla, and P. Varaiya, "Regulating TNCs: should Uberand Lyft set their own rules?" Transp.Res. Part B Meth., vol. 129, pp. 193-225,Nov. 2019.
4. https://techcrunch.com/2017/12/20/china s-didi-chuxing-raises-4b/.
5. Y. Guo, X. T. Li, and X. H. Zeng, "Platform Competition in the Sharing Economy: Understanding How Ride- Hailing Services Influence New CarPurchases," J. Manag. Inf. Syst., vol. 34, no. 4, pp. 1043-1070, Oct.
6. Pedro M. d'Orey and M. Ferreira, "Can ride-sharing become attractive? A case study of taxi-sharing employing a simulation modelling approach," IET Intell. Transp. Syst., vol. 9, no. 2, pp. 210-220, Feb. 2015.
7. Lakshmi K, Mahaboob B, Rajaiah M et al (2021) Ordinary least squares estimation of parameters of linear model. J Math Comput Sci 11(2):2015–2030.
8. M. Zhu, X. Y. Liu, and X. D. Wang, "An

   Online Ride-Sharing Path Planning Strategy for Public Vehicle Systems," IEEE Trans. Intell.Transp. Syst., vol. 20, no. 2, pp. 616-627, Feb. 2019.
9. J. B. Ni, K. Zhang, X. D. Lin, H. M. Yang, and X. M. Shen, "AMA: Anonymous Mutual Authentication with Traceability in Carpooling Systems," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, 2016, pp. 1-6.
10. A. B. Sherif, K. Rabieh, M. Mahmoyd, and X. H. Liang, "PrivacyPreserving Ride Sharing Scheme for AutonomousVehicles in Big Data Era," IEEE Internet Things J., vol. 4, no. 2, pp. 611-618, Apr. 2017.

11. C. Caballero-Gil, C. Caballero-Gil, J.Molina-Gil, F. Martín-Fernández, and V. Loia, "Trust-Based Cooperative Social System Applied to a Carpooling Platformfor Smartphones," Sensors (Basel), vol. 17, no. 2,pp. 245-257, Feb. 2017.

12. Leaf disease detection using ensemble classification approach in machine learning Rajaiah, M., Vijaya, C.K., Subramanyam, N., Kanth, P.K. AIP Conference Proceedings, 2024, 2802(1), 120004.

13. Penchalaiah, N. and Seshadri, R. "Effective Comparison and Evaluation of DES and Rijndael Algorithm (AES)", International Journal of Computer Science and Engineering, Vol. 02, No. 05, 2010, 1641-1645.

14. Prasath, J.S. et al. 'An Optimal Secure Defense Mechanism for DDoS Attack in IoT Network Using Feature Optimization and Intrusion Detection System'. 1 Jan. 2024 : 6517 – 6534.