International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 12 | Dec 2024 www.irjet.net p-ISSN: 2395-0072

Trip-Share with Advanced Technology

Nitesh Waykar[1], Arti Vinkar[2], Dashrath Kshirsagar[4], Prof. V M Mhalgi[4]

[1,2,3]U.G. Student, [4]Assistant Professor
Department of Computer Science and Engineering
Shree Tuljabhavani College of Engineering Tuljapur.

Abstract- *Trip-Share Connect is a modern online platform that transforms the trip-share experience, offering individuals and communities a seamless, sustainable way to share rides. The platform acts as a bridge, connecting drivers with available seats to passengers traveling along similar routes. By facilitating cost-sharing, reducing traffic congestion, and lowering carbon emissions, Ride-Share Connect promotes a more eco-friendly and efficient transportation system. Designed with simplicity in mind, the platform allows users to easily plan and coordinate their trips. Drivers and passengers can set their travel schedules, select routes, and calculate fair contributions for their shared journeys. The user-friendly interface makes it simple for everyone to navigate the platform and find suitable trip-sharing options, making the process of organizing rides both convenient and accessible. Key features of Ride-Share Connect include live tracking of rides, which allows both drivers and passengers to stay updated on their journey in real-time, ensuring transparency and security. The automated payment system adds another layer of convenience by streamlining the financial aspect of trip-share, eliminating the need for manual transactions. To further enhance trust and safety, the platform employs a comprehensive user verification process, ensuring that all participants are trustworthy and verified before engaging in the ride-sharing process. Traditional trip-share systems typically rely on centralized models, which can be vulnerable to system failures or security breaches. In contrast, Ride-Share Connect embraces a decentralized approach, which addresses these risks and strengthens the platform's overall security and resilience. This decentralized framework ensures that user data and ride-sharing activities are stored in a more secure and distributed manner, reducing the likelihood of a single point of failure and offering a more robust and dependable trip-share experience.*

1.INTRODUCTION

Trip-sharing systems have become an essential solution for addressing urban transportation challenges, including increasing traffic congestion, rising pollution levels due to vehicle emissions, and the shortage of parking spaces resulting from the growing number of privately owned cars. These systems allow individuals to access vehicles without the financial burden and responsibilities associated with owning one. Instead of having to purchase and maintain a car, people can simply use a shared fleet of vehicles on a flexible, as-needed basis. This shift away from personal vehicle ownership helps to alleviate common urban issues related to car use and promotes a more sustainable approach to transportation. As urbanization continues to expand, fuel prices rise, and awareness of environmental impacts increases, the demand for more sustainable and efficient transportation options grows. Trip-share platforms serve as a modern solution to these challenges, connecting individuals who share similar routes, enabling them to carpool, reduce travel expenses, and cut down on their carbon footprint. These platforms act as digital hubs where users can easily create profiles, browse available trips, or post their own, making it easier than ever to find matching rides and coordinate schedules.

One of the key advantages of trip-share platforms is the integration of advanced features such as real-time route matching, which ensures that users find the most efficient shared rides, as well as payment systems that streamline financial transactions. Additionally, these platforms often include safety protocols, like verified profiles and background checks, to build trust among users and ensure a secure experience.

The impact of these systems extends beyond cost savings for individuals. By promoting shared rides, trip-share platforms help reduce the overall number of cars on the road, which leads to lower traffic congestion and decreased emissions, contributing to cleaner air and a more sustainable urban environment. These platforms also foster a sense of community, as they enable individuals from diverse backgrounds to collaborate on daily commutes, strengthening social connections and building a more cooperative commuting culture. Ultimately, this shift towards shared, eco-friendly transportation plays a vital role in creating greener, more livable cities that prioritize sustainability and improved quality of life for their residents.

1.1 Trip-sharing Security Purpose

While trip-sharing systems offer solutions to transportation challenges, they are not without security concerns. In these systems, users typically lease a shared vehicle through an online application, often controlled via their smartphone. However, since information is transmitted over public networks, it is vulnerable to interception, alteration, or misuse by malicious attackers. For instance, if a digital key or access code is exposed, an attacker could gain unauthorized control over the vehicle, potentially leading to

theft. To address these risks, secure authentication protocols are essential to establish a protected communication channel. Additionally, a robust user authentication process is critical to verify that users possess the necessary credentials, such as a valid identity and driving license, ensuring they are authorized and qualified to operate the vehicle.

Traditional trip-sharing systems often rely on centralized servers to store and manage user and service data. However, this centralized architecture introduces significant vulnerabilities, such as a single point of failure. If a service server is compromised, essential records, such as vehicle usage history, could be erased or manipulated. This poses challenges in resolving disputes or holding users accountable for misconduct during trip-sharing. Moreover, the exposure of stored user data could result in severe privacy breaches, as it may contain sensitive personal information. To mitigate these risks, transitioning to a decentralized system is crucial. Such a system would enhance data security, reduce the likelihood of single points of failure, and safeguard user privacy by distributing data storage and control across multiple nodes.

2. Advance Function of Trip-Share Service

Canceling a Booking: -

1. Cancellation Options:
    - Users can access their booking history or upcoming trips section on the website.
    - From there, they can select the specific booking they wish to cancel.
2. Reasons for Cancellation:
    - The website may prompt users to choose a reason for cancellation (optional), such as a change in plans, incorrect booking, or unforeseen circumstances.
3. Cancellation Policy:
    - The system may follow a cancellation policy where users are informed about potential penalties, such as partial charges for last-minute cancellations.
    - For cancellations made well in advance, no charges might apply.
4. Seamless Process:
    - Once the user confirms the cancellation, the system updates the availability for other users who may want to book the same ride.
    - Users receive a confirmation of cancellation via email or notification, along with details about any refunds (if applicable).

3. System Services

The proposed authentication framework for a trip-sharing system is built on a blockchain structure and involves five key entities: the Trust Authority, Stations, Vehicle Owners, Vehicles, and Users. The Trust Authority is responsible for setting up the system and issuing credentials and pseudo-identities to both users and vehicle owners, acting as a trusted entity within the network.

Stations serve as data storage and computing hubs, facilitating the operation of the consortium blockchain. These stations play a critical role in managing the decentralized network, storing relevant data, and enabling communication between entities. They organize the blockchain's consensus mechanism, ensuring that all transactions are verified and recorded in a secure, transparent, and immutable manner.

Users who wish to use a shared vehicle submit a trip-sharing request to the vehicle owner through the station. The request is processed through the blockchain, allowing both the user and owner to securely exchange information, such as availability and terms of use, without the need for a centralized intermediary. Blockchain ensures that all actions taken during the trip-sharing process are authenticated, recorded, and auditable.

The vehicle owner is also a key player in this system, as they grant access to their vehicle to verified users. Vehicle data, such as location, condition, and usage history, is recorded on the blockchain, creating a transparent, tamper-proof record of each car's activity.

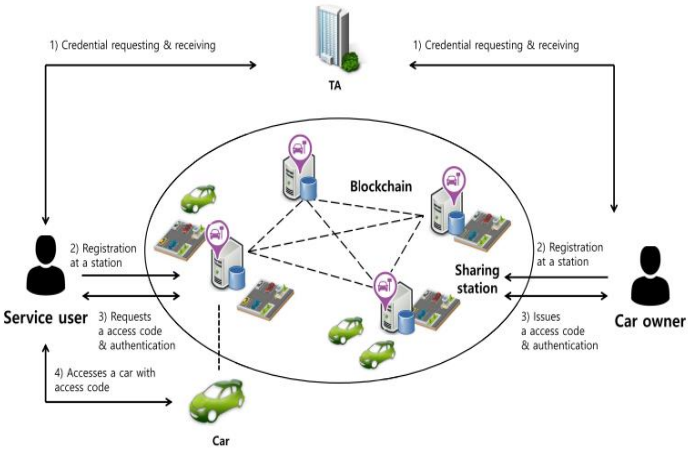

Fig 1. The proposed system service.

By leveraging blockchain technology, this authentication scheme ensures security, trust, and privacy. It addresses concerns related to data manipulation, fraud, and unauthorized access, while promoting a decentralized, efficient, and user-centric trip-sharing system. Additionally, the integration of blockchain allows for greater accountability, as every transaction and interaction between users, owners, and vehicles is permanently recorded on the distributed ledger.

3.1 Rust authority: The Trust Authority is a pivotal component in the trip-sharing system, functioning as a trusted and secure entity that oversees the operation of the platform. It is responsible for the initialization and continuous maintenance of the system's integrity. One of its key functions is to generate cryptographic keys for the stations, which are required for secure communication within the network. Additionally, the Trust Authority assigns digital credentials to both users and vehicle owners. These credentials not only authenticate users but also verify their qualifications to drive, ensuring that only authorized individuals can participate in the system.

In addition to these credentials, the Trust Authority issues pseudo-identities to users and vehicle owners. The use of pseudo-identities is crucial for protecting users' privacy, as it ensures that sensitive personal data (such as their real names) is not directly exposed within the system. This method helps to minimize the risk of identity theft or privacy breaches, while still allowing for secure verification and interactions within the platform.

To further enhance its role, the Trust Authority is designed to be a highly secure and resilient entity, built to withstand potential attacks or compromises. It is positioned to be tamper-proof and resistant to unauthorized access, which is vital for maintaining the integrity of the system as a whole.

In cases of disputes or fraudulent activities, such as when there is a case of unauthorized access or misuse of a vehicle, the Trust Authority can utilize blockchain-stored data to trace and uncover the true identity of any malicious actor. Since blockchain technology is inherently immutable and transparent, it provides a reliable source of truth, ensuring that evidence is secure and tamper-proof. The Trust Authority uses this information to hold wrongdoers accountable, maintaining the overall trust and security of the system while protecting the privacy of legitimate users.

In summary, the Trust Authority plays an essential role in ensuring the seamless, secure, and privacy-conscious operation of the trip-sharing system. Its combination of cryptographic controls, privacy protection through pseudo-identities, and its ability to resolve disputes through blockchain transparency makes it a cornerstone of the system's overall trustworthiness and security.

3.2 Stations: Station serve as the operational hub for the trip-sharing system, providing a platform that facilitates interactions between users and vehicle owners while acting as a mediator when disputes arise.

1. Credential Registration and Verification:
    - The station collects and processes the credentials of both users and vehicle owners during registration.
    - These credentials are verified for authenticity and securely recorded on the blockchain, creating a reliable and tamper-proof repository of participant information.
2. User Authentication:
    - Upon receiving a trip-sharing request from a user, the station validates the user's credentials against the records stored on the blockchain.
    - This step ensures that only authorized users can access the trip-sharing services, enhancing overall security.
3. Service Coordination:
    - After user authentication, the station communicates with the relevant vehicle owner to facilitate the service request.
    - It handles the transfer of essential information, such as access details or vehicle availability, between the owner and the user.
4. Blockchain Record Management:
    - All transactions and service-related activities, including vehicle usage and service approval, are logged by the station onto the blockchain.
    - These records provide a transparent and immutable audit trail, which can be referenced in case of disputes.
5. Dispute Resolution Support:
    - In the event of disagreements or issues, the station provides the necessary blockchain-stored data to assist the trusted authority in resolving disputes.
    - This ensures a fair and efficient arbitration process, preserving trust in the system.

3.3 User: Users are central to the trip-sharing system, utilizing mobile devices such as smartphones to interact with the platform. They start by creating a profile and providing necessary credentials, including identity verification and

proof of driving eligibility. Once registered, users can browse available vehicles and submit requests for trip-sharing services.

When a user decides to request a vehicle, they send a service request accompanied by authentication details to the station. These details verify their identity and ensure they are authorized to drive. The station validates this information by checking the blockchain, which contains securely stored user data. This process ensures that only verified individuals can proceed with the request, adding an essential layer of security to the system.

After successfully passing the authentication, the user receives a unique digital access code, delivered securely to their mobile device. This access code enables the user to unlock and operate the vehicle during the approved period. The user can then begin their journey, benefiting from the convenience and flexibility of the trip-sharing platform.

In addition, users have access to features such as real-time tracking of their journey, trip history, and automated payment systems for a hassle-free experience. Any feedback or issues during the trip can be logged through the app, ensuring continuous service improvement. By participating in the trip-sharing system, users not only enjoy cost-effective and eco-friendly transportation but also contribute to reducing traffic congestion and environmental impact in urban areas.

3.4 Owner: Vehicle owners play a crucial role in the trip-sharing system by offering their vehicles for shared use. They begin by registering their vehicles with the station, providing detailed information such as the vehicle's make, model, condition, and necessary ownership documents. This data is verified by the station and securely recorded on the blockchain to ensure transparency and prevent tampering.

Once a user requests to share a vehicle, the station notifies the owner with the request details, including the user's credentials and intended usage. The owner reviews the information and decides whether to approve the request. If approved, the owner generates a unique digital access code that enables secure entry and operation of the vehicle.

The access code is transmitted back to the station, which manages its secure distribution to the authorized user and the vehicle. This ensures that only the verified user can access the car for the specified period. Owners also have the ability to track their vehicle's status in real time through the system, ensuring peace of mind and accountability during its use.

Additionally, the blockchain maintains a complete, immutable record of all transactions and interactions related to the vehicle. This includes the sharing history, access logs, and user feedback, providing owners with comprehensive documentation that can be used for dispute resolution or future reference. This system not only optimizes vehicle utilization but also ensures that owners retain control and oversight of their assets while contributing to a sustainable transportation model.

4. CONCLUSIONS

Trip-sharing systems have gained significant attention as an effective solution to address transportation challenges in urban areas. However, traditional trip-sharing models face security vulnerabilities due to their centralized architecture and reliance on public communication channels. This paper introduces a secure, decentralized trip-sharing system model, along with an authentication scheme designed to provide a reliable and user-friendly service for authorized participants. The proposed system leverages blockchain technology to ensure the integrity of service information and enable a decentralized framework for trip-sharing. To protect user privacy, a pseudonym system is employed, replacing real identities with pseudonyms. This ensures that even if stored data is compromised, an attacker cannot discern the true identity of users.

The proposed authentication protocol was validated using BAN logic analysis, demonstrating its ability to achieve secure mutual authentication among users, stations, and vehicle owners. The protocol effectively defends against various attacks, including impersonation, stolen device misuse, offline password guessing, replay, and man-in-the-middle attacks. Additionally, the protocol ensures essential security properties such as user anonymity, data confidentiality, and mutual trust through an informal security analysis.

Performance comparisons with existing schemes show that the proposed protocol is both efficient and well-suited for integration into blockchain-based trip-sharing systems. Future work includes developing a simulation to further evaluate the protocol's effectiveness and implementing it in real-world trip-sharing platforms. This advancement promises a secure and privacy-preserving solution to modern urban transportation needs.

5. REFERENCES

[1] J. Jung and Y. Koo, ''Analyzing the effects of car sharing services on the reduction of greenhouse gas (GHG) emissions,'' Sustainability, vol. 10, no. 2, p. 539, Feb. 2018.

[2] F. Ferrero, G. Perboli, M. Rosano, and A. Vesco, ''Trip-sharing services: An annotated review,'' Sustain. Cities Soc., vol. 37, pp. 501–518, Feb. 2018.

[3] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, ''The blockchain as a decentralized security framework [future directions],'' IEEE Consum. Electron. Mag., vol. 7, no. 2, pp. 18–21, Mar. 2018.

[4] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, Dec. 2017.

[5] B. Vaidya and H. T. Mouftah, "Security for shared electric and automated mobility services in smart cities," IEEE Secure. Privacy, vol. 19, no. 1, pp. 24–33, Feb. 2021.

[6] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[7] AVISPA. SPAN, A Security Protocol Animator for AVISPA. Accessed: Mar. 2021. [Online]. Available: http://www.avispa-project.org/