iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52527

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Secure Decentralized Vehicle Sharing System Using Blockchain

Deekshith B V[1], Harsha H J[2], Hitesh B S[3], Jayanth N[4], Prof. Vanitha G P[5]
[1, 2, 3, 4]*Student,* [5]*Professor, Dept. of Computer Science Engg, SCE Bangalore-560057, India*

Abstract: ***Shared vehicles provided by car-sharing systems can help address several issues in cities, such as reducing the use of personal cars. The popularity of the Internet of Things has made it easier for people to access shared cars through simple mobile operations. However, the car-sharing system has vulnerabilities in terms of security, such as sensitive user data transmitted through public channels, which could be accessed by attackers for illegal purposes. Therefore, it's crucial to establish a secure authentication protocol. In addition, the traditional centralized car-sharing system has a single point of failure, necessitating a decentralized car-sharing scheme, which was proposed in this study using blockchain technology. This model ensures data integrity and offers a decentralized vehicle-sharing service with anonymous authentication of participating entities. The proposed car-sharing system provides mutual authentication, protects against several attacks, and was analyzed for computation and communication costs. The proposed blockchain-based decentralized car-sharing scheme has several advantages over the traditional centralized model. For example, it eliminates the need for a trusted third party. the proposed blockchain-based decentralized car-sharing scheme offers a more secure and efficient approach to car-sharing, addressing several security issues associated with traditional centralized models. It ensures data integrity and provides mutual authentication while offering anonymity to participating entities, making it a promising solution for car-sharing systems in smart cities. to maintain the integrity of the system, as blockchain technology is based on a distributed ledger that allows participants to validate transactions. Additionally, the anonymity of the participating entities ensures privacy while providing security against unauthorized access to sensitive data. Moreover, the proposed scheme's security was analyzed using several methods, such as informal analysis, AVISPA simulation, and BAN logic evaluation, to ensure the system's resilience to various attacks.***

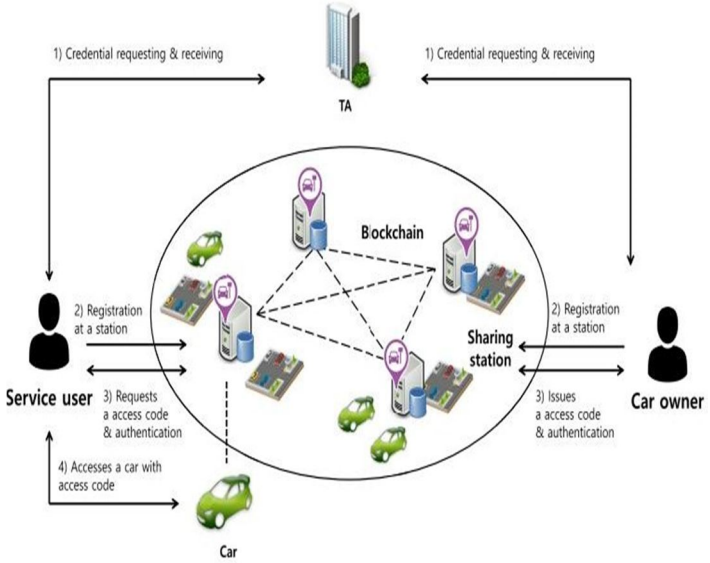


Figure1. System Architecture vehicle sharing system

I. INTRODUCTION

Vehicle sharing was introduced a long time ago but it has gained attention and popularity in recent times or maybe in the past few decades.To address transportation problems in urban areas such as traffic congestion, pollution from combustion engines, and limited parking due to the increase in cars, car-sharing systems have been introduced. These systems allow users to access a fleet of shared vehicles without the cost and responsibility of ownership, reducing private car ownership.

The car-sharing market has grown significantly and is expected to continue to expand.

However, the traditional car-sharing system suffers from security issues, particularly in a centralized structure where user information and service records are stored.

A centralized server can be vulnerable to attacks from malicious attackers, leading to data loss, tampering, and privacy breaches.

To overcome these problems, two types of car-sharing service models have emerged: business-to-customer (B2C) and peer- to-peer (P2P). B2C companies offer shared cars that can be rented by users, while P2P models allow car owners to rent out their private vehicles to other users on a short-term basis. In both models, a service provider acts as an intermediary, providing an online platform and customer support to make the exchange possible.

Users can book and rent a shared car through an online service platform using their smartphones. However, because the information is transmitted in a public channel, it is vulnerable to eavesdropping, forgery, deletion, and modification by malicious attackers. Therefore, secure authentication is essential to provide a secure communication channel, and user authentication is necessary to verify that the user has the right and ability to drive a vehicle.

To overcome the security issues inherent in centralized structures, it is essential to decentralize the system and distribute the information among users in a peer-to-peer network. In this system, available cars are spread throughout the city in reserved parking spots, making it easy for users to find them and book their ride.

.

A. Problem Statement

In a conventional car-sharing system, the centralized service server stores and manages the user's information and service details. However, this structure has a vulnerability to single- point failures by malicious attackers. If the service server is hacked and all sharing records are erased, users will lose access to the previously utilized car information if there is a missing item on the car. Moreover, if sharing records are altered or edited when users conduct fraudulent activities during car- sharing, obtaining user evidence becomes difficult. Additionally, if the saved data is leaked, it poses severe privacy concerns since it relates to user privacy. Therefore, addressing the issues caused by a centralized structure is crucial.

B. Objectives

To develop a Decentralize vehicle-sharing system which includes:

1) The goal is to create a decentralized vehicle sharing system that operates using blockchain technology. In this system, vehicle-sharing stations replace a single service provider and maintain the blockchain by acting as nodes.

2) To ensure security, this paper proposes a secure authentication scheme that can withstand various attacks, including impersonation and replay attacks.

3) The Burrows-Abadi-Needham (BAN) logic analysis is used to determine if the proposed scheme offers secure mutual authentication. The automated validation of internet security protocols and applications (AVISPA) is utilized to analyze man-in-the-middle (MITM) and replay attacks.

4) A performance analysis was conducted, comparing the proposed authentication scheme with similar ones, demonstrating that it can be successfully implemented in a blockchain-based vehicle-sharing system.

II. LITERATURE SURVEY

In modern world, ride or vehicle sharing is becoming a popular and effective of reducing the traffic and make the transportation effective and reliable. The rise of digital technologies and cryptocurrencies over the beyond decade has brought big modifications in lots of enterprise sectors. The proposed decentralized ridesharing system is built on the Ethereum blockchain network. With most of the contemporary ridesharing methods being controlled via crucial authorities and huge groups, there is a need for a decentralized device in public area to ensure that ridesharing device will become smoother. this paper are to [1] shows how can vehicle sharing system can reduce the traffic to an extent in any city and potentially decrease the number of cars up to 32% and it can be more in some of the developed cities and one of the important aspects is the effective matching of riders to share rides and finding drivers for those riders and make it reliable and cost effective

[2] with the rise of the blockchain technology and the number of users using the internet and the mobile device is significantly increasing and the efforts of including or incorporate the technology in the transport sector .This article is formulated to passenger The matching problem in a mobility sharing system has been viewed as a monopartite matching problem, and the balance between this matching model and the one that emerges from other systems has been analyzed from efficiency based matching technology or methods.

[3] it shows a matching algorithm for the dynamic vehicle sharing based on the network partitioning which is presented in this article or the paper. The main aim of this approach is to minimize the number of kilometers or the mileage driven by the service provider while keeping the account of inconvenience caused by picking the passengers from their current place and dropping them to their desired location and this current problem should be addressed in a given scale requires the space in which the algorithm searchers and matches. This is achieved by partitioning the road network into district regions which represent certain sub- structures of the road network. [4] in automated or the In a dynamic ride-sharing system, the drivers or riders may not always agree to the matches suggested by the ride-share provider. This makes it essential to consider the reliability and stability of the matches being made and the service provided by the provider. By adopting this approach, various methods can be employed to generate stable or nearly stable ride-sharing solutions for customers.

Failure to consider stability when making matches may result in relatively unstable solutions to the problem. However, we have demonstrated that enforcing complete stability requires only a small price in terms of reduced system vehicle mileage savings. This can result in more sustainable ride-share systems in the long run. [5] a new way of decentralized solution for vehicle communication. It incorporates three primary layers to explore the possibility of using blockchain for communication in the IOV. A prototype of the smart contract on the testnet of Ethereum have been deployed. The proposed solution considers several properties of the solution, including the integrity, availability and the security to test whether the Blockchain is an efficient and secure mechanism for IoV communications. The results showed that this decentralized system can be considered as the real time solution and application for the main challenges of vehicle to X communications such as centralization, security and the lack of privacy. [6] have developed Traffic-Chain and a secure and privacy preserved decentralized traffic information collection service or the system. And, we have implemented a two layer blockchain architecture for efficient communication and block updating in TrafficChain. Besides, a privacy-preserving scheme has been devised to protect users' identities and driving routes. Moreover, we have considered two critical kinds of attacks, i.e., Byzantine and Sybil attacks, in TrafficChain, and developed deep learning based schemes to defend against them.[7] a car sharing domain within a blockchain-based ecosystem incorporating governmental authorities such as a transport authority Kraftfahrt-Bundesamt/KBA and automobile industry partners was chosen. In order to enforce the privacy requirements, the cryptographic techniques based on anonymous credentials and zero-knowledge proofs were used. The proof-of-concepts are implemented leveraging two technologies, namely Ethereum with ZoKrates and Hyperledger Indy. The first solution based on ZoKrates uses zkSnarks for zero-knowledge proof generation and Ethereum blockchain for proof verification. [8] we proposed a decentralized ride sharing organization scheme based on the revolutionary public blockchain. The scheme is decentralized since all interactions made by drivers/riders are done through the blockchain, and the system does not need any of organization or any centralized company to operate or to manage it. Moreover, there is no need to reveal any private information such a email address, phone number or credit card number. Using cloaked technique, only selected driver/rider know the exact pick-up location without revealing any sensitive information to the public. [9] presents a novel or an article on privacy preserving identity verification system, with the extending zero knowledge proof on top of blockchain for use in vehicle sharing applications. In this proposed scheme or system enables the secure verification without the This paragraph discusses a prototype system that addresses the issue of exchanging sensitive information between unauthorized parties.

The system was evaluated under various conditions to determine its performance and feasibility. The results indicate that the system based on the Hyperledger fabric blockchain network can process a high number of transactions with minimal delay. Additionally, the ZKP module enables quick identity verification, making the system suitable for real-world vehicle sharing applications. A related study [10] examines the concept of fair cost-sharing in decentralized ride-sharing systems. The study explores different cost-sharing mechanisms, such as equal, egalitarian, proportional, and segment-based mechanisms, and evaluates the stable matching outcomes associated with each mechanism. [11] To implement this project they have used a library which is capable of WS protocol communication in .NET came down to a library called SignalR. SignalR is an open-source library for ASP.NET which is capable of supporting real-time web functionality to .NET applications, adding the ability for server-side code to push content to the connected clients as it happens, in real time. SingleR is also capable of supporting of .Net, JavaScript and other programming languages. For database they have used Redise which stores data in the form of key-value pair and MongoDB which stores the data in the form of index used to store the current data location of the user. In user interface they have used Html5 and css3 for website and for mobile interface they have used jQuery. [12] Vehicle sharing represents an important transportation scheme which may contribute an important link in the growth and economic development of tier1, tier2 cites. One-way vehicle sharing systems provides a flexible rental model in which customers are allowed to take a vehicle at any station and return it to any other place or station which best suits typical urban journey requirements. So by this system we can reduce increasing number of vehicles.

However, the so- called demand-offer asymmetric problem that is the unbalanced offer and demand of vehicles typically experienced in one-new way sharing systems severely affects their economic viability as it implies that considerable human and financial resources will be engaged in relocating vehicles to satisfy customer demand. [13] A reactive optimal method and scalable real-time performance has been introduced for assigning customer requests to a fleet of vehicles of changing capacity, which quantifies experimentally the tradeoff between fleet size, capacity, waiting time, travel time, and operational charges for low- and medium-capacity vehicles such as taxis in a large-scale city dataset. Assuming one person per ride, it has been shown that only 4,000 taxis of capacity four could serve 98% of the taxi rides presently served by over 11,000 taxis. For ride-sharing, a vehicle capacity of two is sufficient when a small trip delay of 2 min is imposed. Higher-capacity vehicles are found to increase the service rate, reduce the delay time, and reduce the distance traveled by every vehicle if a maximum delay of 5 min or more is allowed, which is comparable to the time spent retrieving a car from parking. Analysis shows that the parameters of a car-pooling service such as vehicle capacity and size depend on the quality of services requirements and demand, and that it can provide a substantial improvement in city transportation systems. [14] Their main objective was to develop a decentralized application for peer-to-peer car sharing. They addressed issues that centralized car-sharing services encountered, such as denial of service and data tampering, by using blockchain technology that is decentralized and immutable. Their approach enhances the security of the entire system by employing blockchain and two different types of security systems. For example, blockchain technology makes it challenging for a hacker to hijack a car since they would only have a digital key to control the vehicle's systems. The digital key is distributed across the internet and can only be accessed with the owner's permission, making it more difficult to hack compared to a single server. Tokenizing car keys can cover many use cases related to car-sharing services, including preventing partial deadlock of cars. Their decentralized application currently includes major activities such as creating the car token, issuing a major unlock token, and offering tokenized renting solutions. Tests indicate that making a car available for rental is a simple process. Additionally, users can rent a car in an average of 12.146 seconds, providing a user experience that is comparable to using centralized car-sharing services. [15] Their proposal is for an authentication scheme based on a semi-trusted authority in VANETs was found to be effective. The system involves combining a self-healing key distribution method with a certificateless signature in a semi- trusted authority framework, which eliminates the need for receivers to request CRLs. As a result, vehicles do not have to store CRLs, saving storage space and communication resources. Additionally, this approach reduces computational costs and improves message authentication efficiency. Since the proposed scheme is based on a semi-trusted authority, it is a superior approach. [16] it is motivated by the enhanced interest in shared mobility, this research work checks how blockchain and IOT technologies can get the advancement of shared mobility, specifically for car-sharing and leasing. This research produced a conceptual design and architecture for blockchain-IOT-based car-sharing platform based on key design principles. Study tells that blockchain, as one possible technology, can advance car-sharing by facilitating intercompany collaboration between several stakeholders within car sharing and leasing and eliminating the need for trust to some extent. The design of the underlying blockchain- based platform depends on the five design principles, namely security and privacy, authenticity, traceability and reliability, scalability, and interoperability. [17] A reservation scheme has been proposed for station-based two-way car-sharing systems that leverages the temporal flexibility of drivers. By combining reservations with flexibility, the scheme can benefit both the car-sharing owner and the drivers by improving the management of reservation information. Presently, car-sharing systems do not prioritize reservations, meaning the first person to reserve a vehicle gets to use it until no vehicles are available at a given station during a specific period. To ensure customer satisfaction and vehicle availability, car-sharing operators may need to maintain an oversized fleet at multiple stations, which can be costly. [18] An algorithm has been developed to address the use of autonomous vehicles in exchange terminals, with the ability to adjust dimensions and geometric designs. The algorithm proposed six different geometric designs, which were modeled using simulation software and the NIC algorithm was employed. The system simulated a real-world scenario of an interchange with a slightly modified geometric design to provide smoother entry to the interchange terminal. To evaluate the system's performance, several assumptions were made, and the six designs were tested against five different traffic demands.

The interchange throughput and delay were found to be impacted by different volume ratios. The best performing design for the highest throughput and lowest delay varied depending on the volume ratio. For instance, when the turning ratio was 30% and through ratio was 70%, the TO design provided the best performance, while the WTOS and WTTS designs had the lowest performance. When the turning ratio and through ratio were equal, the TTOS design demonstrated improved performance, while the WTOS and WTTS designs had the lowest performance. Finally, for the high turning volume of 70% and through volume of 30%, the TTTS design provided better performance, while the WTOS and WTTS designs had the lowest performance. eliminating the need for trust to some extent.

The design of underlying blockchain- based platform depends on the five design principles, namely security and privacy, authenticity, traceability and reliability, scalability, and interoperability.

III. METHODOLOGY

A. Blockchain

Blockchain is a type of distributed ledger that provides benefits such as decentralization, integrity, and resistance to tampering. There are three main categories of blockchains: public (also known as permissionless), consortium, and private (also known as permissioned) blockchains. Public blockchains allow each node to maintain a ledger, participate in consensus, and read and write data, but this can lead to slow consensus and high maintenance costs. Additionally, any node can join or leave the network without authorization, making it unsuitable for a car- sharing system where user privacy is crucial. In contrast, consortium and private blockchains only allow approved nodes to access the ledger, with private blockchains being controlled by approved organizations and having centralized properties. Consortium blockchains offer efficient consensus time and maintenance costs while operating under approved groups. Therefore, we proposed a car-sharing scheme using a consortium blockchain.

B. Elliptic Curve Cryptosystem (ECC)

Elliptic Curve Cryptography (ECC) is a widely used public key cryptosystem that is based on elliptic curves. It is favored for cryptographic protocols because it provides the same level of security as other encryption methods, but with shorter key lengths. In ECC, an elliptic curve is defined as Ep(r, s): y2 = x 3 + ax2 + b over a prime finite field Zq, where q is a large prime, and (r, s) ∈ Zq, and 4a 3 + 27b 26= 0 (mod s). A point R is located on Ep(r, s). The security of ECC is based on two uncontrollable problems:

1) *Elliptic Curve Discrete Logarithm Problem:* Given two points R and S, where Q = x · R, it is difficult to find x ∈ Zq in polynomial time.
2) *Elliptic Curve Decisional Diffie-Hellman Problem:* Given three points Q, R, and P, where Q = x · R and N = y · R, it is difficult to find (x · y)·R in polynomial time.

C. Adversary Model

The Dolev-Yao (DY) attack model is used to determine the capabilities of an adversary. This model is widely accepted as a standard in evaluating protocol security. The adversary is assumed to have the following abilities:

1) Intercept, modify, forge, or delete messages that are transmitted over a public channel.
2) Guess either the user identity or the password, but not both simultaneously.
3) Steal a mobile device belonging to an authorized user and perform a power analysis attack to obtain stored values.
4) Carry out various attacks, including impersonation, replay attacks, and man-in-the-middle attacks.

IV. SYSTEM MODEL

The authentication scheme suggested for a car-sharing system was designed around a blockchain network comprising five entities, including Trust Authority, Station, Owners, Vehicles, and Users. Trust Authority is responsible for creating the system and issuing credentials and pseudo identities to users and vehicle owners. Stations have data storage and processing functions and are responsible for organizing consortium blockchains. Users submit car-sharing requests through stations to owners, and after authentication, receive an access code to unlock and operate the vehicle.

1) *Trust authority:* The trust authority plays a crucial role in establishing the car-sharing system by generating station keys and providing users and vehicle owners with credentials and pseudo-identities. It is important to note that trust authorities are not easily identifiable and may be deemed untrustworthy. In car-sharing systems, real identities are often replaced with pseudo-IDs while IDs are used to validate authorized drivers. In case of any disputes, the trust authority can use the data stored on the blockchain to identify the culprit..
2) *Stations:* The station functions as a mediator and provides locations and platforms for car-sharing services to users and vehicle owners. It receives and registers user and owner access data in the car-sharing system, then validates the credentials and stores the information securely on the blockchain. When a user requests car-sharing services, the station authenticates the user by using the information stored on the blockchain. The station sends the car-sharing service information received from vehicle owners to users. All information regarding provided services is securely stored on the blockchain, making it a reliable source for dispute resolution by trusted entities.

3) *User:* Car sharing services are accessible to users through mobile devices like smartphones. To demonstrate their authorized driving status, users send a request and authentication message to the station. Stations authenticate the user by referring to the information saved on the blockchain. After successful authentication and receiving the vehicle access code, the user can control the car via their mobile device.
4) *Owner:* Owners can make their vehicles available for sharing by registering the relevant vehicle information with the station. Once a user submits a request for sharing a vehicle through the station, the owner generates an access code, which is then sent to the station for distribution to the user and the vehicle.
5) *Vehicles:* Authorized users can find shared vehicles parked at stations, equipped with a communication module and an anti-tampering module. Upon receiving the access code through the communication module, the vehicle verifies the user's authorization to access it. The vehicle's parameters are all kept confidential in a tamper-proof module.

The communication flows on the proposed car-sharing system are depicted as follows:

a) The user and owner submit their actual ID and license to the Trust Authority (TA) to obtain pseudo-IDs and credentials for registering with the car-sharing system.
b) Users and owners register their pseudo-IDs, public keys, and shared vehicle information at the stations to use the car-sharing services.
c) A user uses their mobile device to request access to a shared car from a station. The station verifies the user's identity and informs the owner of the request. The owner then generates an access code for the shared car and sends it to the user and the car through the station.
d) The user uses their saved access code on their mobile device to access the shared car.

V. CONCLUSION

Car-sharing systems have become popular in urban areas as a solution to transportation issues. However, the centralized structure of traditional vehicle-sharing systems and communication through public channels create security concerns. To address these issues, this study proposes a secure decentralized car-sharing model and authentication scheme that uses blockchain to ensure data integrity and provide a decentralized service. A pseudonym for users is also implemented to protect their privacy. The proposed protocol offers secure mutual authentication between users, stations, and owners, and is secure against various types of attacks, including replay and man-in-the-middle attacks. The protocol provides anonymity, confidentiality, and mutual authentication, and has been subjected to informal security analysis.

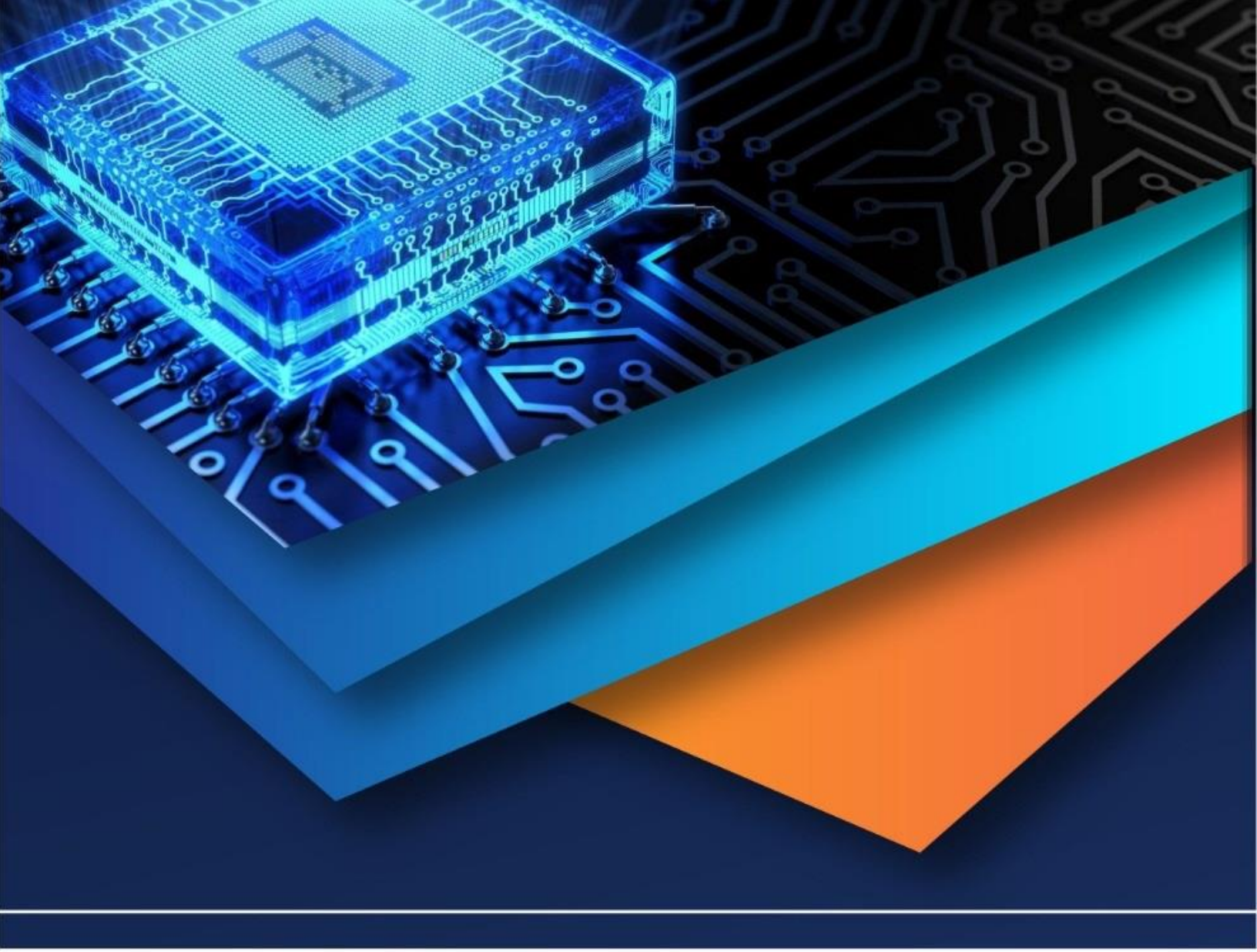
The proposed protocol is efficient and can be implemented in a blockchain-based car- sharing system. Future work includes simulation development and application of the protocol to a real vehicle-sharing system. In conclusion, the proposed decentralized car-sharing system with a secure authentication scheme provides an innovative solution to the security and privacy concerns associated with traditional vehicle-sharing systems. By utilizing blockchain technology and pseudonyms for user privacy, the proposed protocol ensures the integrity and confidentiality of shared data.

The BAN logic analysis and AVISPA simulation demonstrate the protocol's effectiveness against common security threats, making it a reliable and secure option for decentralized car- sharing services. With further development and testing, the proposed protocol could be implemented in real-world car- sharing systems, offering a more efficient and secure alternative to traditional centralized systems.

REFERENCES

[1] Cici, B., Markopoulou, A., Frias-Martinez, E., &Laoutaris, N. (2014, September). Assessing the potential of ridesharing using mobile and social data: a tale of four cities. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 201-211).
[2] H. Zhang and J. Zhao, “Mobility sharing as a preference matching problem,” IEEE Trans. Intell. Transp. Syst., vol. 20, no. 7, pp. 2584–2592, Jul. 2019.
[3] D. Pelzer, J. Xiao, D. Zehe, M. H. Lees, A. C. Knoll, and H. Aydt, “A partition-based match making algorithm for dynamic ridesharing,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 5, pp. 2587–2598, Oct. 2015.
[4] X. Wang, N. Agatz, and A. Erera, “Stable matching for dynamic ride-sharing systems,” Transp. Sci., vol. 52, pp. 739– 1034, Aug. 2017.
[5] Jabbar, R., Kharbeche, M., Al-Khalifa, K., Krichen, M., & Barkaoui, K. (2020). Blockchain for the internet of vehicles: A decentralized IoT solution for vehicle communication using ethereum. Sensors, 20(14), 3928.
[6] Wang, Q., Ji, T., Guo, Y., Yu, L., Chen, X., & Li, P. (2020). TrafficChain: A blockchain-based secure and privacypreserving traffic map. IEEE Access, 8, 60598-60612.
[7] Gudymenko, I., Khalid, A., Siddiqui, H., Idrees, M., Clauß, S., Luckow, A., ... & Miehle, D. (2020, August). Privacypreserving blockchain-based systems for car sharing leveraging zero-knowledge protocols. In 2020 IEEE international conference on decentralized applications and infrastructures (DAPPS) (pp. 114-119). IEEE.

[8] Baza, M., Mahmoud, M., Srivastava, G., Alasmary, W., & Younis, M. (2020, May). A light blockchain-powered privacy- preserving organization scheme for ride sharing services. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020- Spring) (pp. 1-6). IEEE.
[9] Li, W., Meese, C., Guo, H., & Nejad, M. (2020, December). Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof. In 2020 3rd International Conference on Hot InformationCentric Networking (HotICN) (pp. 18-24). IEEE.
[10] Chau, S. C. K., Shen, S., & Zhou, Y. (2020). Decentralized ride-sharing and vehicle-pooling based on fair costsharing mechanisms. IEEE Transactions on Intelligent Transportation Systems.
[11] Dejan Dimitrijevic., & Nemanja Nedic., & Vladmir Dimitrieski. (September 2013) Real Real-Time Carpooling and Ride-Sharing: Position paper on Design Concepts, Distribution and Cloud Computing Strategies. pp. 801–80
[12] Damianos Gavalas., & Charalampos Konstantopoulos., & Grammati Pantziou..Design and Management of Vehicle Sh aring Systems: A Survey of Algorithmic Approach (July 2017)
[13] Javier Alonso-Moraa., & Samitha Samaranayakeb., & Alex Wallara., & Emilio Frazzolic., & Daniela Rusa.. On- demand high-capacity ride-sharing via dynamic trip-vehicle assignment (November 2022). MA 02139.
[14] Viktor Valaštín, Kristián Košt'ál, Rastislav Bencel, Ivan Kotuliak. Blockchain Based Car Sharing Platform (September 2019).
[15] Jie Cui , Di Wu, Jing Zhang, Yan Xu, and Hong Zhong (March 2019). An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs.
[16] Sophia Auer, Sophia Nagler, Somnath Mazumdar, Raghava Rao Mukkamala (January 2022) Towards blockchain- IoT based shared mobility: Car-sharing and leasing as a case study.
[17] Mireia Roca-Riu and Monica Menendez (October 2019). The Potential of Flexible Reservations in a Car Sharing System With an Auction Scheme. IEEE.
[18] Majeed Algomaiah And Zhixia Li (July 2019). Next- Generation Interchange Control Based on Centralized Management of Connected and Autonomous Vehicles. IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY