IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

Blockchain Based Secure Communication in IOT Vehicular Network

Rohit Badhai, Omkar Chavan,Ajay Katare, Bhushan Hon, Prof. Jyoti Pawar

Department of Information Technology, Sinhgad College of Engineering, Pune, India

ABSTRACT-Researchers are focusing on edge computing as a means to improve the efficiency and dependability of information applications inside a vehicle-to-vehicle (V2V) communication network. In recent studies, cloud computing has been employed to execute tasks connected to messages, which has improved response times. We offer Quality of Service (QoS) conscious Internet of Things-based vehicular networks with software-defined fault tolerance. Delay in V2V communication may be mitigated, message failure can be tolerated, and safe service provisioning can be achieved via the use of Edge Computing protected by Blockchain. The interplay between blockchain and edge computing is fascinating. An infrastructure for block chain nodes to store and validate transactions may be provided via edge computing/a distributed compute architecture. However, blockchain technology may make it possible for a fully decentralised cloud marketplace to exist. The fault tolerance algorithm will attempt to resend the failed message if delivery fails. The outcome demonstrates the efficacy of the suggested approach, which makes use of the edge server SDN controller to reduce the total message transmission latency of routine and emergency messages by 55%. The suggested approach makes use of the edge server, cloud server, and blockchain infrastructure to cut down on execution time, security risk, and message failure ratio.

KEYWORDS-Vehicular computing, autonomous vehicles, edge computing, task partitioning

I. INTRODUCTION

There's a fascinating dependency structure between blockchain and edge computing. Blockchain nodes may use the infrastructure provided by edge computing/a distributed compute architecture to store and validate transactions. However, blockchain technology may make it possible for a fully decentralized cloud marketplace to exist. With the goal of increasing openness and trustworthiness in the administration of IVEC's assets, we propose a blockchain-based distributed architecture that gives edge users (such cars) the ability to verify computations. We also suggest a safe paradigm for federated IVECs to use in order to equalize load distribution.A blockchain-based method has been used to lessen security concerns. Many companies have migrated to the IoT because of the security, adaptability, and other benefits that the system provides. In this Project, blockchain is utilized to validate and verify a distant edge server before providing security services to an IoT base network. In terms of both safety and power consumption, blockchain is a very effective method. When it comes to commercial transactions, the blockchain has the lowest latency time, the lowest energy consumption, and the highest dependability. The blockchain's purpose is to ensure that all users' data is protected and may be used in whatever way they choose. A blockchain-based method has been used to lessen security concerns. Many companies have migrated to the IoT because of the security, adaptability, and other benefits that the system provides. In this Project, blockchain is utilized to validate and verify a distant edge server before providing security services to an IoT base network. In terms of both safety and power consumption, blockchain is a very effective method.This project provides solutions on how to optimize this blockchain system by using a wide range of artificially intelligent algorithms.

II. LITERATURE SURVEY

1. N. Z. AITZHAN AND D. SVETINOVIC, 2019

In this research, we looked at how to provide secure transactions while exchanging SG energy in a distributed environment without a central authority. Tokens are used in our private, decentralised energy trading system, which allows users to safely and secretly trade energy with one another. Certain degrees of privacy and security were achieved through the use of blockchain technology, multiple signatures, and anonymous encrypted message propagation streams. To ensure that transactions are safe in the event of a node failure, our system employs a peer-to-peer community based data replication approach. Also, similar to Bitcoin, the system is resilient to Byzantine failures and resistant to double-

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

spending attacks, both of which are crucial to any decentralised electronic payment network. We developed case situations in which peers in an SG engage in energy trading. We investigated and rated the system's security and performance. We ran attack simulations on the system to prove that it is safe against well-known threats, does not expose users' financial profiles to third parties, and does not divulge trade parties' names. We spoke about possible threats and gathered information on what kind of protections should be in place. In conclusion, we discovered that decentralised SG energy trading with increased privacy and security over the conventional centralised trading solutions is possible and reliable with the right mix of blockchain technology, multi-signatures, and anonymous encrypted message propagation streams.

2. P. FRAGA-LAMAS AND T. M. FERNANDEZ-CARAMES,2019

Accelerating technology upheavals in an Internet-enabled global economy, the difficulties of future mobility, and fiercer commercial competitiveness all contribute to the shift towards a society based on data and value. The adoption of blockchain technology may provide the automobile sector a platform for the distribution of reliable and cyber-resilient information, which challenges the present non-collaborative organisational structures in an increasingly complex environment. Despite the hype reported by many organisations, it is important to conduct an objective evaluation of blockchain from the perspectives of business management and cybersecurity before deciding whether or not to invest. This post addressed several of the concerns raised by the introduction of a potentially game-changing technology like blockchain. Furthermore, we review the primary scenarios and the optimisation strategies for designing and deploying these applications, presenting a holistic approach to a blockchain-based advanced automotive industry. Some suggestions were also made to help future researchers and managers address the remaining challenges before the next generation of secure blockchain applications can be deployed.

3. J. LIU AND Z. LIU, 2019.

Smart contracts, one of the most talked-about aspects of blockchain systems, have also brought to light a number of issues. There are three main contributions from our survey. We begin with a comprehensive literature review on the topic of blockchain smart contract security verification, narrowing the field down to 53 studies. In order to demonstrate the current state of the art in this field, we zeroed in on two specific facets: security assurance (20 articles) and correctness verification (33 papers).Second, we provide a classification scheme for this area of study. Environment security, vulnerability scanning, and performance effects are the subcategories into which the security assurance factors fall. While there are two types of correctness verification (programming correctness and formal verification), both are important. We weigh the benefits and drawbacks of each classification.Third, we summarise the research state and suggest up future research paths in smart contract security and correctness by in-depth study of the associated works. Here are the key points:

1) The rising trend of articles on relevant topics suggests that researchers are becoming more concerned with the safety and accuracy of smart contracts. More thorough approaches are needed immediately to guarantee the safety and accuracy of smart contracts and cut down on losses.
2) Vulnerability scanning techniques are being utilised now, with great success, to ensure the safety of smart contracts. Research in this area may be expanded in the future. Some of these include the identification of previously unrecognised vulnerabilities (by speculating on whether other vulnerabilities exist that share the same or similar design principles as those already known) and the optimisation of vulnerability detection methodology to prevent duplicative efforts and oversights.
3) More attention is being paid to the accuracy of smart contract code at the moment. Future research areas include developing consensus on smart contract programming standards, creating a framework for developing smart contracts, and raising developer knowledge of security issues.
4) While there are more papers discussing the importance of correct programming, the upward trend of formal verification is more noticeable. The formal verification approach is more exact since it uses a mathematical model. Therefore, the trend of future study will be to use formal verification method to verify smart contracts. Research in the future can focus on improving formal verification tools, integrating them with vulnerability analysis tools, and developing methods to visualise the execution of contracts using formal modelling tools like coloured Petri nets.

4. SABUR BAIDYA, YU-JEN KU, HENGYU ZHAO, 2020

In this work, we provide a future outlook on the computing requirements and design concerns for the developing smart car. Optimal allocation of existing computing resources for emerging vehicular applications, modelling vehicular application performance for different capabilities and computing architectures, and tools to aid in the development of optimal in-vehicle computing architectures and collaborative computing systems with edge computing nodes have all

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

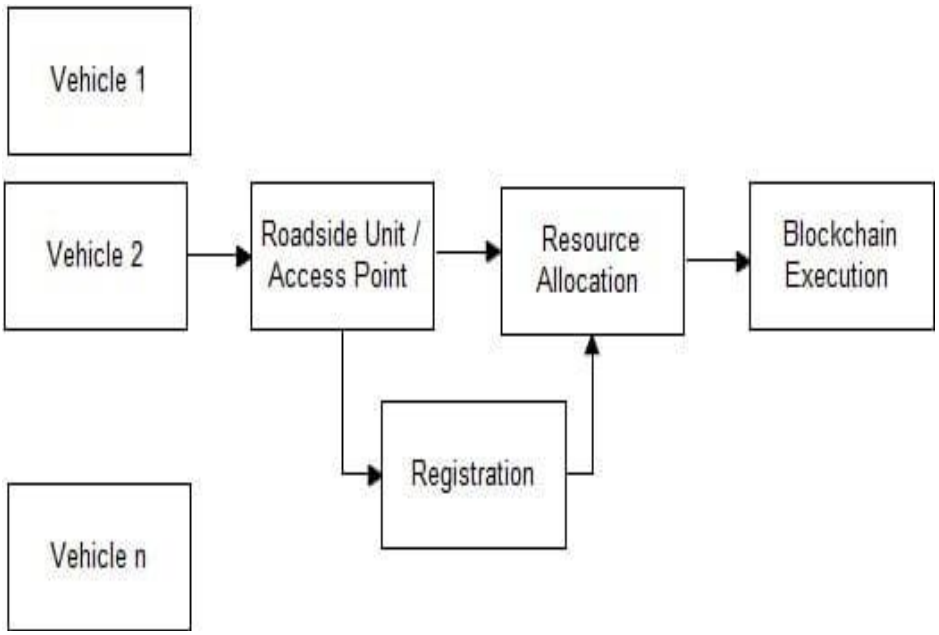
|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

been introduced, along with the associated needs, efficacy, and research opportunities. A distributed architecture is possible for in-vehicle computing, which can add more resilience and parallelisms, especially with simultaneous computations of multi-sensor data, albeit with the overhead of handling synchronisations and causality, which is not addressed in this paper.

III.PROPOSED SYSTEM APPROACH

All of your data will be safe in the cloud since it is encrypted. Data encryption has contributed to the provision of a safe means of archiving information. Since the information is being stored in the cloud, all other authorized users can gain access to it at any time. The user, the system, and the adversary are all present in this system. Authentication is verified to increase the system's safety. The system administrator may submit a request to have it updated. A system will only allow an update request to proceed if the person making it has been verified as a legitimate user. The ECDSA hashing method and the blockchain assist the system guarantee security. In order to verify a user's identity, public and private secret keys are used. The use of blockchain technology makes data safer and more robust.



Block diagram of proposed system

IV. ADVANTAGES AND DISADVANTAGES

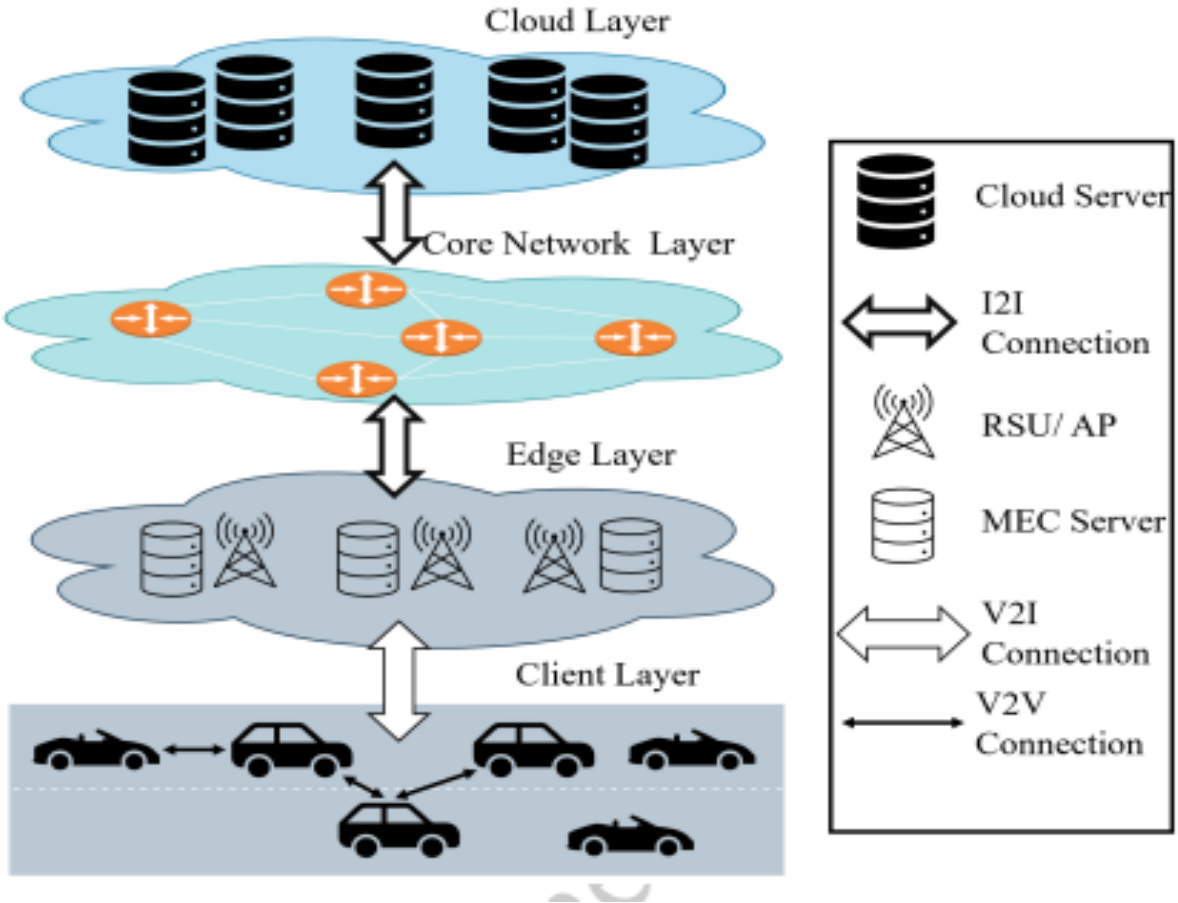
- It's a secure and trusted industry standard: ECDSA and SHA-256 is an industry standard that is trusted by leading public-sector agencies and used widely by technology leaders.
- Collisions are incredibly unlikely: There are 2^{256} possible hash values when using SHA-256, which makes it nearly impossible for two different documents to coincidentally have the exact same hash value. (More on this in the following section).
- The avalanche effect: Unlike some older hashing algorithms, even a very minor change to the original information completely changes the hash value.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

V.METHODOLOGY USED IN PROPOSED SYSTEM



ALGORITHM USED: ECDSA

ECDSA is a digital signature algorithm that makes use of ECC to create the key pairs used in the signing and verification process of the digital signature. Because of the advantages of ECC compared to other public-key algorithms, it is commonly used in blockchain applications to sign transactions or events.A digital signature is an electronic equivalent of a handwritten signature that allows a receiver to persuade a third party that the message was indeed sent by the sender. Handwritten signatures are substantially less secure than digital signatures. A digital signature cannot be forged in any way. Another advantage of digital signatures over handwritten signatures is that they apply to the entire message.

An ECDSA key pair is linked to a specific set of EC domain settings. The public key is a randomly generated multiple of the base point, whereas the private key is the integer used to generate the multiple points.

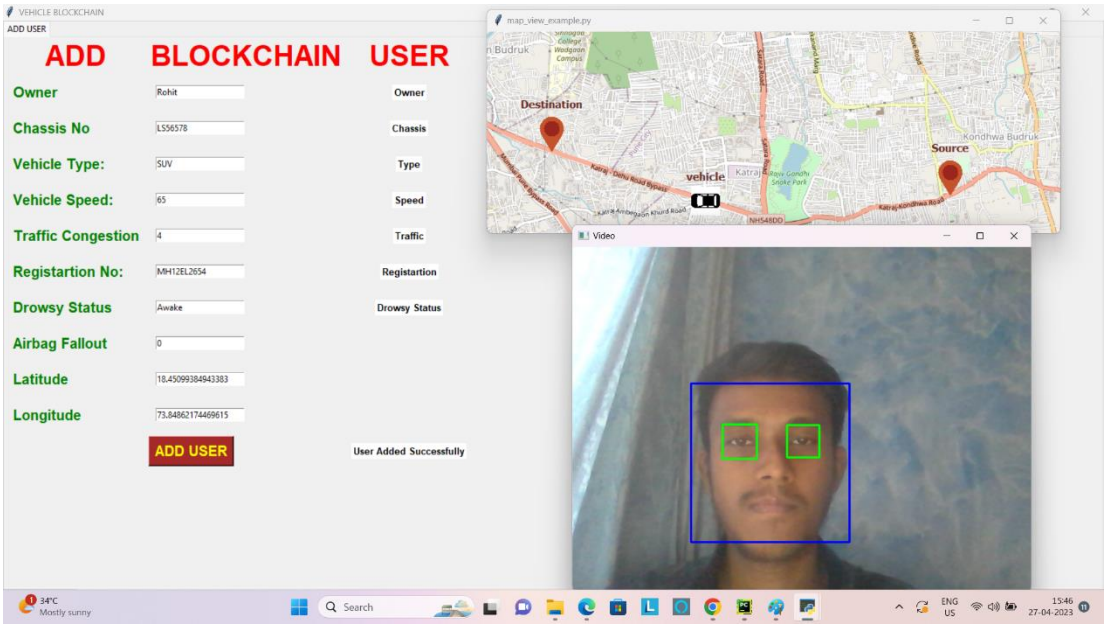
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

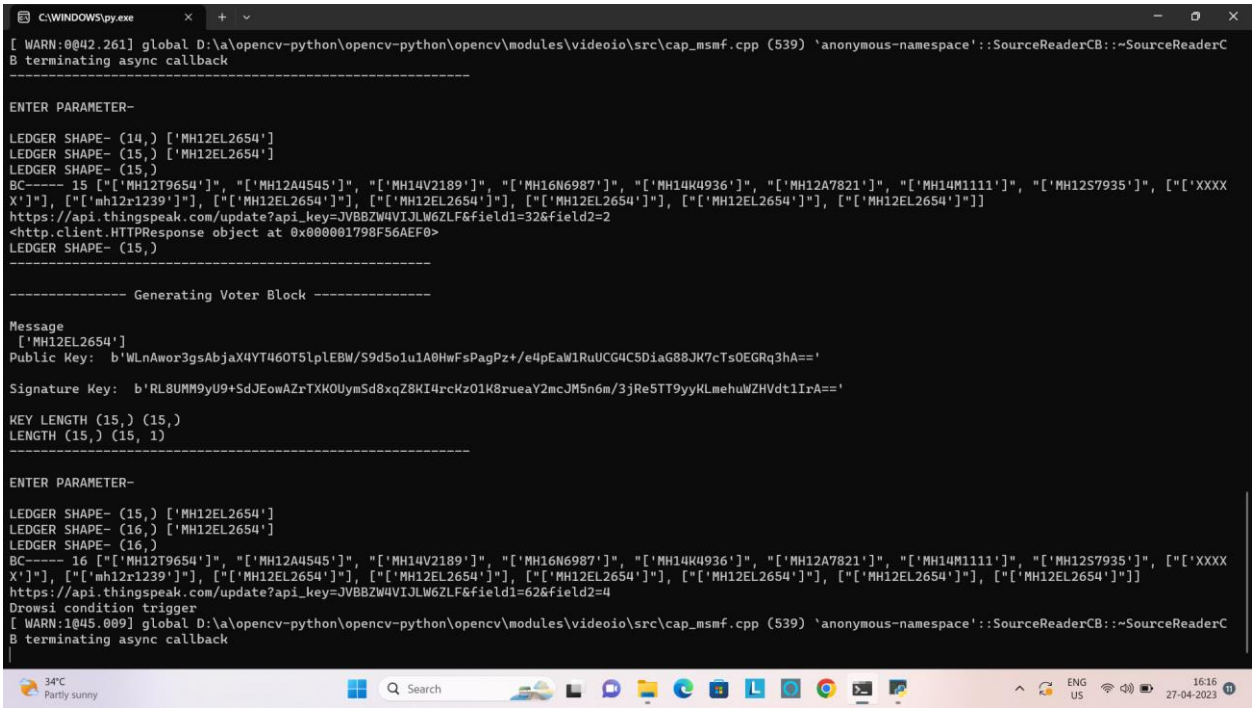
| DOI:10.15680/IJIRSET.2023.1205062 |

VI. RESULTS

VEHICLE 1 UPDATING INFORMATION IN BLOCKCHAIN AFTER EVERY 10 SEC:



BLOCKCHAIN VIEW :

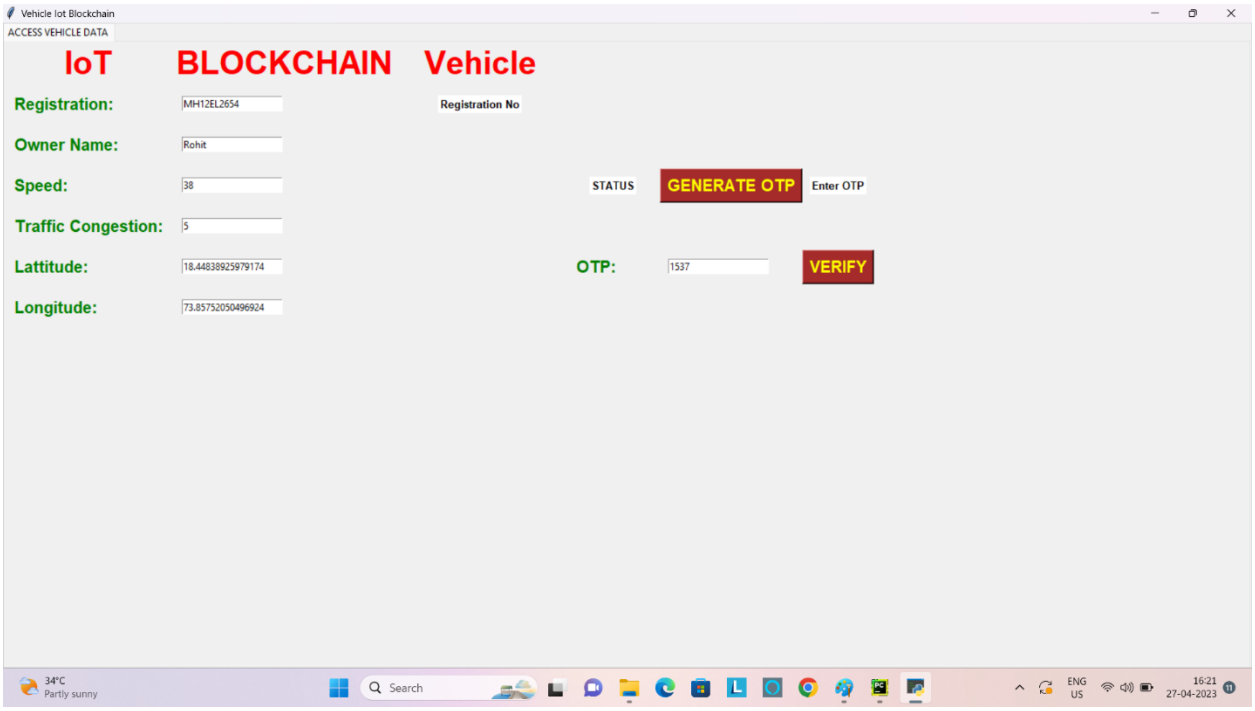


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

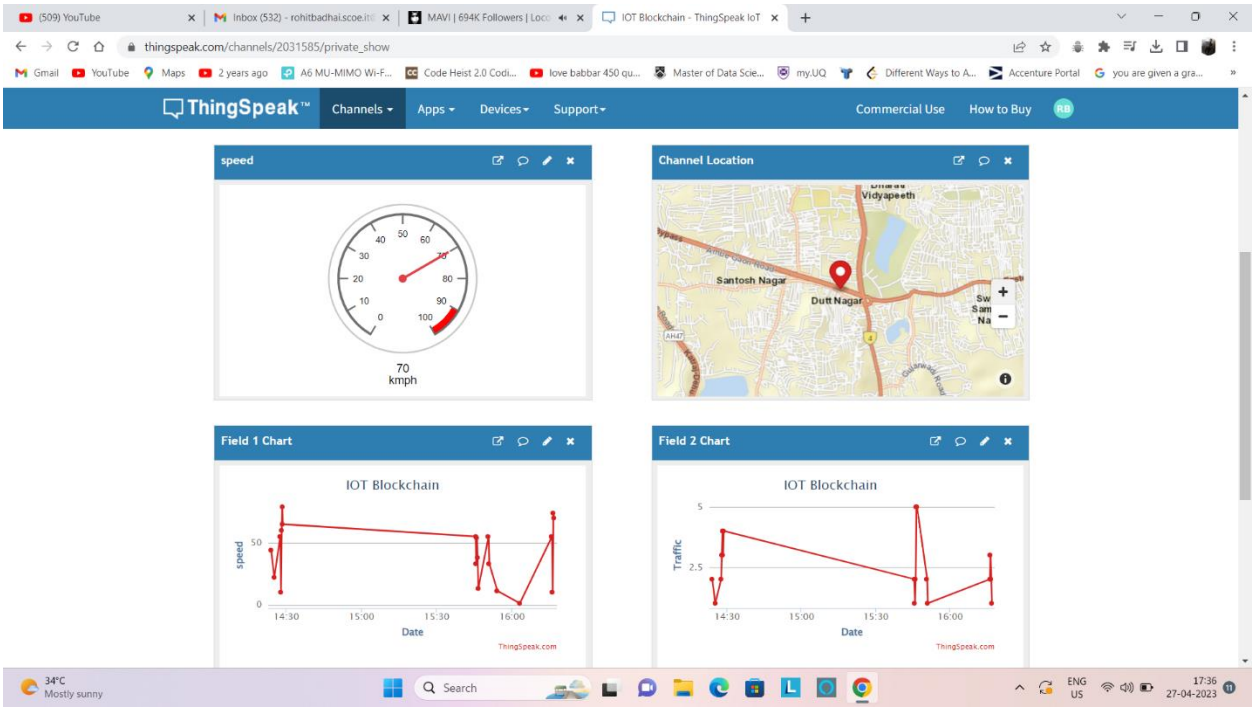
|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

VEHICLE 2 ACCESSING INFORMATION OF VEHICLE 1:



ANALYSING VEHICLE INFORMATION ON CLOUD:

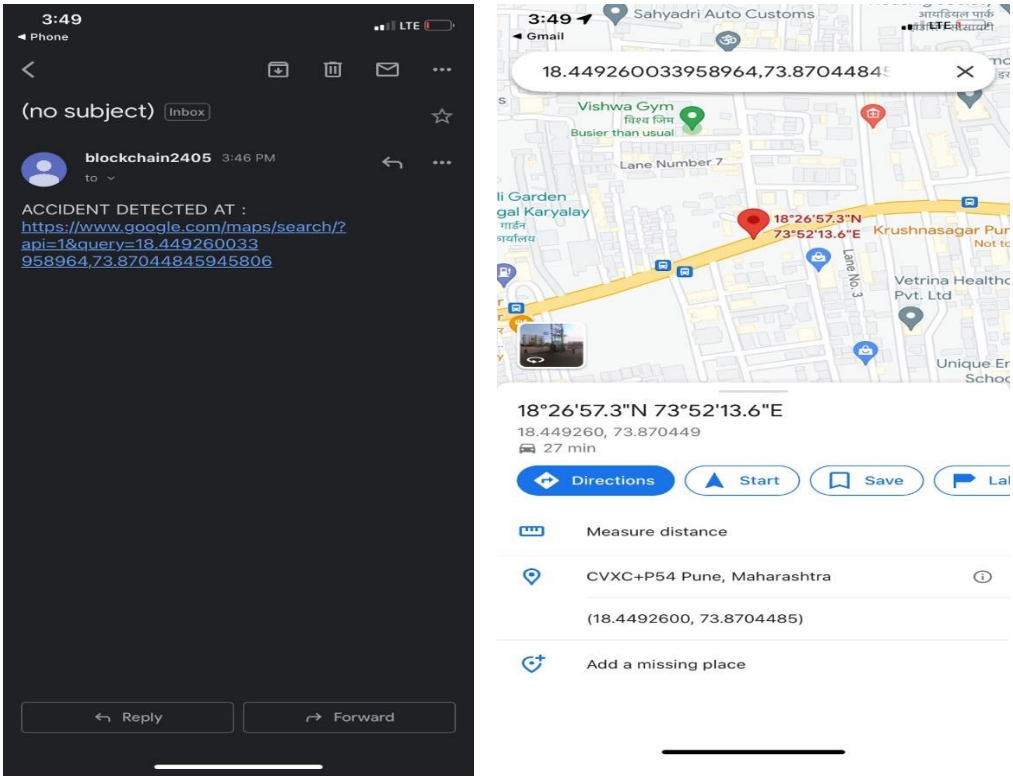


|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

QOS EXAMPLE:



VII. CONCLUTION

There is a huge possibility for exploiting edge resources to handle vast volumes of vehicular data thanks to the combination of artificial intelligence (AI) and vehicular edge computing (VEC). However, there is a gap in the literature concerning the lack of transparency in IVEC and the associated problems (such as Acc bias/unfair resource allocation, free riding, and forged output). Features like immutability and auditable interactivity make the combination of IVEC infrastructure with blockchain compelling in this context. To improve visibility into resource allocation and to provide edge clients (such automobiles and RSES) with computation verification tools, we introduce a hierarchical IVEC architecture based on blockchain technology. To better manage uneven load distribution, we also offer a safe computation trading paradigm in IVEC for increasing edge computing power in the horizontal dimension. We finish with a discussion of some intriguing and cutting-edge future prospects for research and a description of security flaws in the IVEC infrastructure.

VIiI. FUTURE WORK

Work on IoT based vehicle mobility and security forms the vehicles to their destination.
Enhance the routing of a vehicle from source to destination and QOS.

IX. ACKNOWLEDGMENT

A blockchain-based security layer is also implemented for the validation and verification of the edge server, which forwards the data to the cloud server for heavy computation and permanent storage

REFERENCES

[1] M.-K. SHIN, K.-H. NAM, AND H.-J. KIM, ``SOFTWARE-DENED NETWORKING (SDN): A REFERENCE ARCHITECTURE AND OPEN APIS," IN *PROC. INT. CONF. ICT CONVERG. (ICTC)*, OCT. 2012, PP. 360361.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205062 |

[2] D. KREUTZ, F. RAMOS, P. E. VERÍSSIMO, C. E. ROTHENBERG, S. AZODOLMOLKY, AND S. UHLIG, ``SOFTWARE-DENED NETWORKING: A COMPREHENSIVE SURVEY,"*PROC. IEEE*, VOL. 103, NO. 1, PP. 1476, JAN. 2015.
[3] S. SINGH AND S. AGRAWAL, ``VANET ROUTING PROTOCOLS: ISSUES AND CHALLENGES," IN *PROC. RECENT ADV. ENG. COMPUT. SCI. (RAECS)*, MAR. 2014,
[4] E. BORCOCI, ``FROM VEHICULAR AD-HOC NETWORKS TO INTERNET OF VEHICLES," IN *PROC. NEXCOMM CONF.*, VENICE, ITALY, 2017, PP. 2327.
[5] M. O. KALININ, V. KRUNDYSHEV, AND P. SEMIANOV, ``ARCHITECTURES FOR BUILDING SECURE VEHICULAR NETWORKS BASED ON SDN TECHNOLOGY," *AUTOM. CONTROL COMPUT. SCI.*, VOL. 51, NO. 8, PP. 907914, DEC. 2017.
[6] W. RAQUE, L. QI, I. YAQOOB, M. IMRAN, R. U. RASOOL, AND W. DOU, ``COMPLEMENTING IOT SERVICES THROUGH SOFTWARE DENED NETWORKING AND EDGE COMPUTING: A COMPREHENSIVE SURVEY," *IEEE COMMUN. SURVEYS TUTS.*, VOL. 22, NO. 3, PP. 17611804, 3RD QUART., 2020.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details