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 2, February 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

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: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202095 |

A Survey on 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: To Enhance and maximizethe V2V communication network's information application performance and reliability, edge computing has gained the attention of researchers. In current research, cloud computing is used for message related task execution, which increases the response time. We propose a Software-defined Fault Tolerance and QoS-Aware (Quality of Service) V2V communication Using Edge Computing Secured by Blockchain to reduce overall communication delay, message failure fault tolerance, and secure service provisioning for V2V Communication network. Block chain and edge computing have an interesting interdependent relationship. Edge computing/a distributed compute architecture can provide an infrastructure for block chain nodes to store and verify transactions. On the other hand, blockchain could enable a truly open distributed cloud marketplace. If the message delivery fails, the fault tolerance algorithm will resend the failure message. The result shows the performance of the proposed model, which decreased the overall message communication delay by 55% of the normal and emergency messages by using the edge server SDN controller. Furthermore, the proposed model reduces the execution time, security risk, and message failure ratio by using the edge server, cloud server and blockchain infrastructure.

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

I. INTRODUCTION

Blockchain and edge computing have a very useful and interesting relationship.Edge computing/a distributed compute architecture can provide an infrastructure for blockchain nodes to store and verify transactions with very less delay.On the other hand, blockchain could enable a truly open distributed cloud marketplace to ensure a secured environment. We propose a blockchain based decentralized architecture to enhance transparency in IVEC resource management and leverage edge consumers (e.g., vehicles) with a computation verification option. Additionally, we address the unbalanced load distribution issue and propose a secure IVEC federation model for balancing loads.To reduce security risks, a blockchain-based system has been introduced which directly helps for QoS. This system provides security, flexibility, and many more features, which have attracted and motivated many businesses to run on IoT. In this Project, blockchain is used to provide security services to an IoT base network after proper validation and verification of the remote edge server but by generating IoT data manually. Blockchain is an efficient system in terms of security and energy utilization.The blockchain provides the lowest latency time, energy efficiency, and reliability to the user, especially among businesses. The functionality of the blockchain is to provide the security and flexibility of data to everyone.To reduce security risks, a blockchain-based system has been introduced. This system provides security, flexibility, and many more features, which have attracted and motivated many businesses to run on IoT without thinking about data's security. In this Project, blockchain is used to provide security services to an IoT base network' data after proper validation and verification of the remote edge server so even end user has to be verified for accessing the data. Blockchain is an efficient system in terms of security and energy utilization.The project answers on how to make this blockchain system efficient by changing the algorithms and using a variety of artificial-based algorithms to utilize the data efficiently.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202095 |

II. LITERATURE SURVEY

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

In this paper we addressed the problem of providing transaction security in decentralized SG energy trading without reliance on trusted third party. We implemented a token-based private decentralized energy trading system that enables peers to anonymously negotiate energy prices and securely perform trading transactions. We used blockchain technology, multisignatures and anonymous encrypted message propagation streams to provide certain levels of privacy and security. Our system uses peer-to-peer communitybased data replication method where transactions are protected from failure since they are replicated among all active nodes. In addition, the proof-of-work, as in Bitcoin, allows the system to overcome Byzantine failures and to combat double-spending attacks which are critical in any electronic payment system.Wemodeled and simulated energy trading case scenarios among peers in a SG. We performed security and performance analysis and evaluation. We simulated network related attacks and demonstrated our claim that the system is resistant to significant known attacks; it does not reveal identities of trading parties; and it keeps financial profiles secure and private. We identified and discussed potential attacks and elicited security and privacy requirements. Overall, we found that the appropriate combination of blockchain technology, multi-signatures and anonymous encrypted message propagation streams presents a feasible and reliable direction towards decentralized SG energy trading with higher privacy and security compared to the traditional centralized trading solutions.

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

The transition to a data and value-driven world is fostered by the pace of the technological disruptions of an Internet-enabled global world, the challenges of future mobility, and an increasing business competition. In this ever more complex ecosystem, the use of blockchain can provide to the automotive industry a platform able to distribute trusted and cyber-resilient information that defy current non collaborative organizational structures. It must be noted that despite the hype reported by numerous organizations, it is necessary to perform an objective evaluation about how and whether to invest or not in blockchain from a business management and cybersecurity standpoint. This article covered a broad suite of issues that arise from the advent of a disruptive technology like blockchain. In addition, we present a holistic approach to a blockchainbased advanced automotive industry with a review of the main scenarios and the optimization strategies for designing and deploying these applications. Furthermore, some recommendations were mentioned to guide future researchers and managers on some of the open issues that will have to be confronted before deploying the next generation of secure blockchain applications.

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

As one of the most important features in blockchain systems, smart contracts have attracted much attentions but also have exposed many problems. The major contributions of our survey include three aspects. First, we make a in-depth survey about the security verification of blockchain smart contracts and selected 53 most related papers. To show the state-of-art of this topic, we focused on two aspects, where 20 papers related to the security assurance and 33 papers related to the correctness verification.Second, we propose a taxonomy towards such topic. More specifically, the security assurance aspects is classified into three categories, including environment security, vulnerability scanning, and performance impacts. While the correctness verification aspect is classified into two categories, including programming correctness and formal verification. We discuss the pros and cons of each category.Third, through in-depth analysis of the related papers, we summarize the research status and point out the further research directions in smart contract security and correctness. The main points are as follows:

According to the growth trend of related papers, we can see that the security and correctness of smart contracts are getting more and more attention. We urgently need the more comprehensive methods to ensure the security and correctness of smart contracts, thereby reducing losses.

In the security of smart contracts, vulnerability scanning method is currently widely used and have achieved significant results. In future, we can continue to expand research in this direction. For example: discovering unknown vulnerabilities (try to infer whether there are vulnerabilities that have identical or similar principles to the known vulnerabilities) and optimizing vulnerability detection method, which avoids repeating a lot of vulnerability detection work and reduces errors or omissions.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202095 |

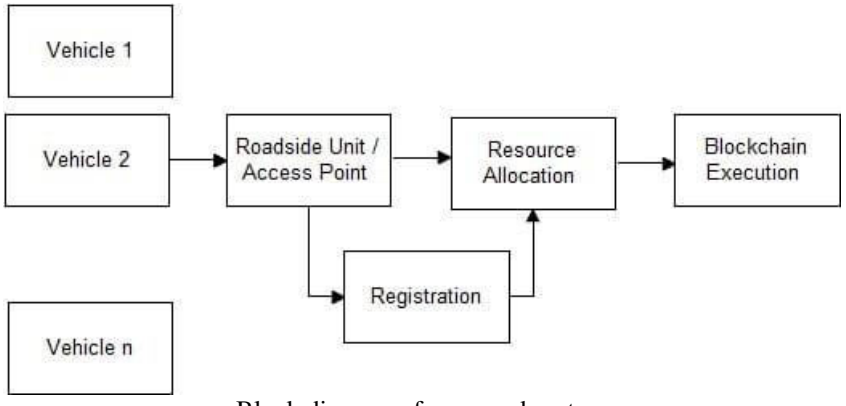
1) In the correctness of smart contracts, more work is currently focused on programming correctness. Formulating the programming standards for smart contracts, designing a set of smart contract development processes, and improving the security awareness of programmers are all the future research directions.
2) Although the amounts of papers related to programming correctness is more, the growth trend of formal verification method is more obvious. Formal verification method is based on mathematical model and is more rigorous and reliable. Therefore, using formal verification method to verify smart contracts will be the trend of future research. In future, we can consider the following research directions: designing the more complete formal verification tools, combining formal verification methods with vulnerability analysis methods to complement each other, and visualizing the contract execution process using other formal modeling tools such as CPN (colored Petri Nets).

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

In this paper, we have introduced a vision for the evolving smart vehicle's computing needs and architecture considerations. We have introduced the needs, efficacy and research opportunities of optimally allocating existing computing resources for emerging vehicular applications, modeling vehicular application performance for different capabilities and computing architectures, and tools to help develop optimal in-vehicle computing architectures as well as collaborative computing system with edge computing nodes. Although this paper mainly focuses on a centralized architecture for in-vehicle computing, a distributed architecture is feasible, which can add more resiliency and parallelisms, especially with simultaneous computations of multi-sensor data, albeit with the overhead of handling synchronizations and causality.

III.PROPOSED SYSTEM APPROACH

The data that is stored over the Thing speak cloud is encrypted. The encryption of the data has helped in providing a secure method of storage of data. As the data is being stored over the cloud, it can be accessed by the other authenticated members of the system. In this system user, system and attacker are present. To provide more security to the system authentication is checked. Admin can change in the updating request to the system. If user is authenticated then updating request is accepted otherwise system block to that request and consider that as attack. System provide security with the help of block chain, ECDSA and SHA 256 algorithm.ECDSA is the building block of Block chain.Using public and private secret keys authentication is checked. Hence using blockchain data become more secure and system become powerful.



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).

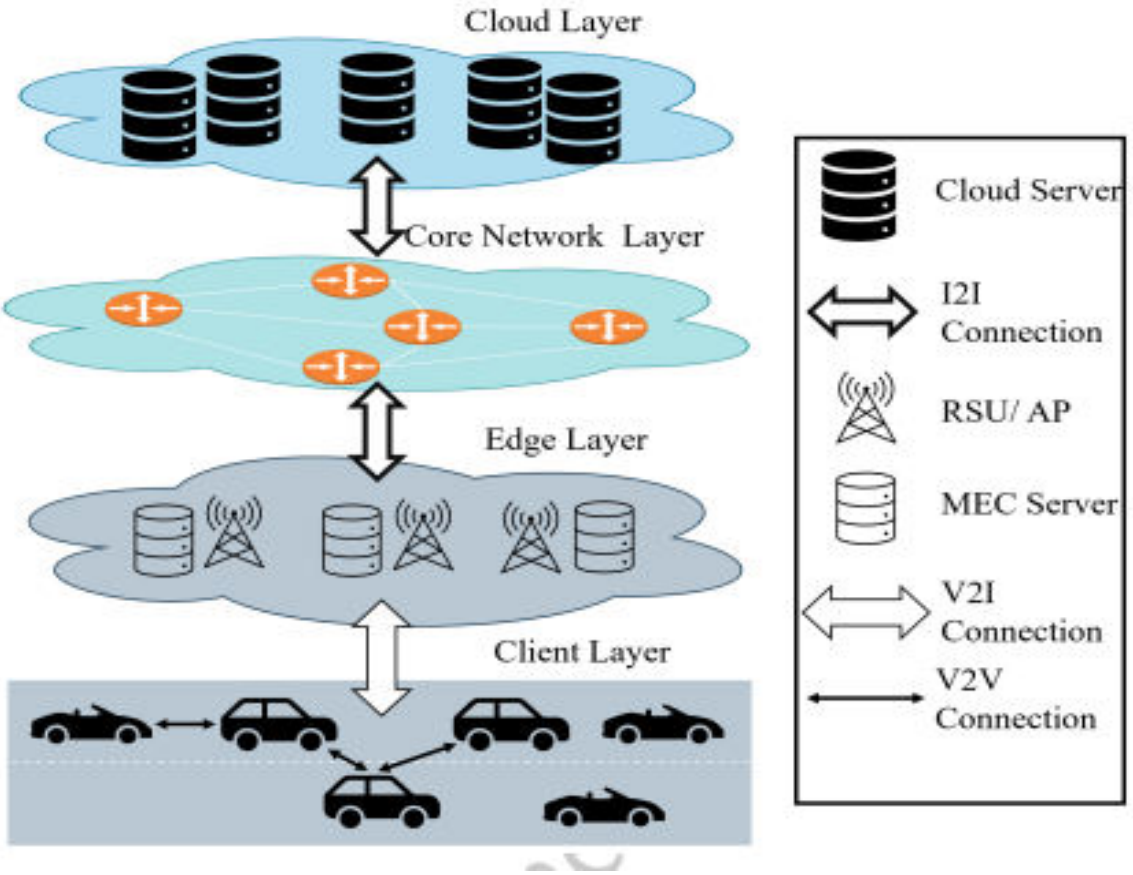
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202095 |

- The avalanche effect: Unlike some older hashing algorithms, even a very minor change to the original information completelychanges the hash value.

V.METHODOLOGY USED IN PROPOSED SYSTEM



Provide data to the System which represents Iot data. The data is the values to various parameters like speed, traffic congestion, source, destination, etc. These parameters are updated after some seconds. With the help of digital algorithm ECDSA which is building block of block chain encrypt and update the transaction in the ledger. At the same time send the data to the cloud for heavy computation. But at breach in the normal range of any parameter alert the user without waiting for response from cloud.

VI. CONCLUSION

The Integration of Blockchain and vehicular edge computing (VEC) creates an enormous opportunity for leveraging edge resources to process high volume vehicular data. However, the existing works lack in investigating issues (such as Acc bias/unfair resource allocation, free riding, forged output) related to lack of transparency in IVEC. In this regard, the integration of IVEC infrastructure and blockchain is persuasive due to its features such as immutability and auditable interaction. In this article, we present blockchain based hierarchical IVEC architecture to enhance transparency in resource management and leverage edge clients (such as vehicles and RSES) with computation verification options. Furthermore, we propose a secure computation trading model in IVEC for expanding edge computation power in horizontal dimension in

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.118| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2023 ||

| DOI:10.15680/IJIRSET.2023.1202095 |

order to efficiently man age unbalanced load distribution. We also describe security vulnerabilities in IVEC infrastructure and conclude with some exciting and state of the arts research directions.

VII. FUTURE WORK

Work on IoT based vehicle mobility and security forms the vehicles to their destination. Also, able to improve existing services like routing which still doesn't provide accurate result. This project p

VIII. 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.
[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: 8.118

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