IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133116

Vision based architecture of Home Security System

Tanushri Raut[1], Siddhi Thakur[2], Sania Chorge[3], Sheetal Sapate[4]

Scholars, Bharati Vidyapeeth's Jawaharlal Nehru Institute of Technology[1-3]

Guide, Bharati Vidyapeeth's Jawaharlal Nehru Institute of Technology[4]

Abstract: Researchers have focused on edge computing to improve and maximise the information application performance and reliability of the V2V communication network. In the present study, cloud computing is employed for message-related job execution, which boosts reaction time. We present a Software-defined Fault Tolerance and QoS-Aware (Quality of Service) V2V communication using Edge Computing Secured by Blockchain to minimise overall communication latency, message failure fault tolerance, and secure service provisioning in a V2V communication network. Block chain and edge computing have an intriguing interdependence. Edge computing/distributed computation architecture may offer a platform for block chain nodes to store and validate transactions. On the other side, blockchain may allow a fully open distributed cloud marketplace.

If the message delivery fails, the fault tolerance mechanism resends the error message. The results demonstrate the performance of the suggested model, which reduced the total message transmission time by 55% for routine and emergency messages by using the edge server SDN controller. Furthermore, the suggested approach uses edge servers, cloud servers, and blockchain infrastructure to minimise execution time, security risk, and message failure ratio.

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

I. INTRODUCTION

Blockchain and edge computing have a highly beneficial and fascinating interaction. Edge computing/distributed compute architecture can offer infrastructure for blockchain nodes to store and validate transactions with little latency. On the other side, blockchain has the potential to create a fully open distributed cloud marketplace, ensuring a safe environment. We propose a blockchain-based decentralised architecture to improve transparency in IVEC resource management and provide edge customers (such as automobiles) with a computation verification alternative. Additionally, we examine the problem of imbalanced load distribution and offer a secure IVEC federation architecture for load balancing. To eliminate security threats, a blockchain-based system has been implemented, which directly contributes to QoS.

This system offers security, flexibility, and many other benefits that have enticed and pushed many firms to operate on IoT. In this project, blockchain is utilised to offer security services to an IoT base network once the distant edge server has been properly validated and verified, however IoT data is generated manually. Blockchain is an energy-efficient and secure solution. The blockchain offers the lowest latency time, energy efficiency, and dependability to users, particularly companies. The blockchain's functionality is to give security and flexibility to all data. To mitigate security issues, a blockchain-based solution has been implemented.

This technology offers security, flexibility, and many other benefits that have enticed and pushed many firms to operate on IoT without worrying about data security. In this project, blockchain is utilised to offer security services to an IoT base network's data after appropriate validation and verification of the distant edge server, and even the end user must be validated before accessing the data. Blockchain is an energy-efficient and secure solution. The research addresses how to make this blockchain system more effective by modifying the algorithms and using a number of artificial-based methods to optimise data utilisation.

II. LITERATURE SURVEY

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

In this article, we tackled the issue of ensuring transaction security in decentralised SG energy trading without relying on a trusted third party. We built a private decentralised energy trading system based on tokens, allowing peers to negotiate energy pricing secretly and securely. We employed blockchain technology, multisignatures, and anonymous encrypted

DOI: 10.17148/IJARCCE.2024.133116

message propagation streams to offer privacy and security. Our system employs a peer-to-peer community-based data replication mechanism in which transactions are secured against failure since they are replicated across all active nodes. Furthermore, the proof-of-work algorithm, as used in Bitcoin, enables the system to overcome Byzantine failures and prevent double-spending assaults, both of which are crucial in any electronic payment system.We modelled and simulated energy trade scenarios among peers in an SG.

We conducted security and performance analyses and evaluations. We simulated network assaults to show that the system is immune to important known vulnerabilities, does not expose trade partners' names, and maintains financial profiles safe and confidential.

We identified and discussed possible assaults while also gathering security and privacy needs. Overall, we discovered that the appropriate combination of blockchain technology, multi-signatures, and anonymous encrypted message propagation streams provides a viable and dependable path towards decentralised SG energy trading with greater privacy and security than traditional centralised trading solutions.

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

The rapid rate of technology innovations in an Internet-enabled global environment, the problems of future mobility, and increased economic competitiveness all contribute to the shift to a data and value-driven world. In this increasingly complex environment, blockchain technology may offer the automobile sector with a platform for distributing reliable and cyber-resilient information that defies present non-collaborative organisational structures. Despite the euphoria generated by various organisations, it is critical to conduct an impartial review of how and if to engage in blockchain from a business management and cybersecurity perspective.

This article addressed a wide range of concerns that come with the introduction of a disruptive technology such as blockchain. In addition, we give a comprehensive approach to a blockchain-based advanced automotive sector, including a study of the key scenarios and optimisation methodologies for creating and implementing these applications. Furthermore, suggestions were made to help future researchers and managers through some of the outstanding challenges that must be addressed before implementing the next generation of safe blockchain applications.

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

Smart contracts, as one of the most essential aspects of blockchain systems, have garnered a lot of interest, but they have also revealed a number of issues. Our survey's key contributions consist of three areas. First, we conduct an in-depth assessment on the security verification of blockchain smart contracts and choose the 53 most relevant publications.

To demonstrate the state-of-the-art in this area, we concentrated on two aspects: 20 articles on security assurance and 33 papers on correctness verification.Second, we offer a taxonomy for such topics. More precisely, security assurance components are divided into three categories: environmental security, vulnerability screening, and performance implications.

The accuracy verification component is divided into two categories: programming correctness and formal verification. We analyse the advantages and disadvantages of each group.Third, we summarise the current state and identify future research paths in smart contract security and correctness based on an in-depth examination of the relevant works.

The main points are as follows:

1) According to the increasing number of linked articles, the security and accuracy of smart contracts are receiving more and more attention. We urgently want more extensive solutions to assure the security and accuracy of smart contracts, decreasing losses.
2) In the security of smart contracts, vulnerability scanning is presently frequently utilised and has produced substantial results. In the future, we can continue to do study in this area. For example, discovering unknown vulnerabilities (attempting to determine whether there are vulnerabilities with identical or similar principles to known vulnerabilities) and optimising vulnerability detection methods, which avoids repeating a large amount of vulnerability detection work while reducing errors or omissions.
3) More effort is now being done to ensure the accuracy of smart contracts in terms of programming. The next research directions include developing programming standards for smart contracts, defining a set of smart contract development methods, and increasing programmers' security awareness.
4) Although the number of works on programming correctness is increasing, the rising trend of formal verification methods is more apparent. Formal verification uses a mathematical model and is more rigorous and dependable. As a

DOI: 10.17148/IJARCCE.2024.133116

result, future research will focus on formal verification methods for smart contracts. In the future, we can consider the following research directions: developing more comprehensive formal verification tools, combining formal verification methods with vulnerability analysis methods to complement one another, and visualising the contract execution process using other formal modelling tools such as CPN (coloured Petri Nets).

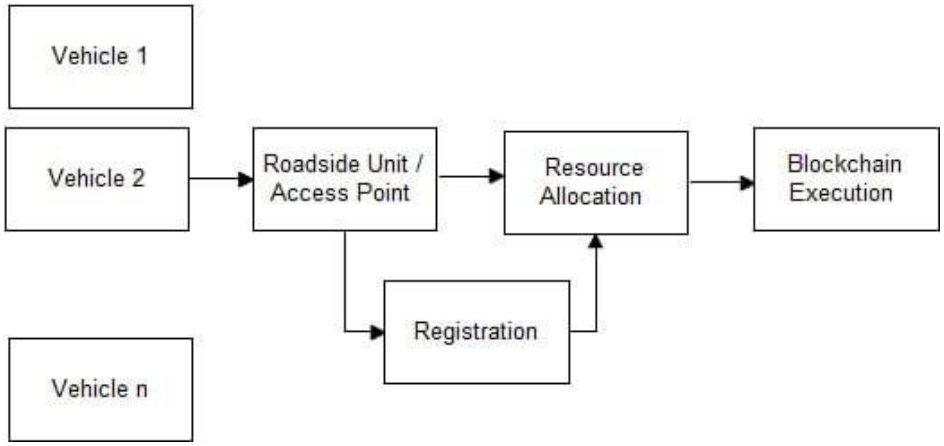
4. SABUR BAIDYA, YU-JEN KU, HENGYU ZHAO, 2020

In this work, we provide a perspective for the future computing demands and architectural concerns of smart vehicles. We have discussed the requirements, efficacy, and research opportunities for optimally allocating existing computing resources for emerging vehicular applications, modelling vehicular application performance for various capabilities and computing architectures, and tools to assist in the development of optimal in-vehicle computing architectures as well as collaborative computing systems with edge computing nodes. Although this paper primarily focuses on a centralised architecture for in-vehicle computing, a distributed architecture is possible, which can add more resiliency and parallelism, particularly with simultaneous computations of multi-sensor data, albeit at the expense of handling synchronisations and causality.

III. PROPOSED SYSTEM APPROACH

The data saved on the ThingSpeak cloud is encrypted. The encryption of data has contributed to a safe technique of data storage. The data may be viewed by other authorised members of the system since it is stored in the cloud. There are three components in this system: the user, the system, and the attacker. To add security to the system, authentication is verified. The administrator may make changes to the system's update request.

If the user is authorised, the updating request is granted; otherwise, the system blocks the request and considers it an attack. The system provides security via the use of block chains, ECDSA, and the SHA 256 algorithm. ECDSA is the foundation of Block Chain. Authentication is verified using both public and private secret keys. As a result of implementing blockchain, data is more secure and the system becomes more powerful.



Block diagram of proposed system

IV. METHODOLOGY USED IN PROPOSED SYSTEM

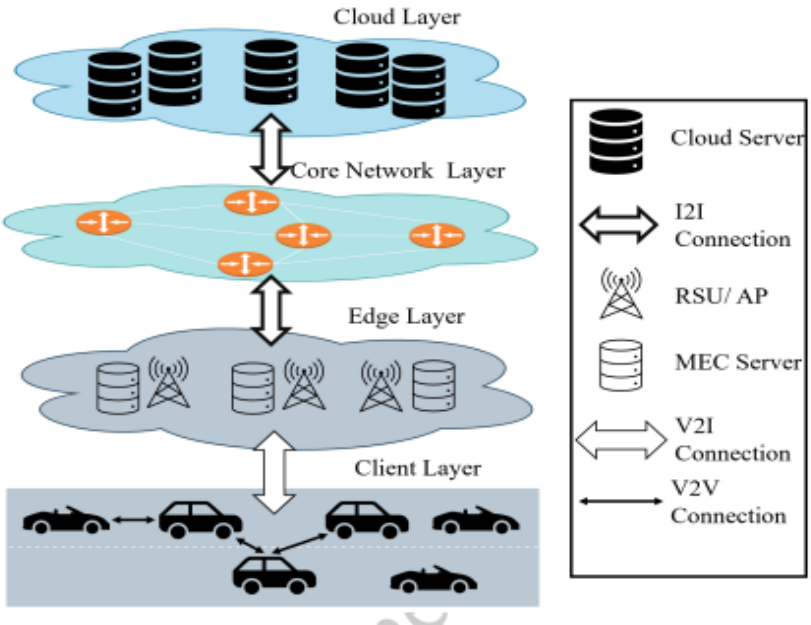
Provide data to the System that reflects IoT data. The data represents the values for several characteristics such as speed, traffic congestion, source, and destination. These parameters are updated after a few seconds. Encrypt and update the ledger transaction using the digital technique ECDSA, which is a block chain building block. At the same time, transfer the data to the cloud for intensive processing. However, a violation in the typical range of any parameter alerts the user without waiting for a response from the cloud.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

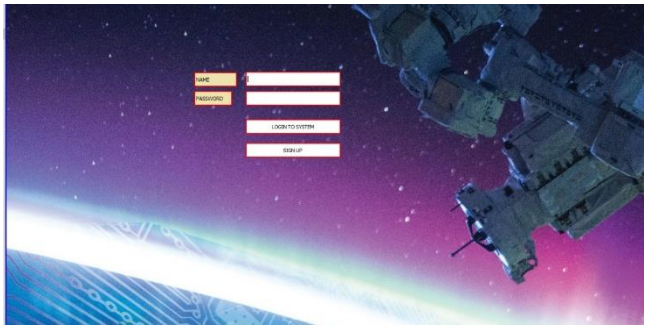
International Journal of Advanced Research in Computer and Communication Engineering

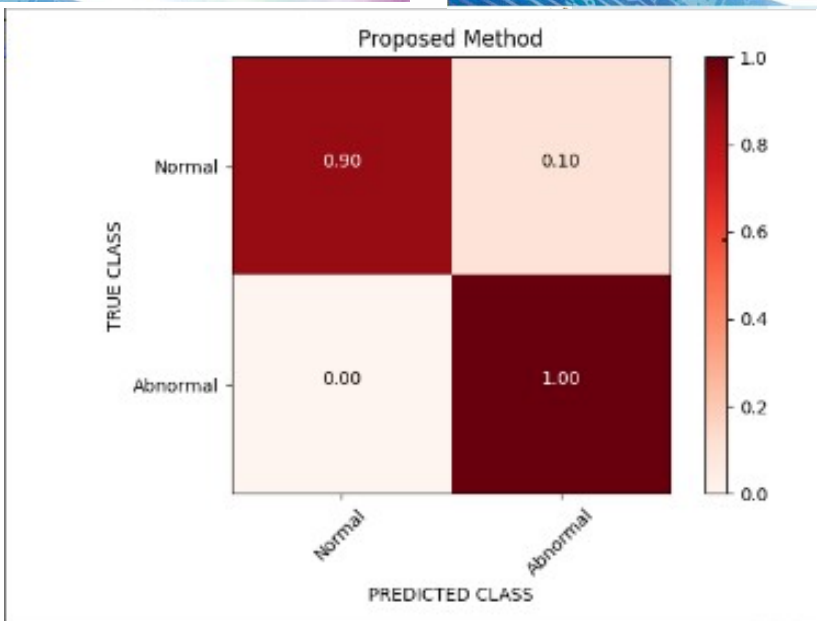
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.133116



V. RESULT





International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024
DOI: 10.17148/IJARCCE.2024.133116

VI. ADVANTAGES AND DISADVANTAGES

- It is a secure and recognised industry standard. ECDSA and SHA-256 are industry standards that are trusted by top public-sector entities and extensively used by technology leaders.
- Collisions are very improbable. When using SHA-256, there are 2256 potential hash values, making it almost difficult for two separate documents to have the same hash value. (More on this in the next section).
- The avalanche effect: Unlike some previous hashing algorithms, even tiny modifications to the source data entirely alter the hash result.

VII. FUTURE WORK

Work on IoT-based vehicle mobility and security enables cars to reach their destination. Also capable of improving existing services such as routing, which currently does not offer correct results.

CONCLUSION

The combination of blockchain with vehicle edge computing (VEC) opens up significant possibilities for exploiting edge resources to analyse large amounts of vehicular data. However, present research does not address concerns (such as Acc bias/unfair resource allocation, free riding, and falsified output) associated to IVEC's lack of transparency. In this context, the combination of IVEC infrastructure with blockchain is compelling owing to properties like immutability and auditable interaction.

In this work, we describe a blockchain-based hierarchical IVEC architecture that improves transparency in resource management and provides edge clients (such as automobiles and RSES) with computation verification choices. Furthermore, we provide a secure computation trading model in IVEC for increasing edge computing power in the horizontal dimension in order to optimally manage uneven load distribution. We also discuss security risks in IVEC infrastructure before concluding with some intriguing and cutting-edge research opportunities.

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.