Blockchain based DApp for VANET

Submitted By

20BCE045 Dhruva Chopda

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

December 2023

Minor Project

Submitted in partial fulfillment of the requirements

for the degree of

Bachelor of Technology in Computer Science and Engineering

Submitted By

20BCE045 Dhruva Chopda

Guided By

Prof. Umesh Bodkhe

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

December 2023

Certificate

This is to certify that the minor project entitled **"Blockchain based DApp for VANET"** submitted by **Dhruva Chopda(20BCE045)** towards the partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering, Nirma University, Ahmedabad, is the record of work carried out by her under my super- vision and guidance. In my opinion, the submitted work has reached the level required for being accepted for examination. The results embodied in this minor project, to the best of my knowledge, haven't been submitted to any other university or institution for the award of any degree or diploma.

Prof. Umesh Bodkhe
Assistant Professor
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Bhavsar

Dr Madhuri Bhavsar
Professor and Head,
CSE Department
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, **Dhruva Chopda**, Roll. No. **20BCE045**, give an undertaking that the Minor Project entitled **"Blockchain based DApp for VANET"** submitted by me, towards the partial fulfilment of the requirements for the degree of Bachelor of Technology in **Computer Science and Engineering**, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Dhruva

Signature of Student
Date: 08|12|2023
Place:Ahmedabad

Endorsed by
Prof.Umesh Bodkhe
(Signature of Guide)

Acknowledgements

- Dhruva Chopda

20BCE045

I would like to express my special thanks and gratitude towards my guide Prof. Umesh Bodkhe who gave us fruitful and insightful guidance and support , throughout the semester. Also , I will remain thankful for giving me the opportunity to explore more about Vehicular ad-hoc network(VANET), Blockchain and decentralized Application. This project helped me to understand topics with real world applications.

Abstract

As automotive technology develops towards an automated and networked future, privacy and security in vehicular communication becomes critical. This study investigates how to incorporate blockchain technology into vehicular ad-hoc networks (VANETs) to solve important issues with data integrity, private communication, and safe car registration. The suggested method makes use of blockchain's decentralized and unchangeable properties to improve reliability and effectiveness of intelligent transportation systems. The VANET blockchain contract serves as an example of how a smart contract-based system might be implemented to protect vehicle registration and enable clear communication among linked vehicles.

Abbreviations

VANET	Vehicular ad-hoc network
MANET	Mobilead-hoc network
DSRC	Dedicated Short-Range Communication

———————————————————————————————————————

_

Certificate

Statement of Originality

Acknowledgements

Abstract

Abbreviations

List of Tables

List of Figures

1 Introduction
- 1.1 Introduction to VANET
- 1.2 Working of VANET
- 1.3 Security issues in VANET
- 1.4 Existing Security techniques to secure VANET attacks
- 1.5 Drawbacks of Existing Security Techniques
- 1.6 How this Drawbacks can be handled by Block-chain based Decentralized Application

2 Literature Survey
- 2.1 Related work

3 Proposed System
- 3.1 Registration phase
- 3.2 Message dissemination phase
- 3.3 Display chat phase

4 Smart contract
- 4.1 Proposed smart contract
- 4.2 Security analysis of smart contract

5 Result and Discussion
- 5.1 Registration phase
- 5.2 Message dissemination phase
- 5.3 Display chat phase

6 Conclusion

List of Table

2.1 Literature review table

List of Figures

3.1 Registration phase
3.2 Message dissemination phase
3.3 Display chats phase
4.1 Security analysis of smart contract
4.2 Security analysis of smart contract(after update)
5.1.1 Vehicle id cannot be empty
5.1.2: Vehicle already registered
5.2.1: Sender is not registered
5.2.2:Recipient is not registered
5.2.3: Sender & Recipient must be different
5.3.1: Vehicle is not registered

1 Introduction

VANET are created from mobile ad hoc networks, which are networks created from the wireless network of mobile devices. VANET is an architecture for vehicle-to-vehicle and vehicle-to-roadside communications. It offers functions including intelligent car communication, road safety, and navigation, among others.

1.1 Working of VANET

The functioning of VANETs relies on wireless communication technologies to enable seamless interaction among vehicles on the road. In the ad hoc network, every equipped car acts as a mobile node, dynamically connecting to nearby cars to establish a web of connected communication. DSRC or other wireless protocols are commonly used by VANETs to exchange data on road conditions,speed, and location updates. Vehicles can communicate real-time status updates through these data exchanges, which helps the network react as a whole to shifting traffic conditions and possible threats. VANETs can be used to execute cooperative techniques, such as collaborative collision avoidance and platooning, which improve road safety and efficiency.

1.2 Security issues in VANET

- Attacks on Confidentiality: Traditional methods like encryption, access control, and network segmentation are typically used to protect confidentiality. Blockchain and DApps may not be the primary solution for confidentiality-related attacks, as they often involve public and immutable ledgers, making it challenging to protect sensitive information.
- Attacks on Integrity: Message Suppression/Fabrication/Alteration,
  Blockchain and DApps can help ensure the integrity of data by providing an immutable ledger where data cannot be easily altered or fabricated. Smart contracts can also be used to enforce data integrity rules.
- Attacks on Availability: Distributed Denial of Service (DDoS) Attack, While DApps can potentially mitigate DDoS attacks by distributing data and processing across a decentralized network. DDoS attacks can still target specific nodes or services within a blockchain network, affecting availability.

- Spamming: Blockchain networks often have mechanisms to prevent spam transactions, but they are not always foolproof. Spamming can still clog the network and reduce availability.
- GPS Spoofing: GPS spoofing is not typically addressed by blockchain and DApps, as it's a physical attack on the Global Positioning System and not directly related to data security or availability.
- Sybil Attack: Blockchain networks employ consensus mechanisms (e.g., Proof of Work, Proof of Stake) to mitigate Sybil attacks to some extent. However, Sybil attacks can still occur, especially in smaller or less-secure networks.
- Node Impersonation: Blockchain networks use cryptographic keys to authenticate nodes, making it difficult for unauthorized nodes to impersonate legitimate ones. However, the security of these mechanisms depends on the implementation.

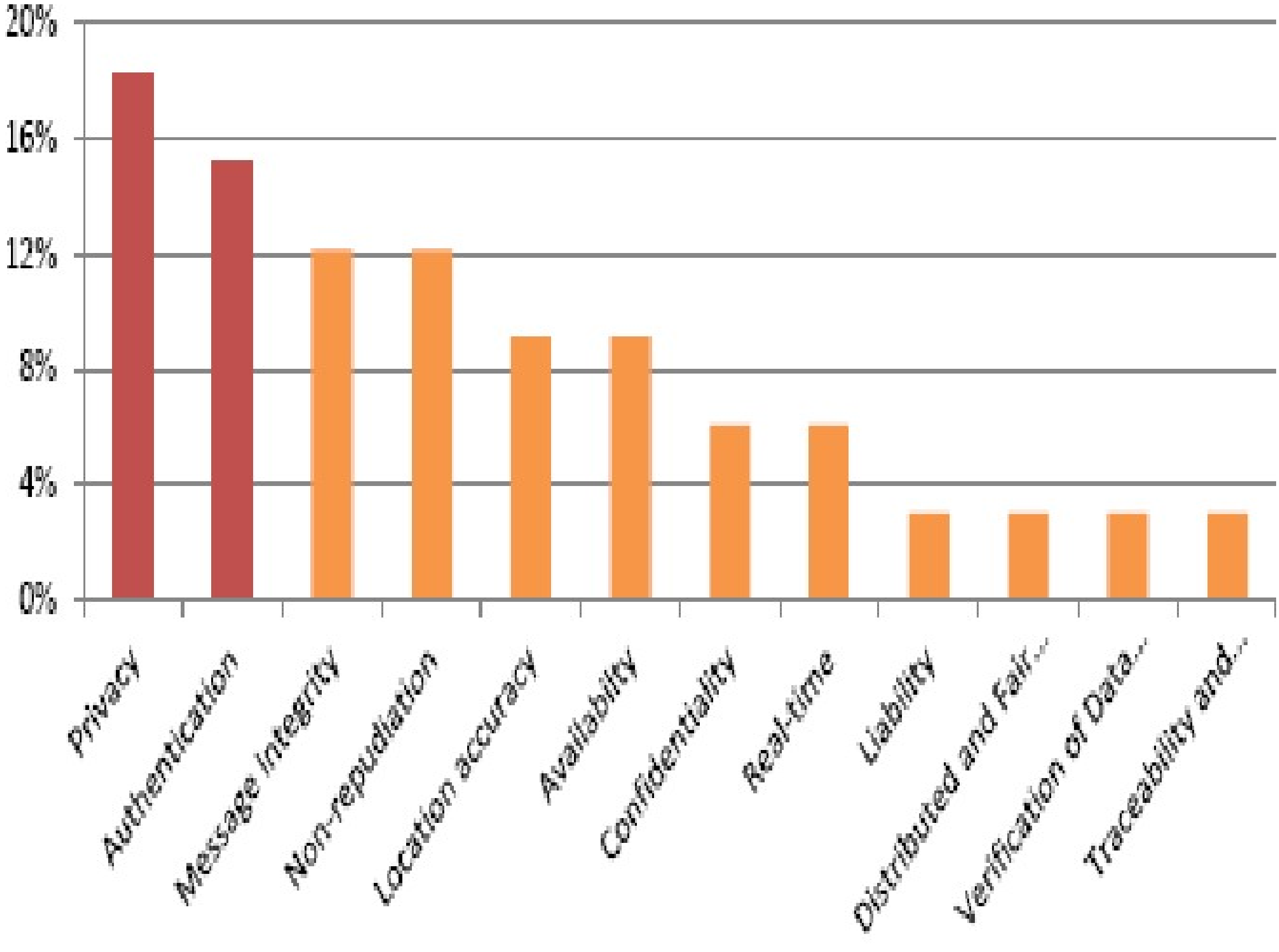

Figure 1.1: VANET security requirements

1.3 Existing Security techniques to secure VANET attacks

VANETs can communicate with infrastructure elements, including roadside devices, to improve traffic control and make it easier to implement intelligent transportation systems. Vehicle Ad-Hoc Networks (VANETs) can be secured using a combination of traditional and advanced safety techniques. Network segmentation, access control, and encryption are commonly employed to prevent privacy invasions and safeguard confidential data. Techniques like digital signatures and message authentication codes are used to confirm the integrity and authenticity of sent messages in order to thwart attacks on data integrity. Furthermore, in real-time security threat identification and mitigation, intrusion detection and prevention systems are essential. These techniques could, however,have disadvantages, including restricted scalability, higher overhead, and susceptibility to complex attacks such as message manipulation.

1.4 Drawbacks of Existing Security Techniques

Certain security techniques are effective, but they have inherent disadvantages that should be taken into account.For example, due to VANETs' dynamic and highly mobile nature, traditional encryption techniques may find it difficult to adjust, which could cause latency and performance problems. Additionally, depending only on centralized security measures may result in single points of failure, increasing the vulnerability of the network to deliberate attacks.Vehicular devices are resource-restricted, which presents a barrier because putting strong security mechanisms in place may tax the devices' low computing and energy capacities.

1.5 How this Drawbacks can be handled by Block-chain based Decentralized Application

The shortcomings of the current VANET security methods may be addressed by blockchain technology. Data integrity and attack resistance are improved by blockchain's introduction of decentralization and immutability. By automating security procedures, smart contracts can lower the chance of human error and the requirement for manual intervention.

Furthermore, because blockchain is decentralized, it is not susceptible to single points of failure, which strengthens the security architecture as a whole. Blockchain technology can offer secure and effective solutions to handle the dynamic and resource-constrained nature of VANETs by utilizing cryptographic concepts and consensus procedures. Blockchain technology solves scalability, decentralization, and automation problems, offering a potential path forward. The use of blockchain technology into VANET security designs has the potential to enhance the security posture of interconnected vehicle networks by creating a more robust and adaptable framework.

2 Literature Survey

2.1 Related work:-

This section gives idea related to work which has been done previously.Literature review table gives summary of the work done during 2011 to 2022:
In paper of IA Sumra et al.(2011), They focuses on enhancing security in VANET, crucial for safety applications.It introduces five classes of attacks within the VANETenvironment, aiming to classify and identify diverse threats.The paper’s significant contribution lies in proposing solutions for the classification and identification of attacks, addressing the growing concerns in the field of automotive and wireless communication security.

In paper of MAH Al Junail et al.(2018), The vital task of protecting VANET(VANETs), which are essential to the Intelligent Transport System (ITS), is examined in this study. It assesses security concerns, talks about difficulties, and compares security needs, possible assaults, and attacker capa-bilities in the context of the VANET. The goal of the research is to provide insights for resolving vulnerabilities that are inherent in VANETs’ special characteristics.

In paper of AA Khan et al.(2022), The study addresses issues with centralised systems by pre-senting a safe lifecycle for networks of unmanned aerial vehicles (UAVs) that makes use of blockchain hyperledger technology.’B-UV2X,’ a consortium structure based on blockchain technology, and a modular infrastructure for Vehicle-to-Everything (V2X) are presented.These components providesafe and transparent communication between connected cars in smart cities.In comparison to cen-tralised systems, simulation findings show decreased network consumption, enhanced security features,and improved computational load efficiency.

In paper of N Dhamani et al(2022),A decentralised web application (DApp) called ”Welcome Wag-gons” allows users to reserve cars securely online by leveraging blockchain technology. It lets driverscharge for their services and get paid, and it lets passengers hail rides.Advanced tools like Tail-wind CSS, Firebase, React JS, Next JS, and Blockchain web3.0 are used in the development of the application to improve the efficiency and security of online automobile reservation services.

Sr No.	Author	Year	Objective	Pros	Cons
1	IA Sumra *et al.*	2011	Proposing a classification system for identifying different classes of attacks in VANETs.	Enhances understanding and addresses security challenges in VANETs, providing a framework for classifying and identifying attacks.	limitations in applicability and coverage may arise based on specific VANETscenarios and evolving attack methodologies.
2	MAH Al Junaid *et al.*	2018	Evaluate and address security challenges in VANETs.	Comprehensive analysis of VANETsecurity issues and a comparative review of security requirements, attack types, and attacker capabilities.	Potential limitations in depth due to the broad scope of issues covered.
3	AA Khan *et al.*	2022	Introducing a secure blockchain-enabled lifecycle for UAV-assisted vehicle networks to enhance communication and address challenges in centralized systems.	Offers transparency, increased security, and reduced network consumption, with improved computational load efficiency in UAV-assisted vehicle communication.	Potential challenges in real-world implementation, scalability and effectiveness may be context-dependent.
4	N Dhamani *et al.*	2022	Developing a decentralized web application (DApp) named "Welcome Wagons"for secure car booking using blockchain technology.	Enhances security for online transactions, provides a decentralized platform for passengers and drivers, and utilizes advanced tools for efficient web application development.	challenges in real-world adoption and scalability, and reliance on blockchain technology may introduce complexities.
5	S Narayan *et al.*	2022	Implementing a blockchain and IPFS-based data storage solution for Vehicular Ad HocNetworks.	Enhances data security and accessibility in VANETs, leveraging the decentralized and immutable nature of blockchain and the distributed file system capabilities of IPFS.	Implementation complexity and scalability, requiring careful consideration of VANET-specific requirements and constraints.
6	H Feng et al.	2022	Implementing blockchain in Digital Twins-based vehicle management for VANETs to enhance intelligent transportation in smart cities.	Improves traffic situation mapping using Digital Twins, ensures secure and efficient storage and transmission of vehicle data through blockchain and achieves high network security with low latency in the in-vehicle self -organizing network model.	complexity of integrating Digital Twins and blockchain, and the need for careful consideration of real-world scalability and implementation.

Table 2.1: Literature review table

Proposed System

3.1 Registration Phase:

In this registration phase, the foundation of the registration module of the blockchain-based vehicle management system is the registerVehicle function, which gives users a safe way to enroll their vehicles. With the need of ID, location, speed, and heading, among other necessary information, the function guarantees a complete image of every registered vehicle, which is stored in the registeredVehicles mapping along with a timestamp for historical context. In order to protect the system's integrity and deter pointless registrations, a payable condition is added that requires an ether payment that is bigger than zero. An additional layer of economic deterrence against unauthorized or superfluous registrations is added by this financial commitment. By carefully examining IDs and current registrations, as well as storing data in an organized manner and using time markers, the registration module creates a framework that is transparent, responsible, and financially viable for incorporating vehicles into the blockchain.(Figure-3.1)

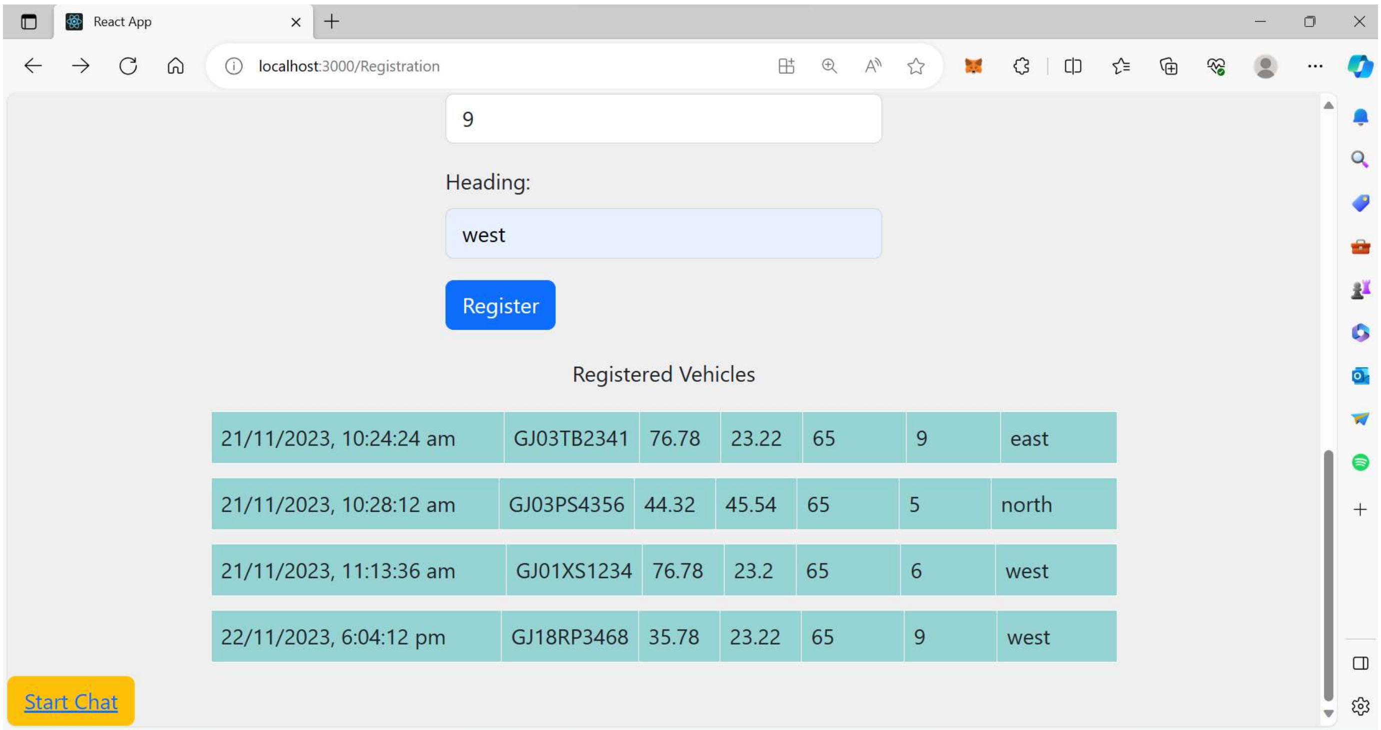

Figure 3.1: Registration phase

3.2 Message Dissemination Phase:

In message dissemination phase,A key component of the blockchain-based vehicle management system's messaging application is the sendMessage feature, which facilitates safe and rewarding communication between registered cars. In order to start a message transmission, the sender must include an ether payment in the transaction. This adds a business element to the communication and deters spam and pointless messages. Important information is recorded by the function, such as the sender and recipient's contact details, the message's content, and the location linked to the exchange. The memos array then contains this data, generating an extensive and unchangeable log of all messages sent and received within the system. In addition, the programme makes sure that the message is visible to both the sender and the recipient at the same time by adding it to both their sentMessages and receivedMessages arrays. In addition to providing both parties with an open record of their communication history, this dual storage strategy makes it simple to retrieve messages for later use. The decentralized and transparent character of the blockchain-based vehicle management system is in line with the messaging application's integrity, security, and accountability, which are enhanced by the payment feature and the methodical message data storage.(Figure-3.2)

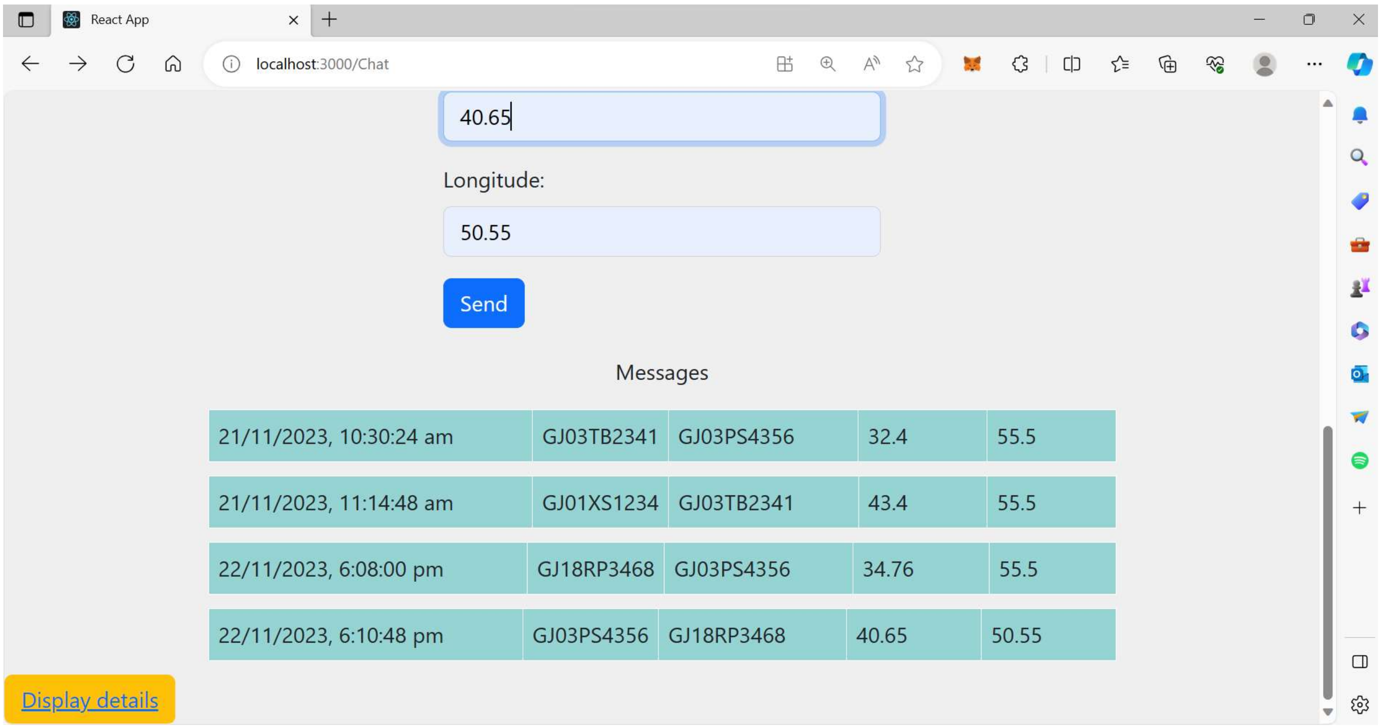

Figure 3.2:Message dissemination phase

3.3 Display Chats Phase:

In this display message phase, features provide customers with an informative and intuitive interface for accessing their communication history. Two important features are launched by the system when a user enters their vehicle ID into the display message portal: getSentMessages and getReceivedMessages. The getSentMessages function first checks to see if the vehicle ID supplied matches one that is registered. The function obtains and presents an extensive list of messages delivered by that specific car, provided that it is registered. This gives the user an open record of all their outgoing messages, complete with timestamps, recipient information, and message content. Similar to this, before getting and displaying an extensive list of messages that the user's vehicle has received, the getReceivedMessages method verifies that the registered vehicle ID is legitimate. This dual functionality allows users to effortlessly access and review both sides of their communication interactions within the system. Vehicle registration gives an extra degree of protection and keeps communication records safe from illegal access. In general, the display message portal promotes accountability and transparency within the blockchain-based vehicle management system by providing users with an easy-to-use and safe way to learn about the messaging history of their vehicle. (Figure-3.3)

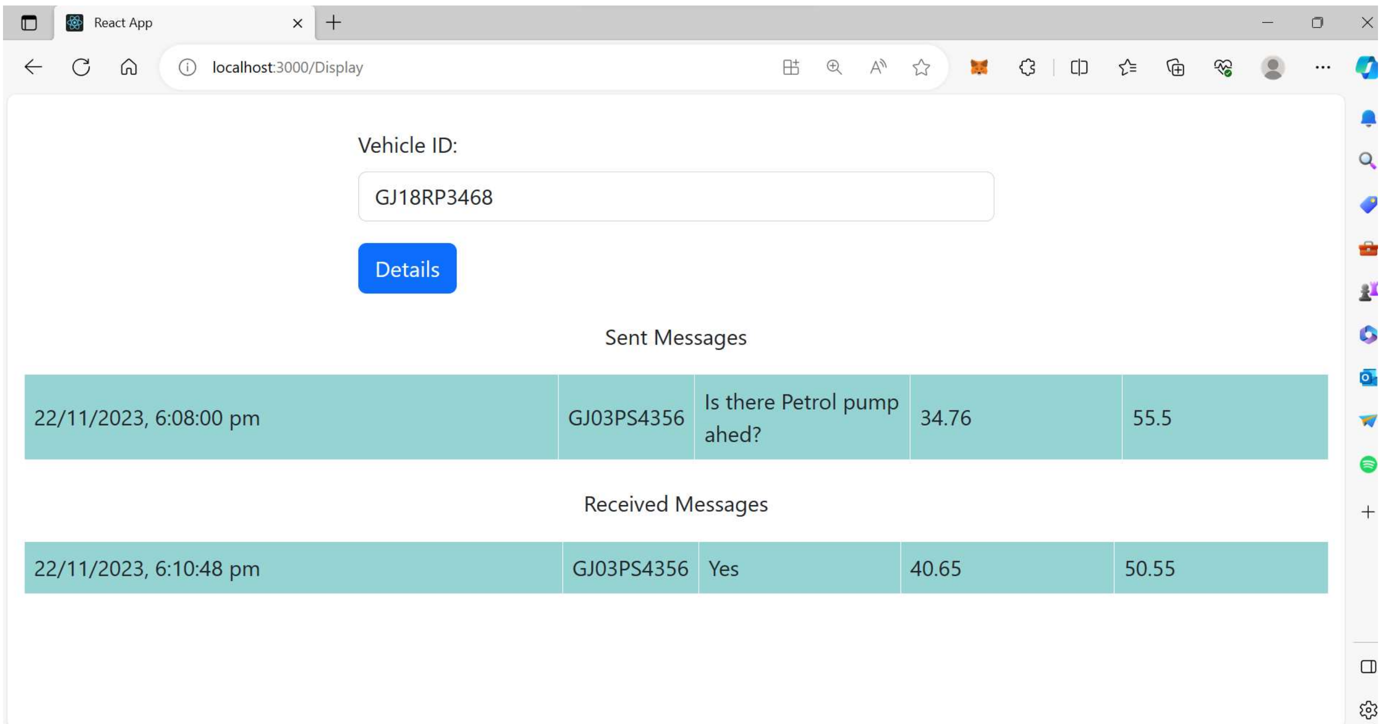

Figure 3.3:Display chats phase

4. Smart Contract

4.1 Proposed Smart Contract

The below smart contract is responsible for all backend processes like checking constraints, storing registered vehicle-data and communication history.

Contract:

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.5.0 <0.9.0;

contract vanet {
    struct Register {
        uint256 timestamp;
        string vehicle; //id
        string x;
        string y;
        string speed;
        string acc;
        string heading;
        //address from;
        bool isRegistered;
    }
    struct Message{
        string sender;
        string recipient;
        string _message;
        string latitude;
        string longitude;
        uint256 timestamp;
    }
    mapping(string => Register) public registeredVehicles;
    mapping(string => Message[]) public sentMessages;
    mapping(string => Message[]) public receivedMessages;
    Register[] reg;
    Message[] memos;
    address payable owner;

    constructor() payable{
        owner = payable(msg.sender);
    }
```

```
    function registerVehicle(
        string memory vehicle,
        string memory x,
        string memory y,
        string memory speed,
        string memory acc,
        string memory heading
        ) external payable {
        require(msg.value > 0, "No ether sent");
        require(bytes(vehicle).length > 0, "Empty vehicle ID");
        require(!registeredVehicles[vehicle].isRegistered, "Already registered");
        owner.transfer(msg.value);
        reg.push(Register(block.timestamp,vehicle,x,y,speed,acc,heading,true));
        registeredVehicles[vehicle] = Register(
            block.timestamp,
            vehicle,
            x,
            y,
            speed,
            acc,
            heading,
            true
            );
    }

    function getVehicles() external view returns (Register[] memory) {
        return reg;
    }

    function sendMessage(
        string memory sender,
        string memory recipient,
        string memory _message,
        string memory latitude,
        string memory longitude
        ) external payable {
        require(msg.value > 0, "No ether sent");
        require(registeredVehicles[sender].isRegistered, "Sender not registered");
        require(registeredVehicles[recipient].isRegistered, "Recipient not registered");
        require(keccak256(abi.encodePacked(sender)) != keccak256(abi.encodePacked(recipient)),
"Recipient & Sender must differ");
        //require(sender != recipient, "Sender and Recipient must be different.");
        Message memory message = Message(
            sender,
```

```
            recipient,
            _message,
            latitude,
            longitude,
            block.timestamp
            );
        memos.push(message);
        sentMessages[sender].push(message);
        receivedMessages[recipient].push(message);
    }

    function getSentMessages(string memory user) public view returns (Message[] memory) {
        require(registeredVehicles[user].isRegistered, "Vehicle not registered");
        return sentMessages[user];
    }

    function getReceivedMessages(string memory user) public view returns (Message[] memory) {
        require(registeredVehicles[user].isRegistered, "Vehicle not registered");
        return receivedMessages[user];
    }

    function getMemos() public view returns (Message[] memory) {
        return memos;
    }
}
```

4.2 Security Analysis of Smart Contract

Security analysis of smart contracts is required to check the security of smart contracts. So, we have used the'solidityscan' online tool to check the security of our smart contract. Initially, our smart contract had a security score of 44.44%, which is low. This contract has 2 high, 5 low, 12 info, and 10 gas related threads.

The list of threads includes reentrancy, use of floating point pragma, variables that should be immutable, missing state variable visibility, defining constructor as payable, functions that should be external, long strings, etc. (Figure 4.1)

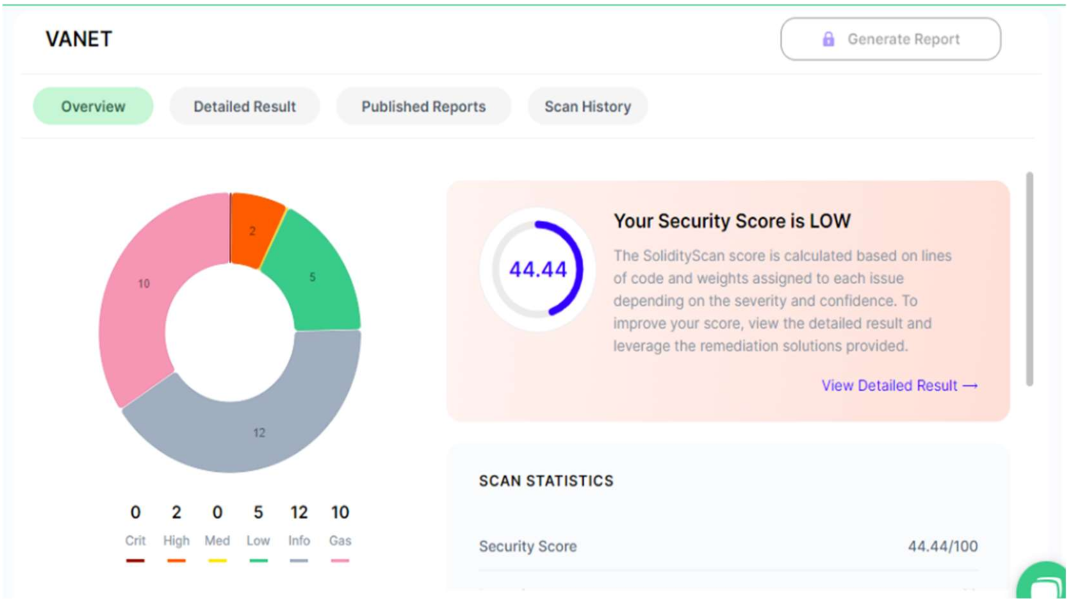

Figure 4.1: Security analysis of smart contract

After that, we made some changes, like declaring the constructor as payable, changing the function type to external, and shortening the revert strings. After updating the smart contract, we were able to solve issues and increase the security of the smart contract, so now we have only 1 high, 5 low, 11 info, and 5 gas related issues and are able to achieve a security score of 70.59%. (Figure 4.2)

Figure 4.2:Security analysis of smart Contract (After Update)

5. Result And Discussion

5.1 Registration Phase

The registration portal is used to register vehicles in the network. (Figure-3.1) depicts a snapshot of the registration phase. This module has some constraints, like that the vehicle ID cannot be empty (Figure-5.1.1) and registered vehicles cannot register again. (Figure-5.1.2)

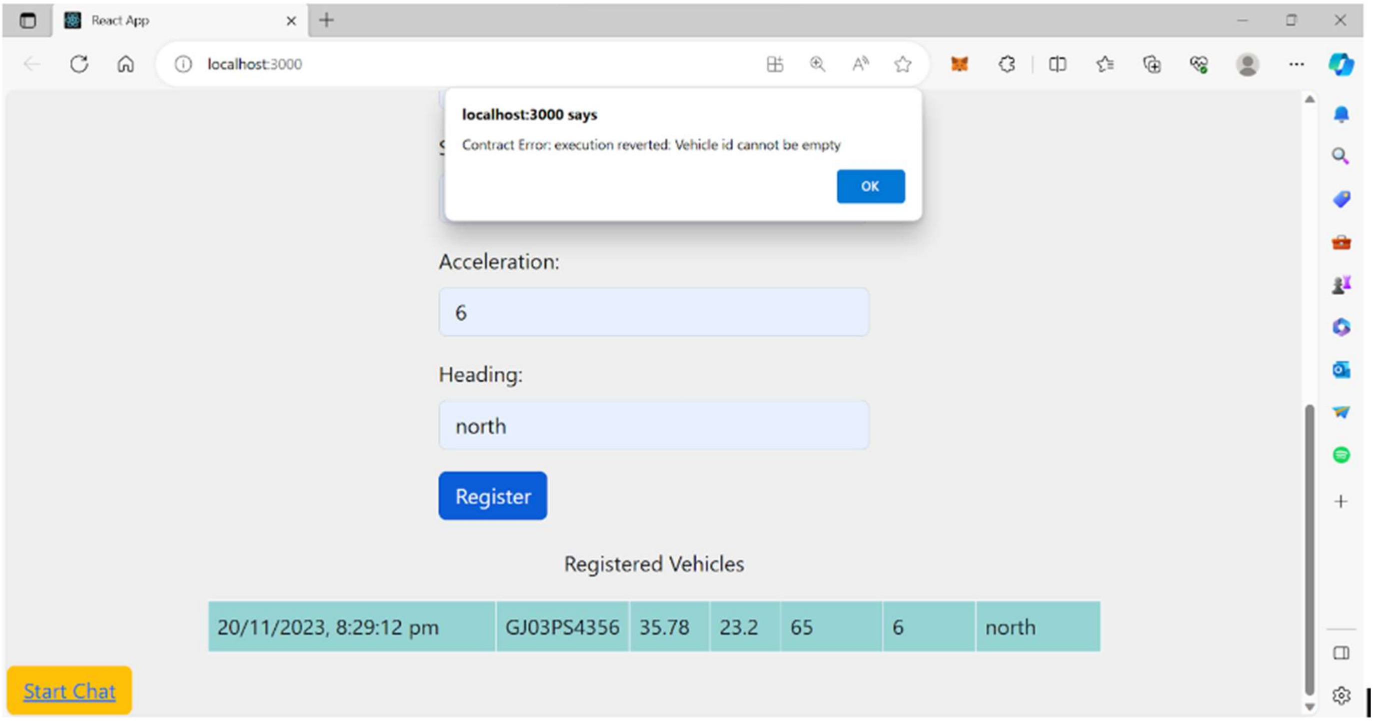

Figure 5.1.1: The vehicle ID cannot be

empty

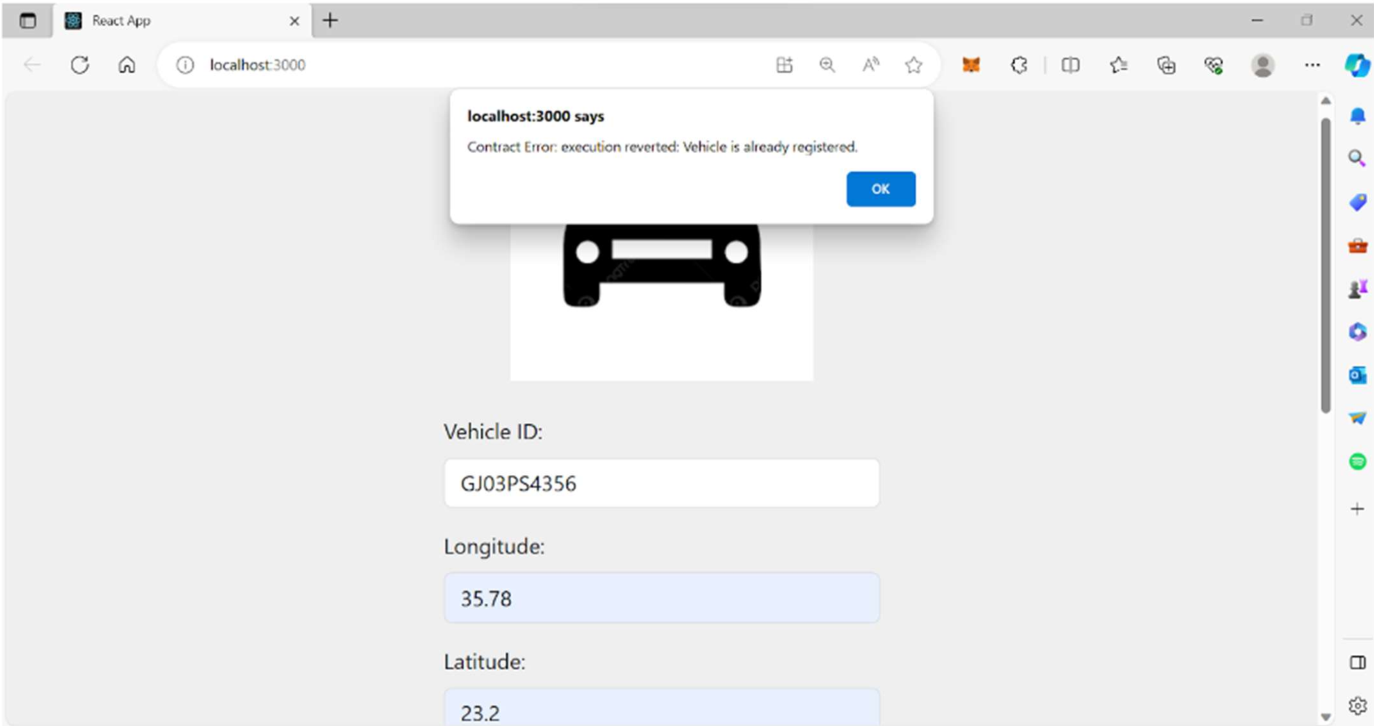

Figure 5.1.2: Vehicle already registered

5.2 Message dissemination phase

A messaging portal is used to communicate with other registered vehicles in the network (Figure-3.2). This module has some constraints, like the sender vehicle (Figure-5.2.1) and the register vehicle (Figure-5.2.2) must be registered and different (Figure-5.2.3).

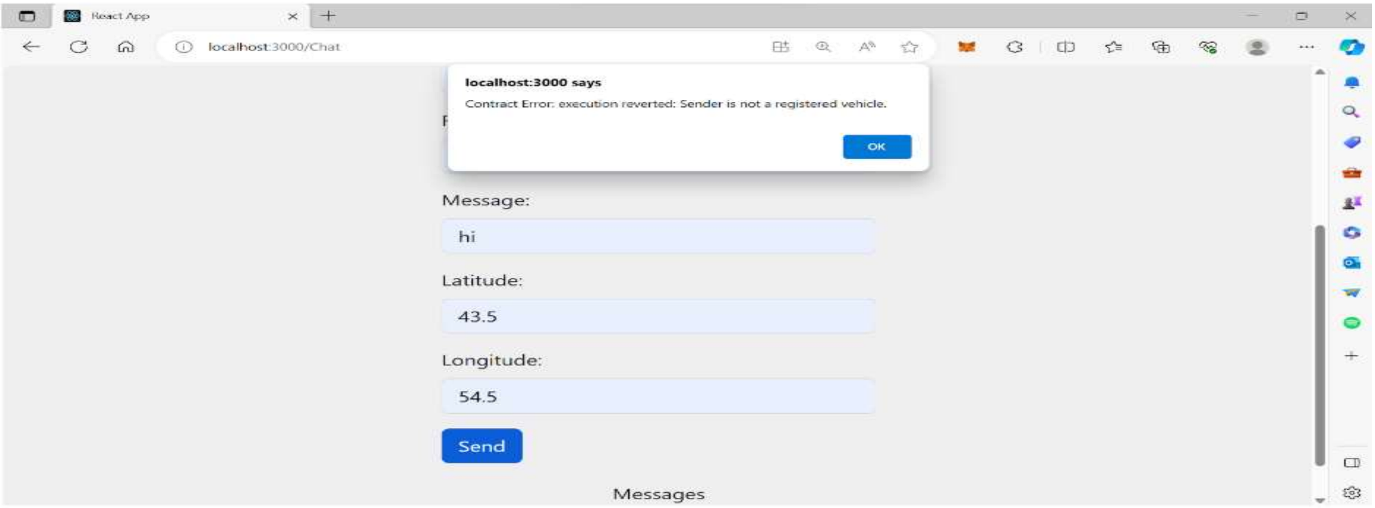

Figure 5.2.1: Sender is not registered

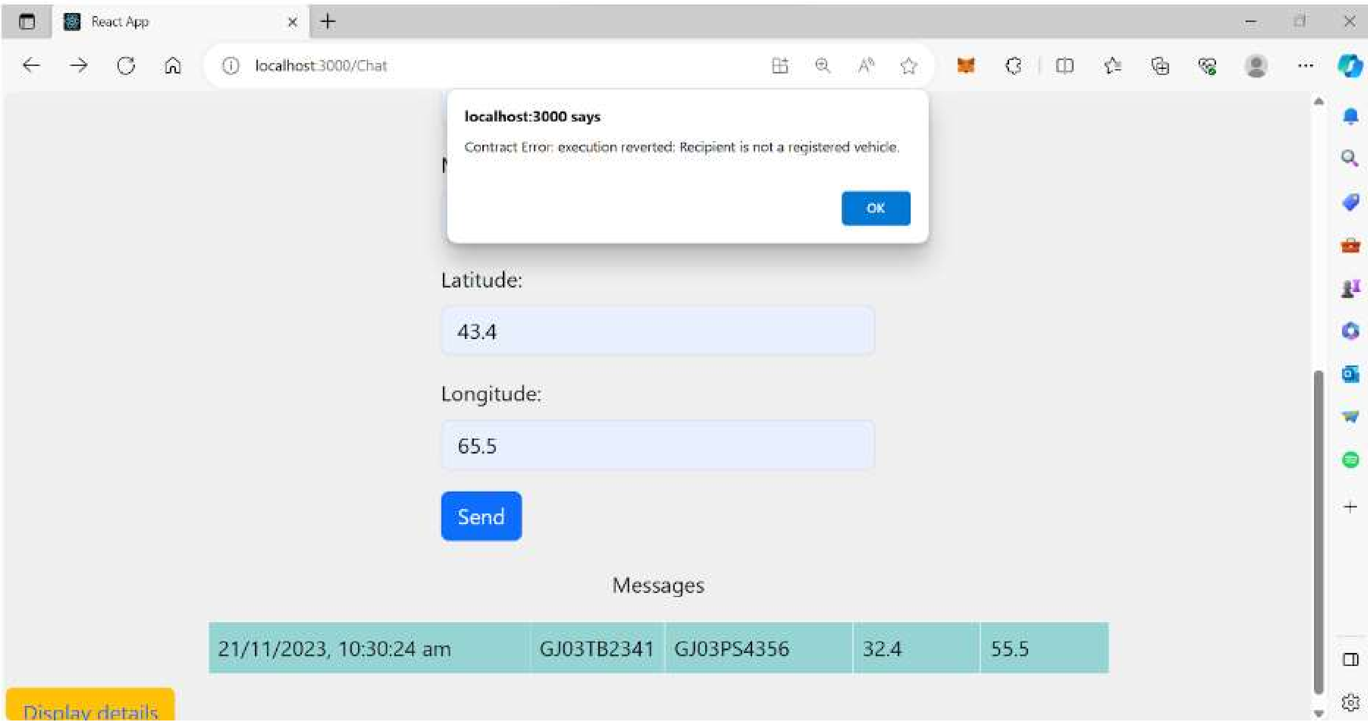

Figure 5.2.2:Recipient is not registered

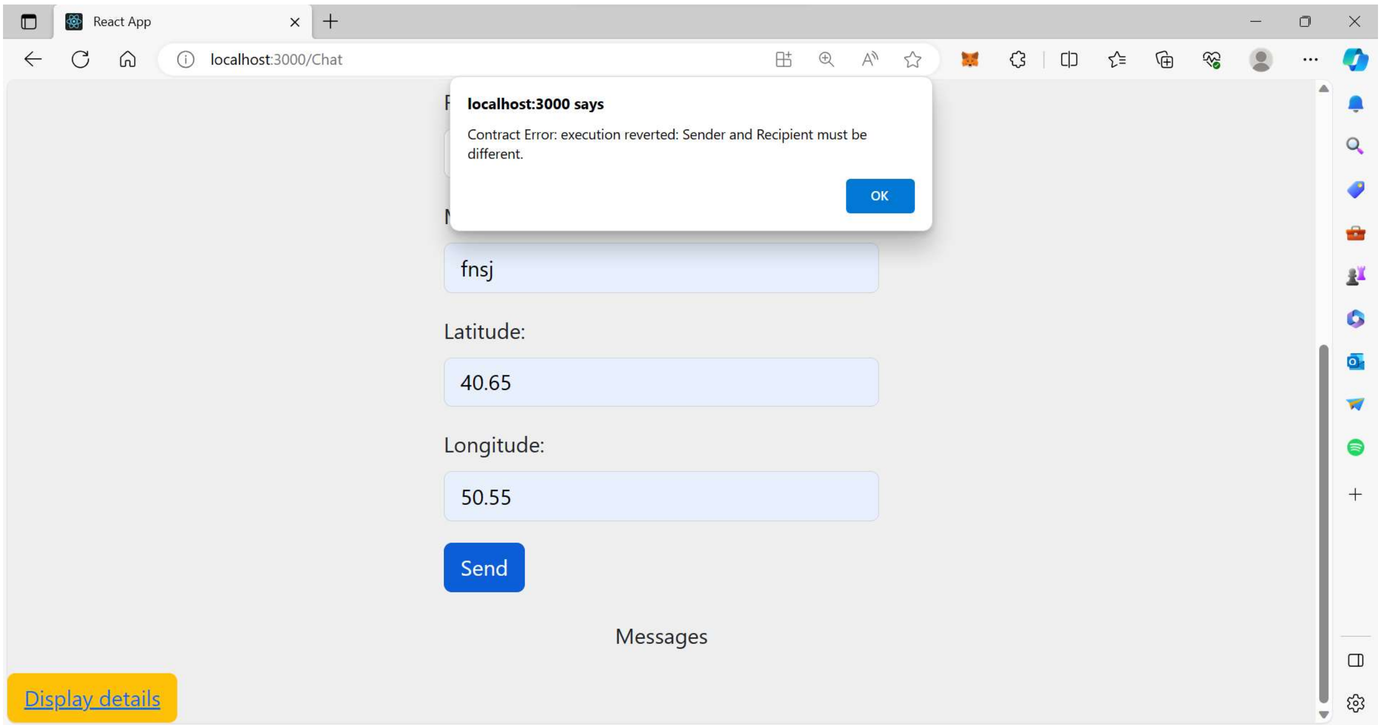

Figure 5.2.3: Sender & Recipient must be different

5.3 Display chat phase

A display chat phase is used to see all communication done by the vehicle. It will display all messages that are sent by and received by the vehicle (Figure 3.3). It has constraint that vehicle must be registered (Figure 5.3.1).

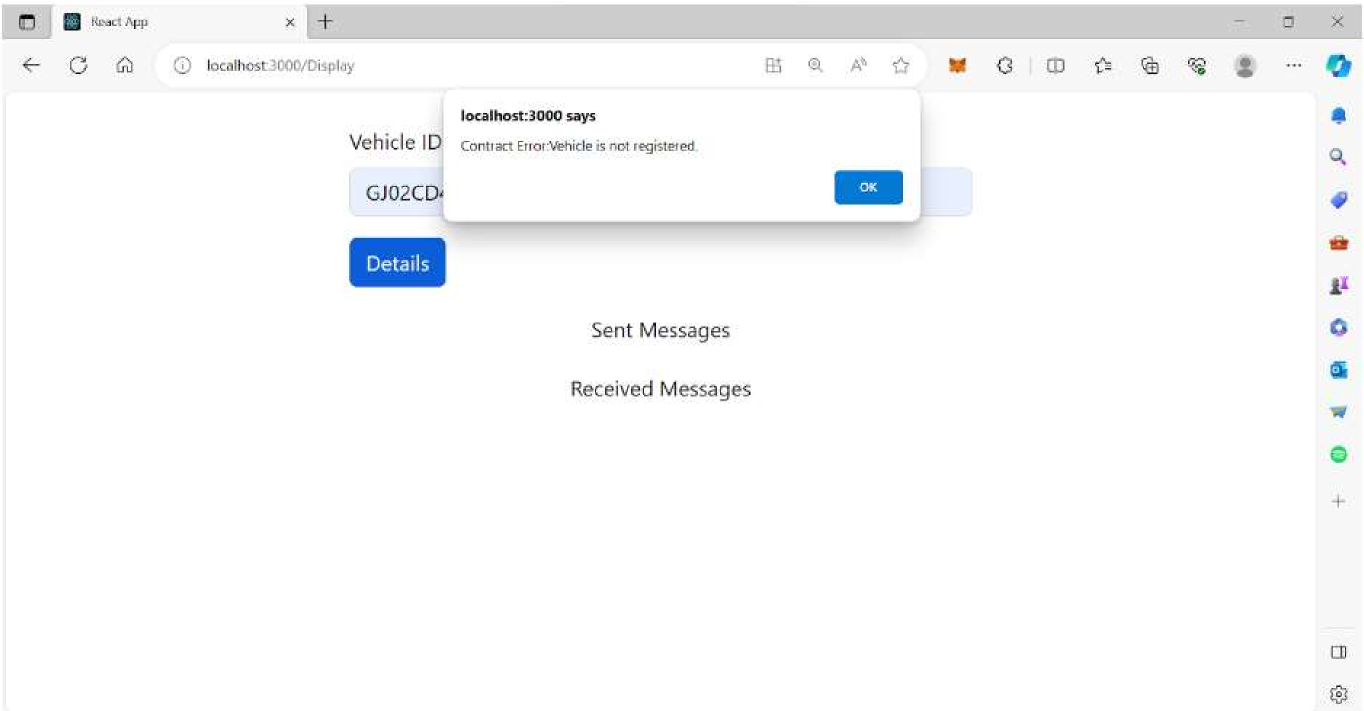

Figure:5.3.1: Vehicle is not registered

6. Conclusion:

We have proposed a Blockchain based Decentralized application for vehicular Ad-hoc networks, in which we have included registration, message and display chat phases. By this application, we have achieved security, decentralization of data, data transparency and auditability, immutability and trustless transactions.

References

[1] Sumra, Irshad Ahmed, Iftikhar Ahmad, and Halabi Hasbullah. "Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET)." 2011 3rd international congress on ultra modern telecommunications and control systems and workshops (ICUMT). IEEE, 2011.

[2] Al Junaid, Mohammed Ali Hezam, \textit{et al}. "Classification of security attacks in VANET: A review of requirements and perspectives." MATEC web of conferences. Vol. 150. EDP Sciences, 2018.

[3] Khan, Abdullah Ayub, \textit{et al}. "Vehicle to everything (V2X) and edge computing: A secure lifecycle for UAV-assisted vehicle network and offloading with blockchain." Drones 6.12 (2022): 377.

[4] Dahmani, Nadia, \textit{et al}. "Welcome Wagons: A Block Chain based Web Application for Car Booking." 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2022.

[5] Narayan, Sangeeta, \textit{et al}. "Blockchain and IPFS-based Data Storage for VANET." 2022 13th International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2022.

[6] Feng, Hailin, Dongliang Chen, and Zhihan Lv. "Blockchain in digital twins-based vehicle management in VANETs." IEEE Transactions on Intelligent Transportation Systems 23.10 (2022): 19613-19623.

[7] Mir, Farooq Ahmad, and Mohamad Tariq Banday. "Control of Spam: A Comparative Approach with special reference to India." Information & Communications Technology Law 19.1 (2010): 27-59.

[8] Rehman, Sabih-Ur, et al. "Vehicular ad-hoc networks (VANETs): an overview and challenges." Journal of Wireless Networking and communications 3.3 (2013): 29-38.

[9] Mohammad, Sajjad Akbar, Asim Rasheed, and Amir Qayyum. "VANET architectures and protocol stacks: a survey." Communication Technologies for Vehicles: Third International Workshop, Nets4Cars/Nets4Trains 2011, Oberpfaffenhofen, Germany, March 23-24, 2011. Proceedings 3. Springer Berlin Heidelberg, 2011.

[10] Mishra, Rashmi, Akhilesh Singh, and Rakesh Kumar. "VANET security: Issues, challenges and solutions." 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT). IEEE, 2016.

[11] Sharma, Sparsh, et al. "A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions." International Journal of Communication Systems 34.14 (2021): e4905.

[12] Inedjaren, Youssef, et al. "Blockchain-based distributed management system for trust in VANET." Vehicular Communications 30 (2021): 100350.

[13] Ma, Zhuo, et al. "An efficient decentralized key management mechanism for VANET with blockchain." IEEE Transactions on Vehicular Technology 69.6 (2020): 5836-5849.

[14] Nema, Megha et al. “Analysis of Attacks and Challenges in VANET.” (2014).

[15] Yang, Chengjun, et al. "Edge Computing-Based VANETs’ Anonymous Message Authentication." *Symmetry* 14.12 (2022): 2662.

Prof. Umesh Bodkhe

DAPP VANET

nov2020

nov2020

Institute of Technology, Nirma University

Document Details

Submission ID

trn:oid:::1:2776061409

Submission Date

Dec 7, 2023, 4:48 PM GMT+5:30

Download Date

Dec 7, 2023, 4:52 PM GMT+5:30

File Name

Minor_Project_report.docx.pdf

File Size

1.3 MB

27 Pages

3,544 Words

21,434 Characters

How much of this submission has been generated by AI?

***12%**

of qualifying text in this submission has been determined to be generated by AI.

* Low scores have a higher likelihood of false positives.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?

The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.

How does Turnitin's indicator address false positives?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?

Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.