UTS UNIVERSITY OF TECHNOLOGY SYDNEY

# Blockchain Based Security for Vehicular Ad hoc Networks

**by Nisha Malik**

*A dissertation submitted in fulfilment of the requirements for the degree of*

**Doctor of Philosophy**

*in*

**Computer Systems**

*Under the supervision of*

**Dr. Priyadarsi Nanda**

University of Technology Sydney

**Faculty of Engineering and Information Technology**

**August 2020**

# Certificate of Original Authorship

I, *Nisha Malik* declare that this thesis is submitted in fulfilment of the requirements for the award of *Doctor of Philosophy*, in the *School of Electrical and Data Engineering, Faculty of Engineering and Technology* at the *University of Technology Sydney, Australia*.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.

**Signature of Student:**

**Date:** 31/08/2020
**Place:** Sydney, Australia

# *Dedicated To*

*My Loving Parents and Parent- In- Laws*

*My extremely supportive husband Deepak*

*My loving daughter Laavanya*

*My Crazy brother Sumit*

*My Motivating Teachers and Mentors*

*My Amazingly Creative and Crazy Friends*

# *And to Everyone Who Reads This*

# Acknowledgements

Foremost I would like to thank and express my sincere gratitude to Almighty God, the sustainer, who kept me going through the highs and lows of this journey and made it achievable for me. He undoubtly is the source of light for me in every aspect of life.

I would like to express my deepest gratitude to my supervisor, Dr. Priyadarsi Nanda for accepting me into the Ph.D. program and guiding me all the way through in this journey of becoming a successful researcher. Dr. Nanda's guidance, patience, and continuous support were essential to the completion of this thesis. His unmatched knowledge and invaluable feedback immensely helped me go forward in my research. I am greatly indebted to him for helping me get through the difficult times I had during my research. I feel very lucky to have worked with Dr. Nanda without whom this thesis would have only been a dream. I would like to thank my Co-supervisor Professor Xiangjian He, who always provided his valuable and expert feedback on my work. His support, co-operation, and generosity throughout the research tenure is truly undeniable. Further, I would like to express my deepest gratitude to Professor Ren Ping Liu, who guided through the NSW Cyber Security Project, which forms an essential part of this research work.

I also wish to thank all of my colleagues and friends from the School of Electrical and Data Engineering at the University of Technology Sydney. Specifically, I would like to thank Dr. Deepak Puthal, Ambar, Ashish, Upasana, Annie, and Amjad for creating a friendly atmosphere in the group and assisting me in whatever manner possible. Many thanks to all the administrative staff at the School of Electrical and Data Engineering, especially Thomas, Eryani and Aprillia who helped me with administrative issues.

I am eternally grateful to my loving and supportive husband Deepak Malik, lovely daughter Laavanya, beloved parents Ashok Kumar Saroha and Krishna Saroha and parents in law Dharampal Malik and Sudesh Malik, my brother Sumit Saroha for their sacrifices, prayers, encouragements, and endless love. Without their everyday support, I would have not been able to reach this stage. I sincerely dedicate this thesis to them. Words cannot express my gratitude and appreciation for their unwavering support and kindness throughout this journey.

# Abstract

*The speedy aggrandizement in Wireless communication technologies concurrently with immediate measure requisites to improve road safety have expedited a considerable development in the Intelligent Transportation Systems (ITS). ITS came into existence with a strong perspective to provide end-to-end, better, worthier, safer, efficient and much more improved transport services, both on-road and off-road. Intelligent communication technologies such as trip guiding smart phone applications (that direct you how much to walk before you take the next bus or train, where to get down, etc.), the latest safety oriented in vehicle systems (such as Anti-Lock Braking systems, air bags, Navigation systems, etc.), are all part of the ITS.*

*Therefore, ITS is not just about modifying or repairing the age-old infrastructures of roads, highways, stations, or bus stops, but persuading security and safety of transport to all the people and goods travelling on roads.*

*With increasing congestion increased the accidents, which made the government authorities, and the automobile manufacturers realize the need and embryonic benefits that can be exploited by means of wireless communications merged with in-vehicular capabilities, consequently, resulting in the formation of Vehicular communication networks termed as* ***'Vehicular Ad hoc Networks'*** *(VANETS).*

*VANETS are therefore, an emerging promising technology of the ITS due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. Vehicle-to-Vehicle (V2V) communications rely on what is called as the DSRC (Dedicated Short-Range Communications). A vehicle periodically broadcasts its position, speed, ID/Pseudo-ID, direction, etc. to other neighboring vehicles at 1-10Hz. These messages are called as Cooperative safety messages or beacon messages. The aim for all these vehicular applications is the ultimate driver assistance and safety to avoid any discomfort and mis happenings. Therefore, to ensure that only accurate alerts, warnings, or messages reach the drivers, without any false data injections or message alterations, security implementations are essential. If attackers send any false warning alerts, say for e.g. Impersonating an authorized user attacker broadcasts an accident alert in his area, it can cause unnecessary havoc among the road users and route diversions which were not required. Also, the authentication of the network users along with privacy perseverance is the most important security consideration. Therefore, security implementation is the foremost necessity in VANETs.*

*In VANETS, information is widely available across multiple systems and is accessible with appropriate authentication and access rights. But, to have access, users need to connect in the wireless environment, which poses various security*

*challenges. This thesis investigates the security challenges and limitations to secure VANET and how the existing solutions can be improved upon. Blockchain has emerged as the solution to securing identity and authentication along with access control among the network entities.*

*This thesis is a work to secure the VANET network, by authenticating, revocating, and establishing trust among the users using the shared Blockchain Ledger, to enable them to get emergency updates and transmit only if they are authorized users, while they travel on road. This work identifies the trustworthy nodes using blockchain and smart contracts and store their reputation in the Inter Planetary File System (IPFS) storage in a transparent manner, so the reputation score is available to all the nodes without relying on the centralized infrastructure for computation or storage. The thesis provides a detailed review of existing trust and privacy works and merges the neural networks with blockchain to provide the classification of trustworthy nodes as well as providing privacy to the data, by sanitizing the data prior to transmission. The thesis is a work to secure communication in the network to provide end-end security. The proposed model guarantees privacy and security to the information transmitted and multi-level trust evaluation of the nodes before sharing any information. The thesis is divided in three phases of research with blockchain and smart contracts finally demonstrating that our solutions not only strengthen and secure the dynamic VANET, but also significantly improve the performance and efficiency as compared to existing approaches.*

# Author's Publications

1. **Nisha Malik**, Deepak Puthal, and Priyadarsi Nanda, "An overview of security challenges in vehicular ad-hoc networks," in *2017 International Conference on Information Technology (ICIT)*, 2017: IEEE, pp. 208-213.

2. **Nisha Malik**, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 674-679.

3. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, "Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019: IEEE, pp. 34-41.

4. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu, "Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology," *Wireless Networks,* pp. 1-20, 2020.

5. **Nisha Malik**, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu "A Systematic Analysis of Security and Trust Management in Vehicular Networks" (Submitted to Computer Networks).

6. Deepak Puthal, **Nisha Malik**, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine,* vol. 7, no. 2, pp. 18-21, 2018.

7. Deepak Puthal, **Nisha Malik**, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine,* vol. 7, no. 4, pp. 6-14, 2018.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1. Overview

Intelligent Transportation Systems (ITS) came into existence with a strong perspective to provide end-to-end, better, worthier, safer, efficient, and much more improved transport services, both on-road and off-road. Intelligent communication technologies such as trip guiding smart phone applications (that direct you how much to walk before you take the next bus or train, where to get down, etc.), the latest safety oriented in vehicle systems (such as Anti-Lock Braking systems, air bags, Navigation systems, etc.), are all part of the ITS. Therefore, ITS is not just about modifying or repairing the age-old infrastructures of roads, highways, stations, or bus stops, but persuading security and safety of transport to all the people and goods travelling on roads [1]

Congestion on motorways increased proportionally with the increasing number of automobiles, which made the government authorities, and the automobile manufacturers realize the need and embryonic benefits that can be exploited by means of wireless communications merged with in-vehicular capabilities, consequently, resulting in the formation of Vehicular communication networks termed as ***'Vehicular Ad hoc Networks' (VANET)***.

VANET can be briefly defined as ***"spontaneous, self-configurable networks formed between moving vehicles, where each vehicle serving both as a mobile node and router, is equipped with wireless capabilities (radio antennas, embedded sensors, GPS, etc.) to support short range communications and can communicate wirelessly both with other mobile nodes (vehicles, and pedestrians) as well as established Road Side Infrastructure/units(RSU). The vehicles can proficiently gather, and process surrounding data and transmit the same via messages containing the vehicle's unique identifier, current position, timestamp, and any other safety related data in a timely manner to***

***surrounding vehicles, thereby facilitating safe driving with, real time traffic assistance, accident prevention, and emergency warning among others."***

Although VANET are considered as a use case of MANETS, but there are significant differences between the behaviour and characteristics of the two ad hoc networks. Different mobile platforms (laptops, smartphones, PDAs, etc.) come together in MANETS, and communicate wirelessly either forming an independent network (using Bluetooth, infrared) or may have an interface to a fixed network (such as the Internet). The nodes in MANETS, which serve both as host as well as a router, are equipped with wireless transmitters and receivers and are free to move arbitrarily. VANET inherit most of the MANET characteristics, such as infrastructure less functionality due to lack of central coordinator, self-configuration and management of networks, limited physical layer security, but the high speed of vehicles, adds on some more attributes than just these features, such as more dynamic topology with varying density, but no power constraints as the in-vehicular system is a continuous power source for the vehicular networks.

With numerous advantages, comes the security risks and disadvantages given the open nature of the vehicular communications. Numerous researchers have worked extensively in this direction to resolve the issues and propose solutions, but a concrete end-to end solution is the need of the hour. The use of Pseudonyms, multiple encryption decryption techniques, and other secure means of data transmission and verification have occurred in the last two decades. But all these require a centralized party to work as a trusted intermediary in establishing secure communication between the Road-Side Units (RSUs) and On-Board Units (OBUs).

The cloud servers deployed in the conventional centralized mechanism in VANET serve as an excellent bait for the attackers as a single point of failure leading to certain treacherous situations and disrupting the entire network. Also, the malicious messages from suspicious parties or alteration in genuine messages impact the driver's behavior and can cause mishaps jeopardizing the safety of passengers on road. Lack of privacy and security breaches for instance tracking of a vehicle, impose a restriction on using them for providing personalized services.

To address these network challenges, we require a security framework that provides complete decentralization or reduces the maximum dependency on a centralized party while rendering the primitive security requirements of VANET. This framework should guarantee that the self-sustained and self-organized vehicular network allows not just for easy identification/authentication of the vehicles without any intermediary but also, establishes transparency in the computation of trust and reputation among the communicating nodes, and ensures secured communication by restricting access to only reputed nodes.

In this Chapter we study the major security requirements of VANET and understand the need of moving towards decentralization of the traditional VANET and reducing dependency on a centralized party to achieve these critical

security requirements i.e. authentication and revocation, trust and reputation, secured transmission with access control and key management.
We begin by designing our security requirements, background of the problem, then going down with research questions, research aim, and research objectives followed by our research methodology and research contributions, finally concluding with our thesis organization.

## 1.2. VANET Security Requirements

VANET is a promising technology whose idea has been perceived well by the government authorities, automobile manufactures and the research community for the actualization of ITS, due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. Despite these numerous advantages for safety and driving assistance, it brings along a storm of threats specially targeting the security and privacy aspects, due to the vulnerabilities associated with the openly accessible wireless channel. The bandwidth can easily be hacked to perform various malicious activities such as impersonation, eavesdropping, signal jamming, etc. [2] for user-tracking, proving life threating in most scenarios. Hence for the secure functioning of the network we need to ensure following security requirements:

A. **Confidentiality and Access Control:** Data Confidentiality ensures the message/data contents are revealed only to the authorized individuals and prevented from any undesired and unauthorized disclosure both when the data is stored and when in process of transmission. In VANET confidentiality hails as a primitive requirement achieved by applying certain access control policies and cryptographic mechanisms on the stored and transmitted data. This requirement becomes even more imperative, particularly for the military application of VANET, where information disclosure is not just a security breach, but undoubtedly life threatening.

B. **Integrity:** Integrity of data is validated, if the transmission of data from source to destination occurs with no external (unknown and unauthorized) interference and tampering, and accuracy and reliability of data can be ensured at the destination. In VANET, if a malicious attacker alters the transmitted data pretending to offer safety but can lead to traffic congestions, or unwanted route diversions for drivers.

C. **Availability:** To access the network resources, it is necessary for them to be available when required in a timely manner. Considering stringent delay

requirements of messages in VANET, if unnecessary message transmissions by attackers consumes most of the available bandwidth, it leads to DOS for legitimate users. Thus, how we counter DOS attacks, plays crucial role in network availability for rightful users.

D. **Authentication:** Authentication is the process of identifying network users by means of Unique ID and password/biometrics to grant them authorization for accessing the resources. It is a necessary step in VANET to ensure not only the message received by the recipient has come from an authorized user, by means of the user certificate and signature verification.

E. **Conditional Privacy preservation:** Privacy refers to hiding critical and personal user information from unwanted and unauthorized entities, to ensure safety and security. In VANET, it is necessary to keep user's identity a secret or use frequently changing pseudonymous IDs to avoid location tracking or impersonation. Offering complete privacy is impossible in VANET as the user's identity needs to be revealed and traced in case of emergency scenarios such as any accident enquiry requiring the user's location and personal information. Even in case of Pseudo IDs its necessary to use cryptographic mechanism and ID generators secure but less complex to ease traceability.

F. **Non-Repudiation**: Non-repudiation ensures that when recipient identifies who the sender is, the sender takes complete responsibility and cannot deny sending the message. Digital Signatures included in the message can serve the purpose, to avoid any conflicts in abnormal scenarios.

G. **Trust:** It is emerging as the most important requirement to deliver a successful security framework for VANET. Although we can verify, and authenticate received messages, but considering the number of entities involved and the difference in their backgrounds, we cannot trust them.

## 1.3. Background of the problem

When vehicles begin their travel on road, it is important for them to acquire periodic traffic updates, emergency alerts or be able to access value added services. The infrastructure should uphold the monumental purpose of user safety and security for administering and provisioning these services. This brings us to the scenarios which can prove fatal for the users if not dealt appropriately on time such as an accident emergency, congestion on the road, obstacle detected on road, etc. Also, transmitting notifications and warnings securely to those who are under threat is important.

**Authentication and authorization** of network users with reduced latency is the most essential part considering the dynamic nature of the network and what goes hand in hand is maintaining the privacy of users and not disclosing their actual identity. While other peers are not aware of each other's actual identity under ordinary circumstances, in case, an authenticated user turns malevolent, thus launching an 'insider attack', quick revocation and traceability should be possible without any padded overhead, thus ensuring conditional privacy. Usually, authentication of nodes is done in two steps, first, checking of CRL and second identity verification. Both these steps should be prompt enough to elude any delays.

Next most primitive requirement is transparent **reputation computation and trust establishment** among the nodes. the neighboring vehicles cannot be completely trusted due to the large variability and mobility of vehicular networks, this is considered as a serious issue if network suffers from the existence of multiple malicious vehicles. Hence, as the next step after appropriate authentication we need a trust management scheme [3-5]that not only facilitates the vehicles to decide on the trustworthiness of the received messages, but also aids the network operators to decide on the punishments or rewards on appropriate vehicles. Generally, a vehicle's trust value is evaluated based on its past behavior's ratings produced by pertinent nodes, but several works have considered multiple other factors in estimating a nodes' trustworthiness.

From the VANET security requirements we understand that once we establish an environment of trust among the nodes, we must ensure **secure communication with minimal computational complexity** i.e. eliminating the traditional encryption decryption techniques and by doing so render **access control** of any transmission to trusted and reputed nodes only.

Now, as we discussed that in the current approaches the central authority is responsible for the security measures in traditional approaches. This induces opacity in the network and causes latency due to bandwidth consumption in too much of back and forth communication to the central authority by so many vehicles on road.

With the launch of Bitcoin blockchain in 2008, the focus of industry and academia shifted towards approaches which could secure the way centralized networks operated. From then on, some researches in VANET focused on methodologies to improve efficiency, guaranteeing privacy and security using the blockchain technology. After the introduction of autonomous/self-driving vehicles on the road for which efficient and timely communication amongst the nodes is of utmost importance, researchers explored the use of sensing and signalling devices using blockchain public key infrastructure and an inter-vehicle session key establishment protocol. Although, the technological revolution brought by blockchain also imposes certain new challenges like poor scalability, high computational costs due to mining, high bandwidth, and storage requirements, we plan to address the issues discussed above in VANET using this

technology and propose a security framework that leverages the advantages of blockchain and provides security in the network.

## 1.4. Research Questions

Based upon the essential security requirements and the background of the problem, we framed the following research questions which we have addressed as a part of this thesis.

***Q1. How to identify if messages are indeed coming from an authenticated source?***

***Q2. How to identify security breaches by previously authenticated nodes, already part of the network?***

***Q3. How to classify a node sending/receiving information as trustworthy or malicious?***

***Q4. How to compute a node's reputation without relying on a trusted party and thus providing transparent and valid reputation score?***

***Q5. How can the privacy of the users be ensured along with valid authentication (conditional privacy preservation)?***

***Q6. How to ensure secured message transmission with minimal computation?***

***Q7. How to manage the key used for the sanitization process to prevent data leakage and unwanted access?***

***Q8. How to have an optimal key for the sanitization process which ensures maximum sensitive data sanitization with minimal key size?***

***Q9. How to provide access control and ensure data transmitted by a sender node is only accessible to other trustworthy nodes?***

## 1.5. Research Aim

The main and principal aim of the research was to investigate new framework for establishing decentralized security in the VANET network for authentication, revocation, trust, and privacy. The whole purpose of the research was to identify the security threats in the existing schemes, overcome the disadvantages of centralization in the communication among the RSUs and OBUs,

predict security breaches, and control structures for provisioning/coordinating resources for counter attacks.

The research investigated the most important threats that are to be resolved by contemplating the primitive requirement of latency, throughput, and scalability in VANET and rendering end-to end security. The most treacherous of all attacks launched are due to inappropriate authentication of the sender and the receiver, inadequate privacy-preserving scheme, and less secure communication channels. Some of the consequent attacks include impersonation of a legitimate node, Sybil attack (using multiple IDs), replaying previous messages, fabrication of transmitted messages, and location tracking.

To achieve these aims, in this research we addressed these attacks with reduced overhead, efficient data dissemination and preservation of user anonymity by exploiting blockchain's inherent security features. A summary of our main objectives targeted is shown in below process:

1. **Investigated the threats due to lack of appropriate authentication and timely revocation, and proposed a new mechanism based on decentralized blockchain technology for detecting and establishing secure communication by authenticating authorized vehicles and revocating malicious vehicles with purpose of protecting against security breaches.**

2. **Investigated the trust issues in vehicle-to-vehicle communication and identified the advantages and disadvantages of centralized and decentralized trust management systems, reviewed past research works to address the issues.**

3. **Proposed a new trust and reputation scheme to validate messages from a trusted node using blockchain smart contracts, for prevention and protection mechanisms against future security attacks within the infrastructure. In this scheme if a vehicle sends an emergency message, its correctness is evaluated against some parameters along with feedback from other vehicles and a smart contract then computes its reputation score which gets updated in the IPFS storage.**

4. **Proposed a new data hiding and privacy preservation scheme for secure transmission of data in the VANET, and node trustability prediction using Machine Learning. This scheme ensures that the data transmitted**

**is known only to the sender and no vehicle gets access to any message if it fails to pass the trust evaluation process.**

## 1.6. Research Objectives

Though most of the researchers in VANET focusing majorly on the security aspect predominantly addressed the above discussed issues, but they lack to suffice the scalability, computational complexity, communication overhead, latency and reducing dependency on the centralized authority. Keeping all these scenarios into consideration, we derived our problem statement, and achieved the following research objectives under major categories of:

1. *Authentication and Revocation*
2. *Trust and Reputation*
3. *Secure Communication with Access Control and Key Management*

### 1.6.1. Authentication and Revocation

**Objective I**

**Established Mutual authentication between RSUs and OBUs with reduced dependency on the Certificate Authority (CA). This established a decentralized VANET ecosystem, to avoid single point of failure and reduce communication delays.**

To become part of the network and entrust the messages from RSU, mutual authentication must be performed between the On-Board Unit (OBU) and corresponding Road-Side Unit (RSU), but this should not involve complex computations or frequent communications with the CA. Earlier schemes involve the CA to verify user's identity for every critical data received by the RSUs which causes a delay in connection establishment, bandwidth consumption and increased dependency on the third party. Furthermore, revocation and traceability also rely solely on the CA. The following objectives also fall as sub-objectives under this category:

**Speedy revocation without additional overhead:** The framework should not just be able to perform authentication, but quickly revocate the malicious vehicles. The vehicles revocated should be easy to identify without circulating an entire Certificate Revocation List (CRL) as it causes lot of overhead. For

authenticating as well, RSUs or the in-range vehicles consume plenty of time verifying the CRL before allowing any connections.

**Reduced load on the OBUs:** The transmission and verification process should also consider confined storage and limited processing capability of the OBUs. The OBUs at any time should not be overloaded with computations or run out of storage.

**Privacy protection:** Furthermore, the authentication of users should not incur at the cost of their identity disclosure or perturbing their privacy. When messages are communicated both the message and source authentication should be effectively performed without revealing the actual identity.

### 1.6.2. Trust and Reputation

In our next step of research, we extended out research work to incorporate trust and reputation of the nodes. We proposed a smart contract-based approach to update and query the reputation of nodes, stored, and maintained by IPFS scenario, dealing against colluding attacks. The proposed system runs on a smart contract embedded in the proposed *RepuChain*. The contract just like any other smart contract has their own storage, for data reference. The distributed and decentralized storage for maintaining node's reputation is the Inter-Planetary File System (IPFS)[6]. This is also responsible to maintain copies of node's identity certificates. With multiple nodes rendering requisite data in IPFS[6], there is a reduced latency, dependency, and bandwidth consumption for accessing and storing data.

Though most of the research in VANET focusing majorly on the trust aspect predominantly addressed trust and reputation using different techniques, but they lack to suffice the transparency, latency privacy and reducing dependency on the centralized authority. Keeping all these scenarios into consideration, we derived our problem statement, and achieved the following research objectives:

**Objective II**

**Established trust among the OBUs and between OBUs and RSUs with reduced dependency on the CA. This established a decentralized VANET ecosystem, to avoid single point of failure and reduce communication delays. In this, we identified and verified source of information thereby establishing trust in the network. This usually becomes necessary when authenticated nodes send fake and malicious messages for personal benefits.**

Even though users are authenticated, messages are loaded with digital signatures, and certificates, nothing guarantees the trustworthiness of a node within the network due to the absence of any reputed (centralized or decentralized entity) to continuously monitor the functional and behavioural capabilities of the nodes. The self-made decentralized network demands the potentiality to grant each node capability to derive the reputation of every other node. It becomes important that they are self-sufficient.

Therefore, we proposed a trust and reputation management system, wherein the nodes can transparently view their reputation score, and verify another node's reputation score as and when required. The management and computation is all handled by a smart contract which takes into account a number of factors, such as event occurrence, feedback from other nodes, node's location, time of event, etc., in computing the node's reputation score and making it available for other nodes in an immutable distributed storage which is the IPFS (Interplanetary File System) storage. This scheme achieves the following imperative sub-objectives via our scheme:

**Expeditious message verification and reputation computation without network flooding:** When an emergency event occurs such as an accident, traffic jam, major road conditions or on-going road construction, messages from the vehicles are sent to other reputed vehicles or the roadside units. They would then verify the authenticity of the message, based upon certain conditions. Once the conditions match and the sending vehicle's reputation score is found to be greater than a predecided threshold score, the message is accepted, and accordingly the vehicle's new reputation score is updated.

**Transparency of Reputation:** The nodes are fully aware of the process of computation of their reputation score and view their score as and when they want, along with the events for they were awarded with good or bad score.

**Minimal Latency in reputation evaluation:** There is minimum dependency of information from surrounding mobile nodes or static units (such as the RSUs). The amount of time needed in gathering information to assess the trustworthiness of node is directly proportional to the latency in tackling situations.

**Accurate Evaluation:** An accurate algorithm should consider previous history of the node (identity and its behaviours) and evaluate accordingly. In our case, a smart contract, which is a program coded with the set of conditions and agreements to trigger the event required (which in our case

is updating /calculation of the reputation score), handles the trust and reputation management.

**No collusion attacks:** Our scheme ensures that nodes cannot collude together, while they are asked for a feedback, they cannot bad-mouth or commend any nodes unnecessarily. Our algorithm for reputation evaluation does not let nodes to simply update their reputation score, as it goes through multiple steps of verification and update of score by means of reputed vehicles, our smart contracts and the IPFS storage.

**Message confidentiality, integrity, and non-repudiation:** The messages communicated, should be verified for their authenticity and integrity. The security mechanism should prevent unauthorized access by intruders, to avoid any compromise of confidentiality and authentication should prevent repudiation.

### 1.6.3. Secure Communication with Access control and Key Management

The next objective is to ensure that messages transmitted in the network are securely accessible to the reputed nodes only, and the message formation requires no computational complexity of encryption or decryption.

**Objective III**

**Designed a data hiding technique which sanitizes data before transmission We used a simple XOR technique to perform the sanitization, to ensure minimal computations and no latency in encryption and decryption process. The sanitization works on the sensitive data mostly. The most critical part of this technique is designing the objective function which provides the solution for maximum data hiding with optimal key and used an optimization technique such as Sea-Lion Optimization/Whale Optimization Algorithm to achieve it. These optimization algorithms are explained in detail in Chapter 6.**

**Objective IV**

**Designed a data management technique using the blockchain technique which manages the keys generated for the sanitization process. This would be an immutable storage and records can easily be accessed for desanitization based upon the timestamp.**

**Objective V**

**Designed a trust management system, using Machine Learning, which can classify trustworthy and malicious nodes, based upon certain critical factors such as Packet Delivery Ratio (PDR), Received Signal Strength Indicator (RSSI)values. This can help prevent attacks caused by 'authenticated' but greedy nodes.**

Finally, every component of the framework works together to serve the following objectives

**Objective VI**

**The framework reckons with scalability to the vastness of the vehicular networks. This objective is to keep the above security requirements into consideration as well as keep up with the scalability of the network. As more and more users become part of the network, the framework optimizes the application benefit as well consider the bandwidth usage into consideration.**

**Objective VII**

**Validated and evaluated our proposed security technique through implementation/simulation in the VANET simulation environment. This is done using Omnet++, SUMO, VEINS and MATLAB.**

## 1.7. Research Methodology and Research Contributions

To achieve the above research objectives, we divided the project into the following research tasks along with the timeline required to achieve them.

**Task 1: Review on Vehicular Ad hoc Networks (VANET), Security issues in VANET, VANET Security and Simulation Tools.**

First, a broad literature review was conducted on the related topics, and developed the knowledge about Vehicular Networks, their protocol stack, applications, security, and defense strategies along with various simulation tools like SUMO, OMNET++ and MATLAB. After a level of understanding in the vehicular security issues, worked on the algorithms, techniques and technologies that can be used to combat these issues. Number of them also have been used by other researchers such as using Pseudonyms, multiple encryption techniques, hashing algorithms and involvement of trusted authorities.

**Contribution 1:** This work is based upon our publication[7], which discussed the various security issues, requirements, modes, modules, and components of VANET along with some of the existing security solutions.

**Task 2: Study the latest techniques, technologies, and platforms to address the research gap- "end-to-end VANET security with authentication".**

Proceeding towards the next phase was studying about the Blockchain technology and its current trends. This involved reviewing the existing use-cases of blockchain, studying the latest white papers by Deloitte, which detailed abstract ideas about how blockchain can make a lot of impact in the IoT security. Apart from identity verification, blockchain (depending on types- public, private, consortium) could also be used for access control and privacy of users. After understanding the working, protocols, and types of blockchain, its usage in the VANET security was identified followed by algorithm design for VANET security using blockchain.

**Contribution 2:** This work is based upon our publications [8, 9], which elaborate in detail about blockchain, its components, working and applications.

**Task 3: Develop efficient Authentication and revocation mechanism for securing V2V and Vehicle-to-Infrastructure (V2I) communications using Blockchain.**

This work is a blockchain based authentication and revocation framework for vehicular networks, which not only reduces the computation and communication overhead by mitigating dependency on a trusted authority for identity verification, but also speedily updates the status of revocated vehicles in the shared blockchain ledger. In the proposed framework, vehicles obtain their Pseudo IDs from the Certificate Authority (CA), which are stored along with their certificate in the immutable authentication blockchain and the pointer corresponding to the entry in blockchain, enables the Roadside Units (RSUs) to verify the identity of a vehicle on road. The efficiency and performance of the framework has been validated using the Omnet++ simulation environment.

**Contribution 3:** This work is based upon our publication [10] .

**Task 4: Working on applications that can be used on the blockchain for providing end to end security in other static and dynamic Intelligent Systems (IoT Networks, Edge Devices). Next, learning the Ethereum smart contracts for rendering not just authentication and revocation, but also trust and privacy in these networks.**

Proceeding to the next stage, was working on the Ethereum smart contracts and their use in improving the current issues with trust and privacy in the Edge Data Centers (Similar to RSUs in vehicular networks). Smart contracts are programs deployed on the blockchain to automatically execute a certain set of

code based on the rules predefined by the creator of the smart contract. For example, if a vehicle A sends a message to vehicle B about an emergency, then it should invoke a smart contract to inform the nearest RSUs or the centralized authority. So, a set of conditions (If this…then this) are predefined in the smart contracts, which are automatically performed and updated in the form of transactions in the blockchain. This ensures non-repudiation, authentication, and privacy of users in the network. Basically, using a blockchain to share information and transmit messages establishes trust among unknown users. There has been a lot of work to address the authentication and conditional privacy, but minimal amount of work has been done in the trust area.

**Task 5: Design the threat model, attack scenarios, and accordingly model the defence mechanisms using Blockchain Smart Contracts implementation.**

During this task, various scenarios for different attacks were developed in the distributed IoT networks, say for example, one Edge Data Centre (EDC1) wants to share the load with another EDC2, so before sharing the load, it needs to authenticate the EDC2. As mentioned in section 2 about attacks in the distributed networks, there might be a fake node broadcasting its availability as a node with less load. Only verified nodes should be allowed to share the load.
**Contribution 4**: This work is based upon our publication [11], where we propose the blockchain and smart contracts-based trust and reputation scheme.

**Task 6: Reviewing on Trust and Privacy works in Vehicular Ad hoc Networks (VANET), Comparing the works using centralized and decentralized architecture. Understanding the pros and cons of both, technologies used in both and identifying ways to take a better approach to achieve trust and reputation in VANET.**

Next was conducting a broad literature review on the Trust and Privacy frameworks in VANET as per the VANET-SECURITY-PROJECT. This included reviewing some papers to identify the best approach in achieving privacy, trust, and reputation in VANET, and propose a scheme to overcome the disadvantages of a completely centralized scheme.
**Contribution 5:** This work is based upon our publication [11], which is a review work comparing the trust and security schemes w.r.t. centralized and decentralized approaches.

**Task 7: Design the scheme to achieve node classification with sanitized data sharing using an optimized key for this data generation (August 2019-March 2020)**

After achieving the trust and reputation using smart contracts, the next objective was moving towards 'end-to-end' security, which still lacks privacy in

communication. After this, the Machine Learning was added on top of Blockchain to achieve both node classification with sanitized data sharing.

During this task, various scenarios for different attacks were developed and the objective function for the scheme was derived where we try to provide more sanitized data with the optimized key generation using the selected Sea-Lion and Whale Optimization Algorithms in the VANET. Then the nodes sending data use this optimized algorithm for key generation used to sanitize the data for transmission. For nodes willing to have access the data got through a process of two-step evaluation to find out if they are trustworthy or not. This process used Machine Learning where we trained the machine based on some most prominent factors such as PDR, PFR, RSSI to identify the node's trustworthiness, thus achieving node classification and privacy protection.

**Contribution 6:** This work is based upon our publication [12].

## 1.8. Thesis Organization

The thesis has been organized as follows:

- **Chapter 2** presents the **literature review** i.e. the background and related works relevant to the research area. The Chapter discusses VANET, its protocol stack and threats at the various layers, therefore elaborating the security requirements in a greater detail. Further, we discuss the multiple solutions and security frameworks in place providing authentication, trust, and other security measures. This Chapter further elaborates each research question and the background work to reach the objective corresponding to the research question. It further elaborates upon the working and the limitations of the above-mentioned security frameworks.

- **Chapter 3** presents a detailed study of **blockchain for decentralization**. Here we focus on what blockchain is, how it functions, and what are its advantages that we can leverage in a dynamic environment of VANET. We further discuss the application of smart contracts and how do they work.

- **Chapter 4** presents our proposed **Authentication and Revocation** components of the proposed security framework and discusses in detail its various components and workings. The Chapter sheds light on how the various concerns and limitations related to current authentication and revocation schemes are addressed. This new scheme redefines the traditional schemes with the introduction of blockchain and various scenarios that it can handled are presented. It also presents the various new features and how they are incorporated to provide extended functionality.

- **Chapter 5** focuses on the **Trust and Reputation** component of the framework. The Chapter discusses the various components such as blockchain, smart contracts and the IPFS storage and how they are integrated into VANET, thus redefining a traditional VANET function. It also discusses the various scenarios the proposed scheme handles and how it works efficiently in those scenarios after comparing with existing works.

- **Chapter 6** provides the final component for the security framework and focuses on **Secured Message Transmission, Access Control and Key Management with distribution** utilizing the underlying blockchain technology and optimization techniques. The proposed scheme is discussed in detail with its various components and how they reduce the computation complexity involved in traditional encryption/decryption techniques. The scheme ensures security by only granting access of transmitted messages to reputed nodes.

- **Chapter 7 concludes the thesis** and provides a window into the future works possible in improving and expanding the presented security framework.

# Chapter 2

# Literature Review

*Vehicular Ad hoc Networks (VANET) is emerging as a promising technology of the Intelligent Transportation systems (ITS) due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. But the security threats hinder its wide deployment and acceptability by users. Most importantly, in relations to the proposed security schemes for the vehicular network, most imply a centralization of the various functions and features. In this chapter, we discuss the review work done under the various research objectives and tasks as designed in Chapter 1. First, we give an overview of VANET, which includes its protocol stack, architecture and its applications followed by the security threats at the various layers of the VANET communication stack. In the next step, we studied the latest technologies and platforms to achieve the solution, which is discussed in the following Chapter, Chapter 3. This step is followed by reviewing the works done under our research problems which particularly focusses on the review work done to achieve authentication, trust, privacy, and secured communication in the past. After discussing these existing solutions, we conclude what needs to be considered while designing a security framework for VANET to overcome the various security challenges in VANET and achieve decentralization.*

## 2.1. Introduction

In this Chapter we elaborated the review work done under the designed research tasks and objectives as discussed in Chapter 1. To describe the review works done we briefly go through the research tasks and then describe the work done under each task.

**Review Task 1:**

*Review on VANET, Security issues in VANET, and its Security requirements.*

This task is divided into two sub tasks:

1. **The basics:** Under this task we begin with understanding the basic VANET architecture, its modes of communication, the communication protocol stack, and its use cases and applications

2. **The threats and issues:** Under this task we explored the VANET security requirements and the threats at various layers of the communication stack, to narrow down our research problem.

**Review Task 2:**

*Reviewing on the Authentication, Revocation and Conditional Privacy Preservation schemes. Compare the existing solutions.*

After understanding the VANET security requirements, we review the first problem identified i.e. authentication, revocation and conditional privacy preservation and explore the works done to achieve the appropriate solution. While there have been number of works done, we try to find out the drawbacks of the existing solutions to move towards the solution.

**Review Task 3:**

*Reviewing on Trust and Privacy works in Vehicular Ad hoc Networks (VANET), Comparing the works using centralized and decentralized architecture. Understanding the pros and cons of both, technologies used in both and identifying ways to take a better approach to achieve trust and reputation in VANET.*

Next, we conducted a broad literature review on the Trust and Privacy frameworks in VANET as per the VANET-SECURITY-PROJECT. This included reviewing some papers to identify the best approach in achieving security, privacy, trust, and reputation in VANET, and propose a scheme to overcome the disadvantages of a completely centralized scheme.

## 2.2. VANET overview – Architecture and Applications

VANET can be briefly defined as "***spontaneous, self-configurable networks formed between moving vehicles, where each vehicle serving both as a mobile node and router, is equipped with wireless capabilities (radio antennas, embedded sensors, GPS, etc.) to support short range communications and can communicate wirelessly both with other mobile nodes (vehicles, and pedestrians) as well as established Road Side Infrastructure/units(RSU). The vehicles, can proficiently gather and process surrounding data and transmit the same via messages containing the vehicle's unique identifier, current position, timestamp, and any other safety related data in a timely manner to surrounding vehicles, thereby facilitating safe driving with, real time traffic assistance, accident prevention, and emergency warning among others."***

A vision of *'Connected wireless vehicles'* needs to be justified in aid of wireless technologies and standards reinforcing it. Considering the imperative parameters of short-range connectivity, scalability, latency and throughput, which stands them out from other wireless networks, there have been efforts of modifying the existing wireless technologies and raise new standards to fit to the needs of VANET. Thus, affiliated to VANET are a certain set of standards and protocols that have evolved to ensure invulnerable inside and out network design, attaining impregnable message transmission, identity and data management, controlling access to resources, authorisation and authenticating of network users and safeguarding against tracing and hacking of user privacy. The standards vary owing to their formulation by distinct Standardization Development Institutions (SDI), [13] thus causing the difference in their protocol stack, but mainly overlapping attributes contemplating to the similarity in the fundamental but imperative requirements. There are projects and standardization efforts done collaboratively by different authorities towards the deployment of ITS technologies in every aspect. These have evolved differently in countries putting forth their best towards ITS development and implementation namely WAVE in U.S. [14] and C-ITS [15] in Europe, commonly known as DSRC in both the regions.

They have showcased tremendous transformations provisioning for wide-ranging safety and comfort applications to the masses, thus generating revenue for government and saving fuel for travellers. In the following subsections we discuss the protocol stack, architecture, and applications.

### 2.2.1. VANET Architecture and Protocol Stack

The first milestone towards standardization in US took place in 2002 when on the appeal of ITS America the FCC allocated 75 MHz of spectrum in the 5.9. GHz band specifically for the purpose of connected vehicle applications, thereby

protecting the public from some of the lethal situations by forewarning them of imminent hazards. This has come to be known as the 'Dedicated short range communications (DSRC).

IEEE and SAE are the two different SDIs responsible for standardizing the protocol stack for DSRC enabled vehicular communications. FCC initially referred to a single PHY and MAC standard, developed by the ASTM (ASTM E2213, published in 2003), which was based on the IEEE 802.11A OFDM PHY. [16] After IEEE incorporated all the earlier PHY and MAC features in single IEEE-2007 edition, the IEEE task group p was formed, which amended this IEEE-2007 edition especially for Vehicle-to-Anything (V2X) communications. This WLAN standard known as IEEE 802.11p [17] specifies the physical (PHY) layer and MAC layer for DSRC based Vehicular transmissions. Later, IEEE further developed the IEEE 1609 group [18] which established the family of protocols (IEEE 1609.x) on the top of this IEEE 802.11p PHY and MAC layers to provision open access for V2V and V2I communications.

This protocol stack came to be known as the WAVE (Wireless Access for Vehicular Environment), and the terms DSRC and WAVE are used interchangeably to refer to this stack. Other than IEEE, SAE has contributed to refine this V2X WAVE enabled stack by defining the message sets and other performance requirements.

The overall bandwidth is partitioned into seven channels of 10 MHz each, and one guard band of 5 Mhz. Among these seven channels, one channel is configured as the Control Channel (CCH), to carry high priority, delay sensitive data whereas the rest of the six channels serve as the Service Channels (SCH) for delivering regular data. Thus, IEEE 1609 group, not just defined the architecture, but also developed standards facilitating V2V and V2I communications. Figure 2.1 depicts the WAVE stack defined in IEEE 1609.0-2013. Figure 2.2 Depicts the complete VANET architecture, components involved, and communications achieved.

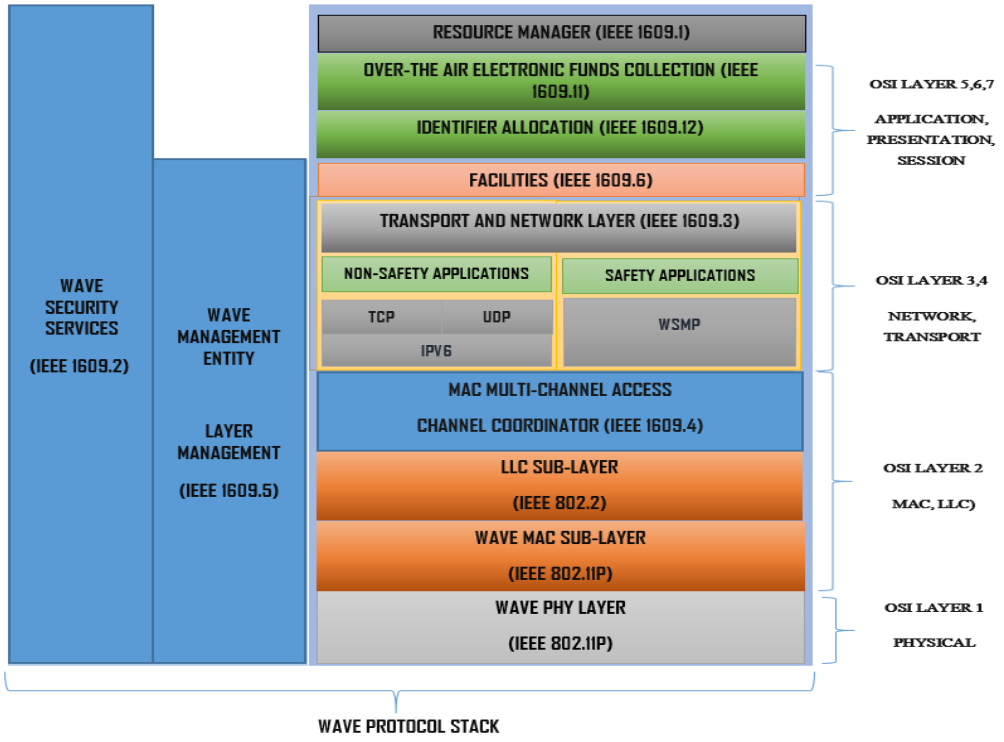


*Figure 2.1 WAVE Protocol Stack*

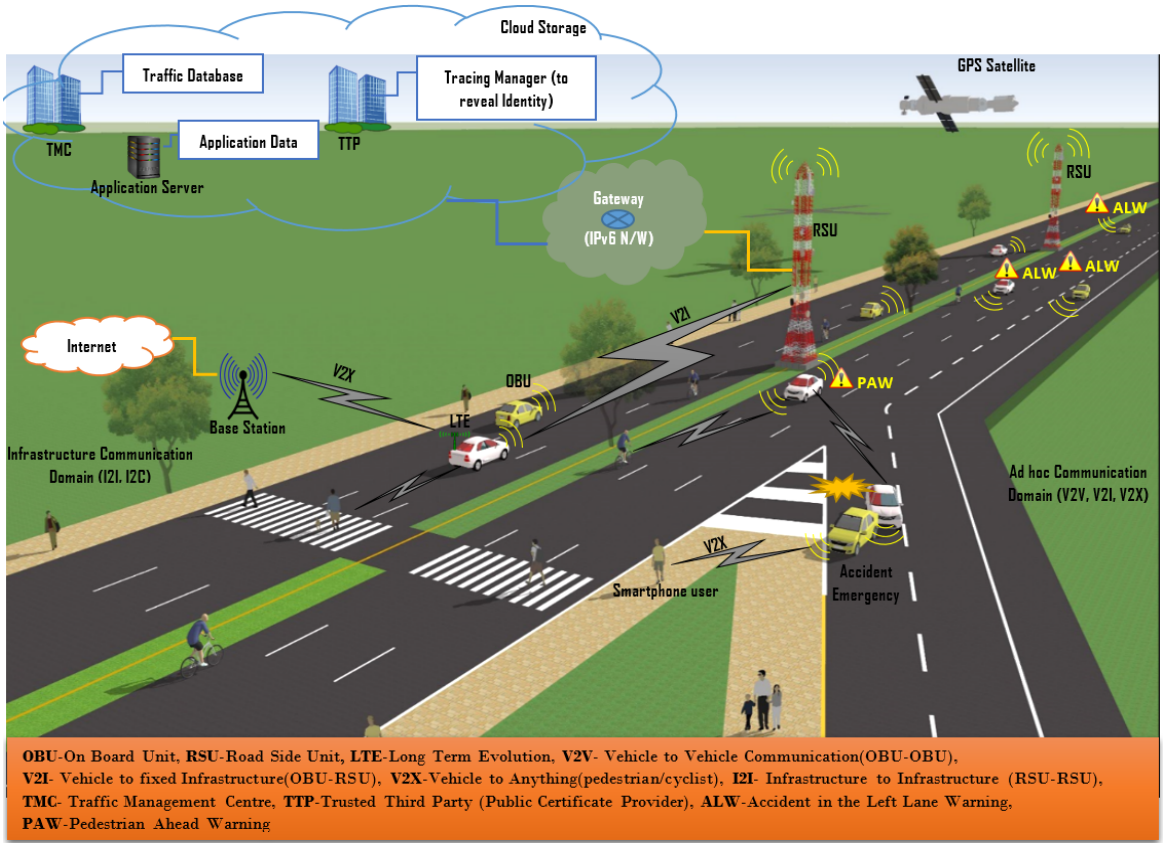


*Figure 2.2 VANET – Overview (Architecture, Components and Communication)*

This architecture clearly defines the support for both delay sensitive safety applications, and internet applications. Considering the stringent delay requirement, efficiency and timely delivery of packets in emergency scenarios, IEEE 1609 group developed a single-hop communication protocol, the WAVE short Message Protocol (WSMP), which allows to send messages with a minimum length of 5 bytes and a maximum of 20 bytes [14]. This is to avoid the communication overhead in IPv6 packet size. Hence, IPv6 is adopted only for non-safety applications, such as software updates for OBU, multimedia downloading, and location-based services. IEEE 1609.3 defines the networking services for both types of applications.

To render security across the stack, IEEE defined the IEEE 1609.2 standard, which intends to provide a complete security framework incorporating all the security requirements for all types of services. Schemes defined, form components of Public Key infrastructure (PKI), where messages are securely communicated by encrypting them using Elliptic curve cryptography (ECC) and authenticated using Elliptic Curve Digital Signature Algorithm (ECDSA) [19] as it delivers preeminent security with a smaller key size.

The WAVE MAC, unlike the traditional IEEE 802.11 networks, provides WAVE Basic Service set (WBSS) and WAVE independent basic service set (WIBSS) for ad Hoc network creation. Vehicles under normal circumstances form networks using WBSS, where the RSU serves as the Access Point (AP), sending messages periodically over the control channel (CCH) to authenticate entities and render services. In case of emergencies vehicles, the security services such as authentication and synchronization are performed by the upper layers, but vehicles in-range can deliver emergency messages which are verified later.

Despite the number of approaches by the industry and academia, VANET, in wide scale have not been completely implemented, due to varied reasons, most vital of them being security. Openly accessible wireless channel houses threats to users' security and privacy and gives attackers the chances to exploit the resources in an unauthorized way leaving legitimate users, deprived of the resources, and compromising on privacy.

#### 2.2.1.1. Modules Performing Communications

To achieve wireless transmissions spanning Local and distant areas, the research community as well as the automakers are coming up with WLAN (IEEE 802.11p compliant) modules which facilitate V2V, V2I and V2X communications. These Modules are specifically known as On-Board Units (OBU) for in- vehicle DSRC enabled embedded devices and Road-Side Units (RSU) for the module fitted in the static road-side infrastructure, such as buildings, red lights, etc.

### A. WLAN compliant OBU

The on-board unit incorporates all the components and devices necessary to communicate with other OBUs and RSU's. These include:

a. IEEE 802.11p radio transceivers

b. Communication Processor

c. Memory to store data captured and processed from the vehicles' Electronic Control Unit (ECU) and communicated to and from the RSU with accurate time stamp

d. OBD-II Interfaces to the vehicle's Controller Area Network (CAN), to perform data acquisition from vehicle's ECU

e. User Interface to access multiple applications.

### B. WLAN Compliant RSU

DSRC modules in the Roadside infrastructure incorporates features to communicate with other RSU's and to support this, they intrinsically contain navigation systems, radio transceivers supporting the openly available WAVE, and for more ITS applications there can be Wi-Fi, LTE, GPRS, WIMAX support.

This unit is responsible to perform registration, association, with all the vehicles entering its region. Hence, it is equipped with slightly greater computation capabilities than the OBU and serves multiple purposes to the OBUs.

RSU is responsible to execute three main functions: [20]

a. Serve as an Information source, as it is the provider/host of numerous safety applications. Through the Infrastructure-to-Vehicle (I2V) communications, RSU's disseminate warnings to the vehicles in their area, such as low bridge warning, or work zone warning. Also, vehicles in an area can query the RSU's regarding traffic on the road ahead.

b. Relays messages to other RSU's and OBUs, thus spreading information over a wiser area.

c. Connecting OBUs to internet via the IPv6 Gateways.

### C. Tamper-Proof Device (TPD) [21]

It stores users' confidential data, such as the user's private key and certificates. It is responsible to generate pseudo IDs [22] and digital signatures using these Pseudo IDs to preserve privacy and provide authentication of messages to the

recipient. It is installed by the manufacturer and is only accessible to authorized parties. The users cannot tamper this device; else it will erase all the cryptographic information.

**D. Application Unit (AU)**

The application unit, equipped in the vehicle, either within the OBU or as a separate unit [23], is a dedicated device with user interface for accessing services rendered by the RSU's utilizing the OBU's communication capabilities, be it safety applications, information services, internet connectivity or forwarding its own application data widely. Depending on the user's need there can be more than one application units serving different needs.

### 2.2.1.2. Modes of Communication

The OBUs communicating with other in-range OBUs form local or Vehicle-to-Vehicle (V2V) communications, whereas RSU exchanging data with other OBUs or RSU's is termed as Vehicle-to-Infrastructure communication (V2I). Operating in a hybrid mode, Vehicles communicating with any other mobile or static entity, pedestrian or platform is referred as Vehicle-to-Anything (V2X) communication defined in 2014 by the 3GPP group [24].

**A. V2V communications**

The vehicle to vehicle communications are achieved by direct radio connectivity between their respective WAVE compliant OBUs. They are responsible to perform the following functions in a timely manner, precisely every 100-300ms according to DSRC specifications. The first step is **Data Acquisition and Processing,** in which data captured by the vehicle itself. The embedded sensors in the Vehicle capture surrounding data, which is analysed by the processor and the Operating system to derive the surrounding parameters such as proximity of any nearby vehicle exceeding speed limits, sudden brakes by a preceding vehicle, hidden vehicle warning, lane change warning, etc. In the next step, **Data Transmission** is done. The values evaluated by the vehicle are then transmitted to vehicles in the 360-degree view of the vehicle in the form of data packets. Thus, V2V is performed for safety and security applications.

**B. V2I Communications**

V2I communications allow a vehicle to access the applications provided by the RSU. The vehicles query the RSU either for gaining road and traffic information,

accessing the internet, or relaying messages to other OBUs in case of multi-hop communications.

**C. I2V Communications**

In this case, RSU's communicate with the OBUs either to revert to any query raised by the corresponding vehicle or to forewarn of any emergency event.

**E. V2X Communications**

As defined by the 3GPP group vehicles performing communications with any entity other than the RSU's and other OBUs is called as V2X communication. For e.g., if using a laptop or smartphone, the vehicle is accessing the internet applications.

### 2.2.2. VANET Applications

The ETSI Basic Application set (BSA) [25] document specifies a group of Applications and their use cases as a reference for the stakeholders developing them under proposed ITS. These focus on all the modes of communication (V2V, V2I, accessing the DSRC standard as well as other wireless technologies such as Cellular networks and broadcasting systems.

These applications are majorly categorized into four parts:

**A. Mutual Road safety**

To achieve cooperative road safety, we need robust mechanisms for driving assistance and cautioning drivers of future collisions. This is achieved both from V2V and V2I communications.

This class of application is subdivided into:

**A.1. Collision avoidance via Cooperative awareness**

- Forward Collision warning
- Intersection collision warning
- Emergency vehicle approaching
- Pedestrian at the crossing
- Emergency Electronic Brake Light (EEBL) warning
- Lane Change warning
- Blind Spot warning
- Road Condition warning

- Cooperative Adaptive Cruise Control

### A.2. Assisting Drivers for Road and Infrastructure threats via V2I communications

- Work Zone warning
- Signal violation warning
- Congestion ahead/Collision risk warning
- Post-crash warning
- Low Bridge warning

## B. Improvising Traffic Efficiency

These applications aim to improvise not just the traffic conditions and efficiency, alleviate congestions on the motorways but are helpful in saving time and fuel for the users.

- Speed limit notifications
- Traffic light signal timing broadcast
- Route guidance for managing traffic and saving time
- Electronic Toll Collection

## C. Location-Based Services

Based on the GPS signals and timing synchronization, the legitimate users are informed about the nearest useful areas such as:

- Parking space assistance
- Nearby cafe, restaurants, movie theatre information, Shopping Malls, etc.

## D. Global Internet services

- Multimedia access
- OBU and RSU software updates

## 2.3. VANET Security Requirements and Threats

Despite these numerous advantages for safety and driving assistance, it brings along a storm of threats specially targeting the security and privacy aspects, due to the vulnerabilities associated with the openly accessible wireless channel. The bandwidth can easily be hacked to perform various malicious activities such as impersonation, eavesdropping, signal jamming, etc. [2] for user-tracking, proving life threating in most scenarios.

As discussed above, the VANET architecture protocol stack takes its reference from the OSI model, almost incorporating all the layers. Thus, security threats span across the entire stack from the Application to the Physical layer, involving different entities, causing multiple security challenges, hindering different modes of communication (V2V, V2I, V2X). Thus, a designing a security framework for VANET needs to consider the threats along the entire stack and should propose mechanism overcoming challenges at each of these layers.

Following subsections discuss in detail the various security requirements, attacks performed by malicious users challenging these requirements.

### 2.3.1. Security Requirements of VANET

A. **Confidentiality and Access Control:** Data Confidentiality ensures the message/data contents are revealed only to the authorized individuals and prevented from any undesired and unauthorized disclosure both when the data is stored and when in process of transmission. In VANET confidentiality hails as a primitive requirement achieved by applying certain access control policies and cryptographic mechanisms on the stored and transmitted data. This requirement becomes even more imperative, particularly for the military application of VANET, where information disclosure is not just a security breach, but undoubtedly life threatening.

B. **Integrity:** Integrity of data is validated, if the transmission of data from source to destination occurs with no external (unknown and unauthorized) interference and tampering, and accuracy and reliability of data can be ensured at the destination. In VANET, if a malicious attacker alters the transmitted data pretending to offer safety but can lead to traffic congestions, or unwanted route diversions for drivers.

C. **Availability:** To access the network resources, it's necessary for them to be available when required in a timely manner. Considering stringent delay requirements of messages in VANET, if unnecessary message transmissions by attackers consumes most of the available bandwidth, it leads to DOS for legitimate users. Thus, how we counter DOS attacks, plays crucial role in network availability for rightful users.

D. **Authentication:** Authentication is the process of identifying network users by means of Unique ID and password/biometrics to grant them authorization for accessing the resources. It's a necessary step in VANET to ensure not only the message received by the recipient has come from an authorized user, by means of the user certificate and signature verification.

E. **Conditional Privacy preservation:** Privacy refers to hiding critical and personal user information from unwanted and unauthorized entities, to ensure safety and security. In VANET, it is necessary to keep user's identity a secret or use frequently changing pseudonyms IDs to avoid location tracking or impersonation. Offering complete privacy is impossible in VANET as the user's identity needs to be revealed and traced in case of emergency scenarios such as any accident enquiry requiring the user's location and personal information. Even in case of Pseudo IDs its necessary to use cryptographic mechanism and ID generators secure but less complex to ease traceability.

F. **Non-Repudiation**: Non-repudiation ensures that when recipient identifies who the sender is, the sender takes complete responsibility and cannot deny sending the message. Digital Signatures included in the message can serve the purpose, to avoid any conflicts in abnormal scenarios.

G. **Trust:** It is emerging as the most important requirement to deliver a successful security framework for VANET. Although we can verify, and authenticate received messages, but considering the number of entities involved and the difference in their backgrounds, we cannot trust them.

To achieve these security requirements, firstly we need to get a clear view of the attacks preventing their accomplishment and later we review some of the existing solutions proposed and efforts made targeting these requirements.

### 2.3.2. Attacker Entities

VANET hosts a group of entities accessing and utilizing the network resources, namely, the drivers and vehicles which cooperatively perform exchange of broadcast and event-driven messages in normal conditions. But situation becomes abnormal if any of these entities turn up to be playing false and intends to cause damage. These can be any of the following:

A. **Rapacious or impatient Drivers:** Under normal driving conditions, a driver follows rules, is ready to go through congested scenarios and delivers reliable safety messages. But, if he turns out to be greedy, then irrespective of other road users' needs he would send false messages by impersonating to be 100 vehicles, thus declaring congestion on the route he desires to follow for his destination.

   In another case, to avoid any fines for speeding up in speed restricted zones, or to escape from message forgery accusations, he might tamper vehicles' hardware and Software, in the absence of TPD [21].

B. **Malicious Attackers:** These also cause deliberate damage, serving them a purpose, either for fun or accomplishment of any illegal activities.

### 2.3.3. Layer wise Attacks in the VANET Stack

As discussed earlier, the attacks span across the entire WAVE stack causing individual damage at each layer.

#### 2.3.3.1. Attacks at the Application Layer

The application layer provides services to the wide variety of applications hosted by the VANET system, which includes, cooperative safety applications, infotainment and Warnings or Alerts. The application layer does not provide them but renders the services needed to access them from the Provider (RSU and other fixed infrastructure) and defines the exact message format. SAE J2735 standard in the WAVE stack specifies the format and message sets to perform transmissions in the DSRC range and defines minimum performance requirements. It is the responsibility of this layer to ensure the following functions:

A. Identifying the reachable provider (RSU, ISP) to render safety and non-safety services.

B. Authentication of the Provider.

C. Abide by the protocols, data syntax and format before commencing any transmission and reception.

D. Ensure integrity of data transmitted and establish trust in the sender.

Following attacks on the application layer interrupt its normal functionalities and compromise the confidentiality, integrity, Privacy and may also result into Repudiation.

1. **Message Falsification/tampering:** It is the act of sending incorrect/false information in the network, either by the greedy drivers, or malicious intruders. To gain complete access and avoid congestion the driver might broadcast false messages, stating some accident emergency or congestion on route. In worst case scenario, an attacker might take over any RSU and send false warning, about work zone or access private information while other OBUs communicate with this RSU by faking identity. If an adversary fakes to be any RSU, which is hosting multiple applications, it would be easier to take control of these applications, such as Toll Collection, Traffic information display, causing not just road havoc, but can cause casualties as well. Thus, message originator authentication and verification become inevitable to ensure integrity and confidentiality.
2. **Repudiation:** If the attacker fakes another vehicles' identity by replicating signatures, it can easily lead to the legitimate user denying of sending messages which were sent using his signature.
3. **Malware Attack:** By faking identities, user can send fake software updates to the OBU, or by sending unnecessary advertisements causing bandwidth consumption.
4. **Location Tracking:** It becomes easy for the adversary to perform 'signature linking' even from Pseudonyms if they aren't changed frequently and thus makes it easy for any insider to track user's activities, monitor route, get other personal details by linking multiple signatures generated.
5. **GPS Spoofing attack:** [26]. If attackers use simulators generating GPS signals stronger than the GPs satellite signals, then they can affect the positions vehicles know they are at, by altering their GPS device information, and therefore also interrupting with the working of other location-based services and applications. [27]

#### 2.3.3.2. Attacks Targeting Network and Transport Layer Functionalities

The network layer makes it possible to deliver messages by performing routing and forwarding functions, logical addressing, and controlling congestion.

Requisite Single-hop, multi-hop communications are performed by selecting appropriate route and QOS. It is responsible to perform uni-cast, multi-cast and broadcast transmissions and the transport layer enforces protocols to achieve these transmissions. The transport layer functions to assure end-to-end, reliable and in-order delivery of data packets. Adversaries which attack these layers disrupt these functionalities by following attacks:

1. **Impersonation Attack:** Every vehicle associated with VANET is assigned with a unique ID. In this attack, an adversary forges the identity of a legitimate user and thus, enters the network falsely by claiming to be an authorized user, participating in the communication either for personal benefits, for e.g. accessing resources available only to authentic users or for producing some incorrect information to clear the route it intends to follow.

2. **Sybil Attack:** It is a type of impersonation attack in which the adversary pretends to be multiple identities (maybe OBUs or RSU's) as presented in the first of works identifying Sybil attacks in peer-to-peer systems.[28]. In VANET, there is no central coordinator, as the WBSS (Wave Basic Service Set), discussed previously is used. Each node/vehicle itself performs the routing functions, hence, the authentication of messages and mapping of entity to identity takes place at the local level, relying solely on the assumption of cooperation and trust among the nodes, which can easily be violated by an intruder. So, this is basically due to lack of a central coordinator responsible for carrying out identity verification. Thus, an adversary can pose to be multiple entities to accomplish various malicious acts. The purpose of Sybil attack lies in the fact of 'believing mass messages delivering same information.

   If a single node communicates falsely regarding some emergency or event, it would be difficult to trust, but similar data when received from multiple authorized identities tends to persuade the legitimate users and act in the favour of the adversary. It is the most treacherous and hazardous attack in the VANET scenario and it's really important to detect the Sybil nodes [21, 29] .

3. **Black Hole Attack:** A black hole is that part of the network, which is created by an attacker, to gain access to the packets of a targeted node. The malicious node is the 'black hole' here, since it is a participant in the network as shown by the neighbour's routing tables, but it is not performing the routing functions, either intentionally or unintentionally [26].

   If the node simply wants to opt out of the network functions, with no catastrophic intentions, it is just a 'link breakage' and all the recipients

connected to this route suffer from data loss. It is a variant of the 'denial of service attack'.

But, if the malevolent node intends to trace the data or interrupt the transmission, then it cleverly advertises itself to be on the shortest route to the destination by cheating with the routing protocols and convinces other gullible nodes, thus causing a new corrupt route formed. The sender nodes being unaware, keep forwarding data packets to this node, which are forwarded to either undesired locations or kept by the node itself, thus initiating 'man-in-the-middle' attack [27]

4. **Grey Hole Attack**: It is a type of Black Hole attack in which the black node routing the data, drops data packets, but the selected ones. For e.g., packets of a certain type, or destined for a node, or only at a time, but otherwise it performs its functions normally [29].

5. **Worm Hole attack** [30]**:** A single or multiple malevolent node come together to launch this wormhole attack, in which messages received at one point are 'tunnelled' to some other point and replayed from there. The attacker is either in possession of some cryptographic information and as a legitimate participant, launches this attack, or as an outsider, attacks in the hidden mode, with a motive to analyse traffic or simply launch 'DOS' attack, thereby dropping packets.

6. **Replay Attack:** In this type of attack previously sent messages are replayed/re-injected by a malicious node, to misguide the recipients and basically take advantage of the situation when the message was transmitted [31]. This affects the routing tables and thus the locations of recipients.

   Replaying nodes could also develop sessions by spoofing credentials of a session and then replaying the same with the recipient, to establish an unauthorized route to acquire data.

   Thus, it is undoubtedly important to authenticate each packet received and include timestamp with every message so that the messages with the same content can be compared if re-transmitted.

#### 2.3.3.3. Attacks on PHY and MAC Layers

Following attacks on the application layer interrupt its normal functionalities

1. **Denial-of-service attack:** It is a type of attack in which the network resources are intentionally kept occupied to prevent the legitimate users from accessing them. The malevolent node would usually flood the network [26] with unwanted messages such as advertisements, or replay messages (replay attack), to affect V2V communications. In another case, a malicious node can send fake emergency messages to keep the RSU busy to respond to other genuine requests, causing accidents and collisions [21].

   To deprive the legitimate nodes of resources, the attacker would either perform 'signal jamming' i.e. signals interfering with the V2V and V2I radio frequencies are generated thus causing a single jam in an area. Only when the attacker causing the jamming leaves the area, normal communications pursue.

2. **Distributed DOS attack:** It is a variant of the DOS attack where the DOS attack is carried out from different locations and different timings [32], creating even more problems for the network users.

   The DOS attacks are specific to the PHY and MAC layers, but all the attacks discussed above, i.e. Sybil attack, message falsification or other attacks at the various layers are a breach to the PHY and MAC layers, because they make use of the network resources either from the inside or outside to perform these attacks.

3. **Spamming:** If intentional spam messages are injected in the network, it affects the channel access by other user for genuine reasons. This is done to increase the transmission latency, to accomplish malicious acts [26]

Table 2.1 summarizes the attacks on various layers of the protocol stack and what communication effected as a result

*Table 2.1 Attacks on layers and communication affected*

| **Layer Targeted** | **Type of attack** | **Compromised security requirement** | **Communication affected** |
|---|---|---|---|
| | | | |
| Application Layer | Message Falsification/tampering | Confidentiality, integrity | V2V, V2I |
| | Repudiation | Non-repudiation | V2V, V2I |
| | Malware attack | Availability | V2V, V2I |
| | Location tracking | Privacy | V2V |
| | GPS spoofing | Privacy | V2V |

| | | | |
|---|---|---|---|
| Network &Transport Layer | Impersonation | Integrity, Authentication | V2V |
| | Sybil attack | Authentication, Availability and Privacy | V2V |
| | Black Hole attack | All except privacy | V2V |
| | Grey Hole attack | All except privacy | V2V |
| | Worm hole attack | All except privacy | V2V |
| | Replay Attack | Authentication | V2V |
| | | | |
| PHY and MAC layers | Denial of Service attack (DOS) | Availability | V2V, V2I |
| | Distributed DOS (DDOS) | Availability | V2V, V2I |
| | Spamming | Availability | V2V |
| | | | |
| | | | |

## 2.4. Centralization vs Decentralization

VANET are spontaneous and self-configurable networks, as each of these vehicular nodes have the potentiality of communicating with each other without any centralized party on road. But, for the security of the entire network such as identity management, trust, and reputation management, one or more centralised/trusted parties are needed. When the vehicles begin their travel on road, these trusted parties come in foremost for their authentication, revocation, access control and trust management. Hence, a traditional VANET is a centralized network. In most of the existing schemes, which work to provide the typical security requirements as identified in the above section, there is due reliance on this centralized party which causes a delay in message relay and consumption of bandwidth.

In the past years, researchers implemented some modifications in the traditional working of the network, by proposing decentralized models in VANET environment. A decentralized VANET model functions by removing or reducing the dependency on the trusted parties. This is to give more independence to the vehicular nodes in assessing the other nodes for trust or security measures. Based upon the need and dependency on the centralised/trusted parties, these schemes can be totally or partially decentralized.

While the sole purpose of the decentralized schemes is to give more power to the vehicular nodes, thereby reducing dependency of the trusted party, such approach in turn reduces the latency and bandwidth consumption. Therefore, any of the schemes applying decentralized technologies such as ring signatures,

blockchain or other schemes, may not be completely decentralized or fully centralized.

In the following sections where we conduct a literature review of existing security works, we categorised them under centralized and decentralized works, to understand the pros and cons under both kinds of schemes.

## 2.5. Authentication and Revocation Schemes with Conditional Privacy preservation

Researchers in past extensively analysed the attacks and security requirement of VANET, starting with the first of efforts by [33] [34] [31] & [21].

[21] for the first time addressed the security threats of VANET and placed the foundation mechanisms to secure them. Solutions to facilitate the most important of security requirements are discussed in detail by the authors.

### 2.5.1. Centralized Schemes

A PKI System is considered for VANET Architecture, to render all the above discussed security requirements.

Methods for storing and distribution of public and private key is addressed, including Certification and revocation. Furthermore, privacy preservation is addressed by means of Electronic License Plate (ELP) and anonymous key pairs.

For Authenticating safe messages, Digital Signatures are proposed to verify the authenticity of messages. The Tamper-Proof device in the vehicle is the storehouse of all the cryptographic information and is thus responsible for storing the private key used to generate the digital signatures and hence, messages sent can also be signed by this device. Keeping in view, the stringent delay requirement, authors also stated the advantages of 'Group Communication' for quicker authentication of emergency messages.

Many of the latest works consider these primitives as the foundation of their work, especially the ones who believe in PKI to be a better option than simple ID based architecture for VANET.

In [35], authors proposed a 'Global security architecture', as shown in Figure 2.3 which is not some standard, but a layer wise architecture, keeping all the security requirements at different levels of communication into consideration.

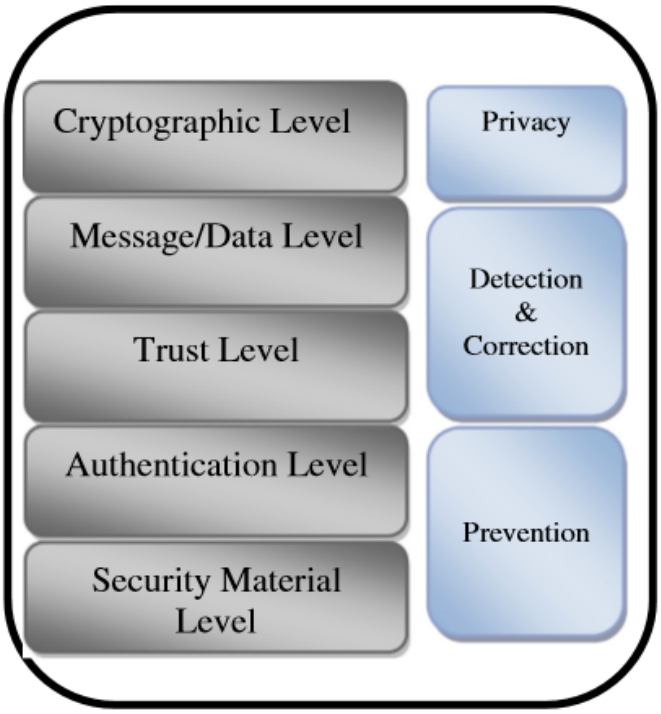


*Figure 2.3 Global Security Architecture*

The material level security comprises of the security of different modules which are adding to different steps of communication, & responsible for acquiring and transmitting data, for e.g. OBU, GPS, antennas, etc. These can be secured by the addition of a TPM connecting them.

The authentication level deals with the authentication of entities and data at different points of communication. To begin with, all the nodes participating is authenticated at the start to avoid any misuse of resources by unauthorized nodes. Secondly, data at the recipient end is verified by to ensure the confidentiality and integrity of data. Also, authentication of user's location is performed to validate the position of the node.

The trust level is meant to ensure the trustworthiness of different nodes and make sure that nodes responsible for transmitting the messages do not deny their participation i.e. non-repudiation.

The message/data level ensures data security using Digital Signatures, and finally the cryptographic level ensures users' privacy by means of identity protection and tracking. It also tends to protect the system from Sybil attacks.

The above papers give a generalized overview of the VANET security challenges, and a survey on the existing solutions. But most of the recent works targeted Authentication with privacy preservation.

Authors in [22] specifically defined privacy preserving anonymous authentication schemes. Privacy preserving authentication as discussed earlier, is an authentication scheme, whereby users authenticate each other without revealing confidential information. PPA schemes are classified based on authentication, i.e. symmetric or asymmetric encryption and on the basis of privacy preservation i.e. whether authentication is done via anonymous key pairs, and only Trusted third party is authorized to reveal identity in abnormal scenarios or is it based on pseudonyms, which can be generated by the TTP, RSU's or maybe the vehicle. These are generated frequently and randomly to avoid any 'tracking of the vehicle'. The existing schemes implementing these or targeting these are discussed with their solutions and further challenges are also brought into limelight. These include the design of VANET with less dependency on the Infrastructure, trusting the origin and need of a heterogeneous solution to support interoperability among the Vehicular and other wireless networks (e.g. WiMAX, Cellular), etc.

Authors in [36] also discussed some of the significant and emerging issues such as trusting the node disseminating data, how to check for its reliability and what would be the immediate and necessary actions to take if the node isn't impeachable and is not able to prevent malware attacks in the OBUs, at that point of time, it is necessary to protect them against malicious code installations or updates.

In a study, pre-shared keys were introduced to implement the authentication of nodes in the network [37]. [38] focused on security and privacy in VANET and proposed a hybrid method, which strengthens the framework using pseudonyms with self-certification, thus, eliminating the need for managing them without compromising on the robustness of the system. To obtain high accuracy and privacy with respect to the vehicle's location, [39] developed a methodology based on dynamic pseudonym generation for mix-zones environment and verified the results using the SUMO simulator.

### 2.5.2. Decentralized Schemes

With the launch of Bitcoin blockchain [9] in 2008, the focus of industry and academia shifted towards approaches which could secure the way centralized networks operated [8]. From then on, some researches in VANET focused on methodologies to improve efficiency, guaranteeing privacy and security using the blockchain technology. [40] introduced a seven-layer secure and decentralized conceptual model for Intelligent Transport System (ITS), discussing the relationship between Blockchain-based ITS and parallel transportation management systems claiming the former to be the future of ITS.

After the introduction of autonomous/self-driving vehicles on the road for which efficient and timely communication amongst the nodes is of utmost importance, [41] explored the use of sensing and signalling devices using blockchain public key infrastructure and an inter-vehicle session key establishment protocol.

### 2.5.3. Disadvantages of Existing Authentication Schemes

After we performed the review, we understand that, to become part of the network and entrust the messages from RSU, mutual authentication must be performed between the On-Board Unit (OBU) and corresponding Road-Side Unit (RSU), but this should not involve complex computations or frequent communications with the CA. Most discussed schemes involve the CA to verify user's identity for every critical data received by the RSUs which causes a delay in connection establishment, bandwidth consumption and increased dependency on the third party. Furthermore, revocation and traceability also rely solely on the CA.

### 2.5.4. Our Scheme and research outcomes

We worked on our authentication component of the security framework, which not just authenticates vehicles with reduced dependency on the trusted third party (thus bringing decentralization) but also preserves their anonymity without revealing the original identity of users. The proposed solution reduces the communication overhead and achieves statutory security requirements. It eliminates the need to circulate CRLs by the *CA* or *RSUs*, instead mends the status of a vehicle's revocation flag to be true. Shortly, our framework achieves the following objectives:

**Speedy revocation without additional overhead:** The framework not just performs quick authentication, but quickly revocates the malicious vehicles. The vehicles revocated are easily identified without circulating an entire Certificate Revocation List (CRL) as it causes lot of overhead. For authenticating as well, RSUs or the in-range vehicles consume plenty of time verifying the CRL before allowing any connections.

**Reduces load on the OBUs:** The transmission and verification process consider confined storage and limited processing capability of the OBUs. The OBUs at any time are not overloaded with computations or run out of storage.

**Privacy protection:** Furthermore, the authentication of users does not incur at the cost of their identity disclosure or perturbing their privacy. When messages are communicated both the message and source authentication are effectively performed without revealing the actual identity.

## 2.6. Security, Trust, and Reputation Schemes

With security and privacy of users, the most emerging issue is trust and certitude in the data origin. We need efficient, methodical and a business-like security framework with user privacy protection.

Security threats such as wormhole attack, message forging, privacy invasion, and black hole attack are most common in VANET [42] [43] [44] and as trustworthy communication is the basis of several applications in VANET, therefore, *"how to assess and provide data integrity and the trustworthiness of nodes among vehicles"* has turned out to be an increasingly significant issue that has received more attention in recent years. Numerous solutions have been implemented to facilitate secured communication in VANET which fall under two categories: trust mechanisms and cryptographic technology [45] [46]. The latter can provide security in VANET; however, it includes extra power consumption and time delay, thus restraining its applications in dynamic environments particularly, under limited energy [47] [48]. While cryptographic solutions work to render the confidentiality, integrity, and user authentication, the trust schemes are required to establish trust among the previously authenticated nodes. Trust schemes endeavour to expose 'greedy authenticated nodes' thus empowering the nodes to classify any nodes as trustworthy or malicious. But these schemes again rely on several factors such as gathering recommendation from the surrounding nodes regarding a message identification or looking for any direct interactions. If happened with the sender node, verifying received information with the one sensed by the vehicle itself or lastly cross verification with a trusted party, such as the Roadside units.

In recent years, researchers proposed robust trust management schemes and from that we can find out that these diverse trust approaches are categorized into three kinds: *"(1) vehicle node-based; (2) message-based; and (3) hybrid"* [49] [5]. In a complex VANET system, the trust model is a fundamental measure to assess the security of the network. In recent times, merging the "trust

management with the mobile model" was extensively deployed. The conventional trust model of VANET can be categorized into two approaches, the "direct trust model and cooperative computing-based trust model". The former one takes decisions regarding the signals and thus it leads to decision error, whereas the latter cooperates with other nodes and evaluates their trust values [3] [4].

The review under this section categorizes the existing schemes under centralized and decentralized models and analyse the methodology and technology used with performance measurement.

### 2.6.1. Centralized Models

Most of the VANET based schemes rely on multi-hop broadcast techniques, which suffer from issues such as, broadcast storm problem, hidden node collision, network congestion, and fragile connectivity. The issue of false alarms triggered by malicious users is solved by Trust based Dissemination Scheme [50] . Also, a unified trust management scheme is proposed to enhance security in CR-VANET [51]. The secured communication model is presented for alert spreading between 'active vehicles' that combines the power of AmI (Ambient Intelligence) and the V2V technologies [52].

The problem of routing security in vehicular ad-hoc networks has become a major concern. When compared to cryptography-based solutions, trust-based solutions are more acceptable as a promising approach, which mainly define two operations: trust computing and security application [45]. To identify and counter the attacker/malicious nodes an attacker and defender security game [53] is used which is also a trust model.

Recently, trust and reputation management has been proposed as a novel and accurate way to deal with the deficiencies [54] in the VANET. For enhancing inter-vehicular communication and preventing DoS attacks trust establishment scheme [55] can be used. Also, reputation management is focussed to ensure security protection and improve network efficiency in Vehicular edge computing [56]. The robustness against the tactical attacks, as well as the preservation of privacy by integrating trust management with the pseudonym technique [57] has been investigated which is also a reputation model which builds both service reputation and feedback reputation. Research is in progress for measuring direct trust and modelling indirect trust to vehicular social networks despite several research challenges [58].

In the following subsections we will discuss the centralized techniques with and without the blockchain technology.

#### 2.6.1.1. Centralized Models without Blockchain Technique

In 2020, [50] presented a novel reputation-based technique that computed trust-score for each node depending on its social- contribution, utility, and behaviour in the network. Numerical analysis revealed the significances of the presented scheme in terms of efficacy and accuracy. In 2019, [51] proposed a trust management approach that enhanced the security for both data transmission and spectrum sensing processes in CR-VANET. At the end, simulations were held, and the outcomes demonstrated the effectiveness of this method. In 2019, [42] presented a novel privacy-preserving technique based on the query processing model for VANET systems. Here, the proportion of query deliverance was found to be higher than the traditional approaches and privacy was also maintained at a better rate. In 2019, [45]analysed the trust properties and constructed a new trust inference approach, which included recommendation trust and subjective trust that quantified the level of trust for a vehicle. At the end, simulations were conducted which proved the efficiency of the presented scheme in resisting the attacks.

In 2017, [53] deployed the game theory-oriented trust approach for VANET. The adopted scheme was dependent on defender and attacker security game that identified and encountered the malevolent nodes. The advantage of the presented technique was demonstrated over the conventional schemes in terms of throughput. In 2017, [56] presented DREAMS technique, in which VEC servers were exploited for executing reputation management tasks for VANET. Experimental outcomes have offered greater advantages in detecting misbehaving vehicles.

In 2012, [54] established trust and reputation management, which was considered as an accurate and novel method for dealing with the unresolved risks. Furthermore, the analysis outcomes revealed the superiority and effectiveness of the presented scheme. In 2015, [58] introduced a social network model for analysing the trustworthy sharing of data in a VANET system. At the end, the simulation outcomes illustrated the improvement of the presented scheme in offering better security.

In 2017, [55] developed a model, which prevented the DDoS attacks and misbehaving nodes in an instantaneous, collaborative, and distributed manner. Moreover, a trusted routing model has accomplished that delivered data in a most consistent way. In 2016, [57] implemented a reputation-oriented model that exploited both feedback reputation and service reputation. Moreover, for preventing the tactical attacks, a feedback reputation model was also presented that detected the false feedbacks. In 2018, [52] developed a secured communication model among active vehicles for spreading alerts. By this novel approach, traffic accidental alerts were confirmed based on the trust range of the sender.

#### 2.6.1.2. Centralized Models with Blockchain Technique

In 2018, [59] exploited the blockchain technique that created a tamper-proof approach for overcoming the security issues. The adopted scheme has proved secured, tamper-proof mechanism with access control modes.

#### 2.6.1.3. Signature Schemes without Blockchain Technique

In 2019, [60] introduced an integrated security approach that assisted the nodes in VANET for identifying the authenticity of messages for better decision making. Finally, the simulated results demonstrated the efficacy of the implemented model. In 2018, [10] developed a secured CPPA approach for VANET. Accordingly, the presented solution has offered both privacy and security needed in a VANET appliance. Lastly, minimal overhead and computational cost were accomplished by the adopted scheme over the state-of-the-art schemes. In 2014, [61] implemented a new T-CLAIDS scheme for VANET. Moreover, a novel classifier was modelled for detecting the malevolent attacks in the network.

In 2015, [62] introduced the announcement model for VANET, which allowed the assessment of message reliability depending on a reputation system. Also, the investigational results revealed the improvements of the adopted scheme in terms of fault tolerance and security. In 2016, [63] presented a secured approach for managing both privacy and trust in vehicles in a flexible manner. Finally, the investigational results assisted the nodes in protecting privacy along with improved decision-making capability. In 2016, [64] adopted a novel scheme for protecting the privacy of vehicles against exterior eavesdroppers and it further concerned on managing the data trust/entity in VANET. Finally, the enhancement of the presented scheme was proved in terms of better decision making.

##### 2.6.1.3.1. Aggregate Signature

In 2019, [10] developed a big data anonymous batch verification scheme depending on a novel CL-AS algorithm. This technique has proved the superiority of the implemented technique with respect to efficiency. In 2010, [65] established a new trust-oriented model for message transmission and evaluation in VANET, in which the peers shared data on considering safety or road condition. Moreover, the efficiency of the implemented approach was demonstrated from the experimental results.

#### 2.6.1.3.2. Group Signature

In 2016, [66] established a new approach called PUCA that defended against the attacks, thus offering better privacy for varied users. In addition, numerous arithmetical illustrations were provided for analysing the privacy of the presented model over the traditional schemes. In 2015, [67] offered privacy and secure based approach for value-added appliances in VANET. Finally, the performance of the established scheme was evaluated in terms of security and malevolent detection. In 2018, [68] adopted a novel authentication approach that offered secured communications in VANET. Here, a fast and secure communicational link was established among TA and RSUs.

The arithmetical experimentation and evaluations revealed the efficacy of the adopted scheme in terms of security. In 2010, [69] presented a trust-oriented preservation approach for VANET. Moreover, simulation results have shown the betterment of the presented model in terms of reliability and accurateness.

#### 2.6.1.3.3. Ring Signature

In 2020, [70] established privacy preserved mutual authentication model that minimized the overhead and computational issues in VANET. It also concerned on minimizing the side-channel attack. In the end, analysis outcomes revealed the betterment of the adopted scheme in terms of the cost factor and it was much suited for large scale networks.

#### 2.6.1.3.4. Digital Signature

In 2015, [71] developed a new technique for distributing warnings among vehicles without depending on the road base. In addition, a novel "Active vehicle concept" was introduced that combined the ambient intelligence with VANET mechanism. In 2010, [72] developed a reputation management model for preventing the distribution of false messages. Finally, the experimentations illustrated the progression of the adopted model in terms of false message filtration. In 2010, [73] established a robust approach called VSRP for employing security in VANET systems. Moreover, the adopted scheme has dealt with the issues regarding the data dropping and data aggregation. In 2011, [74] exploited a trust evaluation approach depending on location verification and information in a NLOS condition. From the numerical analysis, the presented scheme has offered an improved success rate in message deliverance.

In 2015, [75] designed a lightweight and accurate intrusion detection model termed as AECFV, which protected the network in opposition to various risky attacks. Here, the outcomes have revealed better detection of attacks with

higher scalability. In 2014, [76] developed PPREM model that offered authenticated, concise, and explicit data regarding the revocation status, when maintaining the privacy of users. Thus, sensitive information could be protected from malicious attacks and risks.

#### 2.6.1.3.5. Blind Signatures

In 2011, [77] portrayed a novel Portable PAACP approach, which was deployed for non-safety appliances in VANET. Further, experimentations were carried out for revealing the scalability and efficiency of the developed approach.

### 2.6.1.4. Signature Schemes with Blockchain Technique

#### 2.6.1.4.1. Multi-Signature and Smart Contract

In 2019, [78] established a novel scheme depending on the blockchain mechanism for publishing the policies, which allowed the distributed transmission of right amongst users. In addition, numerous arithmetical outcomes were presented that portrayed the enhancement of the implemented scheme.

## 2.6.2. Decentralized Models

Trust management in a decentralized vehicular network is challenging due to the lack of centralized communication infrastructure and a fast-varying feature of vehicular environment [46]. Due to the non-trusted environments, it is difficult for vehicles to evaluate the credibility of received messages.

Blockchain is the emerging technology which attempts to solve the issues like efficiency and security by creating tamper proof event of records in a distributed environment [59]. Therefore, this technology can be used in which the vehicles can validate the received messages from neighbouring vehicles [11, 12, 47]. Also, it is crucial for VANET to prevent internal vehicles from broadcasting forged messages while simultaneously protecting the privacy of each vehicle against reconnaissance attacks [79]. So, a blockchain based anonymous reputation system [80] can be used to support privacy of participating nodes.

Also, the advantages of a distributed storage, such as IPFS can be used, as it improves data availability and prevents DOS attacks. It is a file sharing system that can be leveraged to store and share large files more efficiently. It relies on cryptographic hashes that can easily be stored on a blockchain [81], discussed in

a greater detail in Chapter 5. Also, it is appropriate to use a public blockchain that stores the node trustworthiness and message trustworthiness in a distributed ledger for secure message dissemination [82, 83]. Consortium blockchain and smart contract technologies are exploited to achieve secure data storage and sharing in vehicular edge networks [84].

In most of the privacy-preserving reputation systems it is observed that none of them is truly decentralized and possesses less trust. To overcome this, blockchain based decentralized privacy-preserving reputation system [85] is proposed.

In vehicular networks, early detection of malicious nodes, and accurate assessment of complex data to assess the node reliability are of absolute importance. So, security schemes like trust evaluation methods can be used which introduces a small-time interval to detect the changes in the node behaviours [49]. A privacy preserving reputation scheme protects users by hiding their individual feedback and revealing only the reputation score. So, a privacy preserving reputation protocol can be presented for the malicious adversarial model [86]. It can also be used to enable users to provide feedback in a private and uninhibited manner [87]. Location privacy in the mixed zone depends on the number of cooperative vehicles interacting within the spatio temporal environment. For this an incentive-based co-operation motivating pseudonym changing strategy for privacy preservation in mixed zones [4] is proposed.

In VANET, it is important to have effective trust establishment along with authentication. A neighbour communication-based trust management scheme is presented for secured communications in VANET [88]. A design for trust-based data detection scheme is presented which filter false safety events in VANET [64]. Also, a multi-faceted trust modelling framework is developed that incorporates role-based trust, experience-based trust, and majority-based trust and that can restrict the number of reports that are received [89].

#### 2.6.2.1. Decentralized Models without Blockchain Technique

In 2019, [46] introduced a decentralized trust management approach for VANET. Here, a trust calculation was performed based on fuzzy logic for computing direct trust of the nodes. The simulation analysis has revealed the betterment of the adopted scheme over the other compared schemes. In 2019, [48]presented a BTMS-FDD (Beacon Trust Management System and Fake Data Detection) approach, where the density and speed of information were exploited for establishing an association with neighbourhood vehicles. The experimental analysis illustrated that the presented model efficiently detected the malevolent nodes with reduced overhead. In 2019, [49] presented a security approach, which exploited the “evidence combination technique” for combining the local data with

exterior evidence. The experimentation illustrated that the presented method offered better outcomes in terms of better recall and precision.

In 2012, [87] presented a decentralized security-based reputation approach, which facilitated the users in offering feedback in an uninhibited and private manner. In the end, arithmetical experiments confirmed the efficiency of the adopted technique in increasing the probability of security. In 2013, [86] established a new privacy-preserving approach for the "malicious adversarial model". This approach does not require "centralized entities, trusted third parties, or specialized platforms, such as anonymous networks and trusted hardware". Finally, the experiments demonstrated the efficacy of the adopted scheme.

In 2014, [64] presented numerous issues regarding the current trust approaches in VANET and the ways to counter them were also discussed. From the analysis, the modelled technique offered improved "voting accuracy" when compared to the other approaches. In 2014, [90] modelled TEAM for carrying out communication in VANET. Moreover, the simulated analysis revealed better authentication and it defended against various attacks.

In 2017, [88] adopted an effective neighbour communication-oriented trust management approach for carrying out secured communications in VANET. Furthermore, the investigational outcomes were offered that confirmed the efficiency of the presented algorithm.

Following subsections discuss the signature schemes used under this model.

#### 2.6.2.1.1. Digital Signature

In 2018, [4] modelled an enhanced pseudonym approach and one-way hash function for evaluating the vehicular incentives that facilitated the privacy protection. In addition, the privacy of the presented scheme was analysed over other schemes for illustrating its betterment.

In 2006, [91] presented reputation management, which facilitated devices to get adapted to varying local conditions and trusty relationships. This approach offered accurate reputation-oriented trust along with better confidentiality. In 2016, [89] established a new complex trust modelling architecture, which incorporated majority -based trust, role-based trust and experience-based trust, by which the count of received reports can be restricted.

In 2016, [92] developed a secure trust-oriented framework that exploited the block chain mechanism for increasing privacy and security, by which the attacks in MAC layer could be minimized. Finally, the arithmetical experimentation demonstrated the efficacy of the presented approach in terms of reduced overhead, packet loss, and delay.

#### 2.6.2.2. Decentralized Models with Blockchain Technique

In 2019, [47] suggested a decentralized trust management model in VANET depending on blockchain methods. Here, the vehicles validated the received messages from adjacent vehicles by means of the "Bayesian Inference Model" and it offered feasible and effective trust values. In 2018, [83] developed a novel blockchain technique to solve the crucial message distribution concerns in VANET, for which a local blockchain model was created. From the analysis, the presented scheme offered better trustworthy ness over the other compared schemes. In 2018, [78] developed a new approach that relied on the deployment of smart auditable agreements in the blockchain mechanism. Further, the efficiency of the adopted authentication scheme was confirmed in a realistic scenario.

In 2018, [10] proposed a blockchain based authentication and revocation scheme, which utilised the capabilities of this distributed ledger, to quickly authenticate and revocate vehicles with reduced delay and bandwidth consumption

##### 2.6.2.2.1. Digital Signature

In 2018, [80] established BARS (Blockchain Oriented Anonymous Reputation System) that disconnected the linkability among public keys and real identities for preserving privacy. Finally, the outcomes revealed betterment of the presented model in offering improved security for VANET systems. In 2019, [82] introduced a novel blockchain model that resolved significant message distribution problems existing in the VANET. This work mainly concerned on the public blockchain, which ensured the trustworthy ness for the secure transmission of messages.

In 2018, [79] developed BARS for establishing a privacy-conserving trusted model for VANET. Finally, the analysis was conducted that proved the betterment of the adopted scheme in terms of efficiency and robustness.

##### 2.6.2.2.2. Blockchain and Smart Contracts

In 2018, [81] introduced a new approach that offered an updated version of IPFS, which deployed Ethereum smart contracts for providing file sharing in a controlled manner. Finally, investigational results revealed the enhancements made by the presented scheme.

In 2019, [11] proposed an IPFS and smart contract-based trust and reputation scheme, which shows improved performance using the automated capabilities of smart contract and distributed IPFS storage. In this scheme

feedback regarding events from the neighbouring nodes is evaluated using a smart contract, which computes the reputation score of the reporting vehicle and other neighbouring vehicles using the rules predefined in this contract.

IPFS storage serves the purpose of providing the reputation score on a node by node basis. Therefore, instead of relying on a trusted party for a reputation score verification, each node serves as the score provider.

#### 2.6.2.2.3. Digital Signature and Smart Contract

In 2019, [84] presented an efficient "smart contract and consortium block chain mechanism" for achieving secured sharing of data in VANET. The outcomes confirmed the betterment of the adopted model with respect to security and data sharing.

#### 2.6.2.2.4. Blind Signature

In 2016, [85] presented a technique based on a decentralized blockchain privacy-preserving reputation mechanism. In addition, the security and robustness were offered and accordingly, the need for trusting the third parties was eliminated.

## 2.6.3. Other Security and Trust Based Schemes

#### 2.6.3.1. Other Schemes without Blockchain Technique

In 2019, [44] established a novel SPBAC scheme, where the communication takes place using the onboard unit sensory devices. The analysis outcomes have shown that the presented method offered private, secured communication when distinguished over the traditional schemes. In 2016, [93] developed ART framework for VANET, which detected and resisted against the malevolent attacks. It moreover computed the trustiness of both mobile and data nodes in VANET. In addition, mobility and traffic security were found to be improved by the adopted model. In 2018, [94] established a novel approach, where a variety of security issues were identified for VANET and feasible security methods were provided for mitigating those threats. In addition, defence mechanisms were classified and examined depending on the performance measures. In 2009, [95] deployed the event-oriented reputation approach for preventing the spreading of

fake traffic warning messages. Further, the outcomes exhibited the capability of the adopted scheme in avoiding the spread of false messages.

In 2019, [96] implemented a TBRS for ensuring real-time security and data transmission in a vehicular CPS network. At the end, the outcomes have shown that the presented scheme could attain better reliability and delivery rate. In 2018, [5] introduced a novel method, which selected the reliable CHs depending on the hybridized model that combined the trust and stability factors. Further, the investigational analysis validated the enhancement of the implemented scheme in terms of cluster stability and data sharing. In 2018, [3] developed a flexible and secure approach for VANET system that managed both privacy and trust. It further allowed the nodes in computing the reliability of received events by concerning the privacy of the senders. On carrying out an extensive analysis using the adopted model, the accurate decision was taken in a flexible manner.

In 2018, [90] dealt with a novel TEAM model that served as a distinctive prototype for the management, design, and valuation of trust models. In addition, the efficiency of the analysis was confirmed against various attacks and security conditions. In [97] developed a novel reputation and trust management approach for VANET. In addition, a similarity mining method was exploited for detecting identical vehicles or messages. Thus, a trustworthy message could be identified by the presented method.

#### 2.6.3.1.1. Fuzzy Logic

In 2018, [98] deliberated a TMR for defending the varied attacks and moreover, the routing efficiency was improved. In addition, the efficiency of the introduced scheme was demonstrated through e2e delay and overhead.

### 2.6.3.2. Other Schemes with Blockchain Technique

#### 2.6.3.2.1. Fuzzy Logic

In 2018, [99] established a novel distributive trust management model for verifying the accuracy of the message for VANET. Here, the trust was verified by controlling the behaviour of vehicle by a miner and accordingly, the trustworthiness of the message was verified by CHs.

## 2.6.4. Disadvantages of Existing Trust based Schemes

The self-made decentralized network demands the potentiality to grant each node capability to derive the reputation of every other node. It becomes important that unlike some centralized proposals [100] they should be self-sufficient, due to the absence of any reputed (centralized or decentralized entity) to continuously monitor the functional and behavioural capabilities of the nodes. After analysing the existing works, especially [54, 93, 101-106], that have been done for accurate evaluation of a vehicle's trustworthiness, we can find out that they rely on various criteria for assessment. A few models draw reputations from data-based trust model, while others are more focused on entity-based trust model, and role-based trust model [101]. But a definitive trust model should drive upon a hybrid approach to build a vehicle's trust and it should not solely be dependent on a single trusted party. Among all these works, some are centralized, while a recent shift has been observed towards decentralization.

In a centralized trust inference, the centralized trusted source manages information by gathering multiple inputs and producing an output without any transparency with other vehicles, but as per the nature of the network, each vehicle should not just have independent rights to query the reputation of a node, but also, contribute to its evaluation process, with a clear view of what happens behind the scenes. While the decentralized works that have been proposed in literatures[54, 93], they still rely on a centralized party for disseminating and concealing the reputation information. After analysing some of the critical requirements of a trust and reputation evaluation model, work has been done towards fulfilling those in the proposed trust model. The proposed trust and reputation model stand by to substantiate impregnable requirements in VANET, with proven resolution to decentralization, transparency, reduced latency, dependency on a centralized trust system and more accurate detection of false messages.

### 2.6.5. Our Scheme and its Achievements

The aim is complete decentralization and cost effectiveness, so rather than storing the data in the blockchains as proposed in [79, 80], most of the data is stored in Interplanetary file system (IPFS) network which is cheap and thus allows us to store more data. The former creates an immutable record of transactions that happened amongst the peers, while the later strives to execute a set of instructions upon triggering of an event. The messages transmitted (in the form of transactions), are recorded as it can be a proven history to ensure nonrepudiation and establish reputation of vehicles based on the validity of messages transmitted and the reputation score maintained. The distributed IPFS [6] network is the storage and retrieval repository used for sharing and storing the reputation of nodes. The proposed trust model encompasses following characteristics to have an unimpeachable, robust, and reliable outcome.

**Light, scalable and fast:**

*Highly dynamic topology:* The scheme considers the frequently changing topology, which requires a distributed approach as most traffic conditions require minimum processing time with minimum computation overheads.

*Latency issue:* There is minimum dependency of information from surrounding mobile nodes or static units (such as the RSUs). The amount of time needed in gathering information to assess the trustworthiness of node is directly proportional to the latency in tackling such situations.

**Accuracy of Reputation evaluation:** The scheme considers previous history of the node (identity and its behaviours), current involvement in any fair/false communication and evaluates accordingly.

**Protection against Collusion attacks/ Fair evaluation**:

*No-bad mouthing:* To avoid bad mouthing, a decentralized blockchain and smart contract network with a quick consensus algorithm is deployed for reputation evaluation. Before a node adds the reputation, score corresponding, it is verified and then added.

*Collusion attack:* Colluded bad-mouthing or commendation should be completely avoided.

**Independence of node's movements:** As the nodes move along different roads, highways and pathways, the deployed trust model should be accurate irrespective of the paths taken by a node. The proposed scheme is independent of the route taken and does not presume for a specific path for evaluation.

**Privacy Preservation:** In the process of reputation score evaluation, accepting and forwarding messages, the real identity of the nodes is not revealed.

**Reputation Evaluation:** How trustworthy is the data and the node? Upon reception of a message, following factors are considered in evaluating the extent to which a node can be trusted:

1. *The reputation of the node sending the information*
2. *How many nodes are sending the similar information over a period and their corresponding locations?*
3. *How many other nodes are recommending this node sending the information?*
4. *How can these nodes be queried for reputation scores?*

## 2.7. Advantages and Disadvantages of Existing Systems

### 2.7.1. Advantages of Centralized Systems

In a centralized system, all users are connected to a central network owner or server". It is simpler to set up and it can be designed speedily.

- Simpler deployment
- Affordable for maintenance
- Practical when data requires to be centrally controlled
- Can be quickly developed

### 2.7.2. Disadvantages of Centralized Systems

- High privacy and security risks for users
- Risk of failures
- Consumes more access time for users who are at a longer distance from the server

### 2.7.3. Advantages of Decentralized Systems

"As its name implies, decentralized systems don't have one central owner; instead, they use multiple central owners, each of which usually stores a copy of the resources users can access".

- Improved performance
- Less likely to fail when compared over a centralized system
- Permits for a more flexible and more diverse system

### 2.7.4. Disadvantages of Decentralized Systems

- Privacy and security risks to users

- Higher costs for maintenance
- Performance remains inconsistent if not properly optimized.

## 2.8. Summarizing Research Gaps and Challenges

In VANET, the vehicles are roving on roads and they dynamically vary in topologies around urban or rural areas. The speed of vehicles gets varied depending on the diverse types of road or traffic conditions. While moving at a higher speed, it seems to be difficult to control the position of vehicles. Therefore, it is essential to establish authentication and gain trust with other associated information of vehicles in real-time. VANET is an open and decentralized system [63, 64]. Therefore, there is a feasibility that any vehicle can leave and join the network at any time. However, there is no other method to "meet next time within the network for after communication with the particular vehicle". This may lead to false information to be transmitted by the adjacent node that affects the entire network performance. Thus, false positioning is received by malevolent nodes, which affect traffic-jams on roads and raise the possibility of accidents on roads. Higher mobility in VANET is owing to the random speed of vehicles i.e., On the freeway, vehicle speed ranges up to 60-100 km/hr, i.e., vehicles move quicker since it requires higher transmission power among nodes [65, 90].

Moreover, vehicles move at random in any route on roads and hence, a long-term relationship is not maintained among the nodes/peers. As the condition of the road is dynamic, the actual or traffic condition of nodes cannot be predicted exactly. It is necessary that vehicles are not only authenticated with reduced dependency on the trusted third party but, also preserving their anonymity without revealing the original identity of users. It should not be dependent on the circulation of CRLs by the *CA* or *RSUs.* Though most of the researches in VANET focusing majorly on the security aspect have predominantly addressed authentication and conditional privacy issues, but they lack to suffice the scalability, efficient authentication, quick check on revocation to reduce dependency on the centralized authority.

In addition, while evaluating the trust level of nodes, the vehicle node-oriented techniques eliminate the corrupt nodes from VANET [57, 72]. Still, these techniques do not take account of the quality of message and it assumes that "if a node is trustworthy, then the messages from this node are also reliable". As per the theory of message-oriented techniques, the data quality is said to be the only aspect that impacts the trustworthiness of communication. These techniques compare a set of messages against exchanged data delivered by honest nodes that might cause further cost and delay when a huge dataset was deployed. Further, once a trust management system is established it should restrict the access to

trustworthy nodes only to strengthen the security of communication, which not many schemes have considered.

## 2.9. Conclusion

This Chapter presented a detailed review on authentication, trust, and security in VANET systems. Various works have been reviewed and their advantages and disadvantages have been studied in detail. We discuss how our scheme overcomes the disadvantages of these existing schemes in our proposed framework. Moreover, we differentiate the schemes based on their centralized and decentralized nature and compare them, to understand why it's important to reduce the dependency on a centralized party and move towards decentralization.

# Chapter 3

# Background Studies - Blockchain

*In 2008 blockchain emerged as the foundation of first ever decentralized cryptocurrency which not just revolutionized the financial industry but proved a boon for peer-to-peer information exchange in the most secure, efficient, and transparent manner. Blockchain is a public ledger which works like a log by keeping a record of all the transactions in a chronological order, secured by an appropriate consensus mechanism and providing an immutable record. Its exceptional characteristics include immutability, irreversibility, decentralization, persistence, and anonymity. With these advantages, it has found applications in almost all fields suffering from data sharing among multiple parties but with secure authentication, anonymity, and permanent record. Some of the applications are finance, real estate, and IOT security.*

*With numerous advantages in VANET, comes the security risks and disadvantages given the open nature of the vehicular communications. Numerous researchers worked extensively in this direction to resolve the issues and propose solutions, as reviewed in chapter 2 of this thesis, where we conclude that most of these works require a centralized party to work as a trusted intermediary in establishing secure communication between the Road-Side Units (RSUs) and On-Board Units (OBUs).*

*This chapter is a detailed study of the blockchain technology, which provides the foundation for the proposed decentralized security framework. The comprehensive study elaborates the basics of blockchain, followed by its working model, the phases of operation within, the different kinds of blockchains, the different consensus used by them, and finally its applications. We extracted the best blockchain suitable for the framework with the fitting consensus mechanism. The capabilities and advantages of this technology have been fairly exploited within the framework while its limitations have been worked upon for improvisation. The aim of integrating this technology in the proposed security framework is to reduce dependency on a centralized party thereby reducing the latency and bandwidth consumption in the dynamic VANET environment.*

## 3.1. Introduction

With the eruption of internet, came digital communications, empowering all forms of data and information interchange through online transactions, primarily the financial transactions for making payments and receiving funds. It also enabled simple file communications carrying confidential data (such as an email). The entire transactional and communication system this goes through a trusted intermediary which not only guarantees safe and secure delivery, but in case of financial transactions, ensures accurate changes being reflected in multiple accounts. This trusted party is questionable in case of any failures in updating data, delay in delivery or fraud. But with just a single network controller multiple questions arise:

1. What if this trusted party goes rogue and can't be trusted enough for any data exchange?
2. What if its hacked and an attacker gets hold of all the data? This intermediary here acts as a single point of failure.
3. Each time going through an intermediary creates additional delay in communication, then why not communicate peer-to-peer?
4. The authenticity and validation of each transaction is very important, but can we really trust the intermediary?

The solution to all the above problems, is served by ***Blockchain***, the underlying technology employed by satoshi nakamoto (considered a pseudonym) in introducing the first ever decentralised cryptocurrency called as **'Bitcoin'** [8, 107, 108]. Bitcoin exchange and transfer occur by means of a shared distributed ledger, which records the details of every transaction occurred among the network participants without involving any trusted centralized party. The copy of the ledger resides in synchronization with all the involved parties, thus reducing the risk of a single point of failure. Bitcoin works on Public Key Infrastructure (PKI) in blockchain for authenticating anonymous users and controlling access. Users can access their bitcoins in possession with their private key whereas the public key acts like the user identity or address (just like e-mail) where other users on the same network can send them bitcoins. For source authentication and identification, each transaction is digitally signed by the owner with its private key. Since multiple transactions occur in the network at a time, so to keep a track of all the transactions occurring simultaneously, multiple transactions are grouped together in a structure called as a 'block' uniquely identified by its hash and timestamp. Now validation of transactions and the block, among distrusted users is done using a consensus mechanism, which means the state of the shared ledger is updated by the agreement/consensus of majority of nodes. This updating in case of bitcoin employs the proof-of-work consensus algorithm, whereby

miners strive to find a special value to achieve the block's hash, less than a target value, which is usually set to avoid any conflicts and establish trust. In case of bitcoin, this target value is set in such a way that miners compete to find a nonce in around 10 mins, hence the block generation time is 10 mins. This process by which nodes perform rigorous computations, thus devoting their resources (such as CPU, electricity, etc) to find the nonce is called as *mining* and the nodes doing so are called as *miners*. Through mining, nodes compute the proof-of-work which is a form of achieving consensus among the distrusted modes.

This continuous generation of transactions and thus formation of blocks leads to the creation of 'Blockchain' which can be defined as a cryptographically secured list of blocks chained together and ordered by the timestamp. The logs of digitally signed transactions are grouped together and sealed in timestamped blocks, validated by miners using a predefined consensus mechanism (such as proof-of-work). The blockchain characteristics [109, 110] are depicted in Figure 3.1.

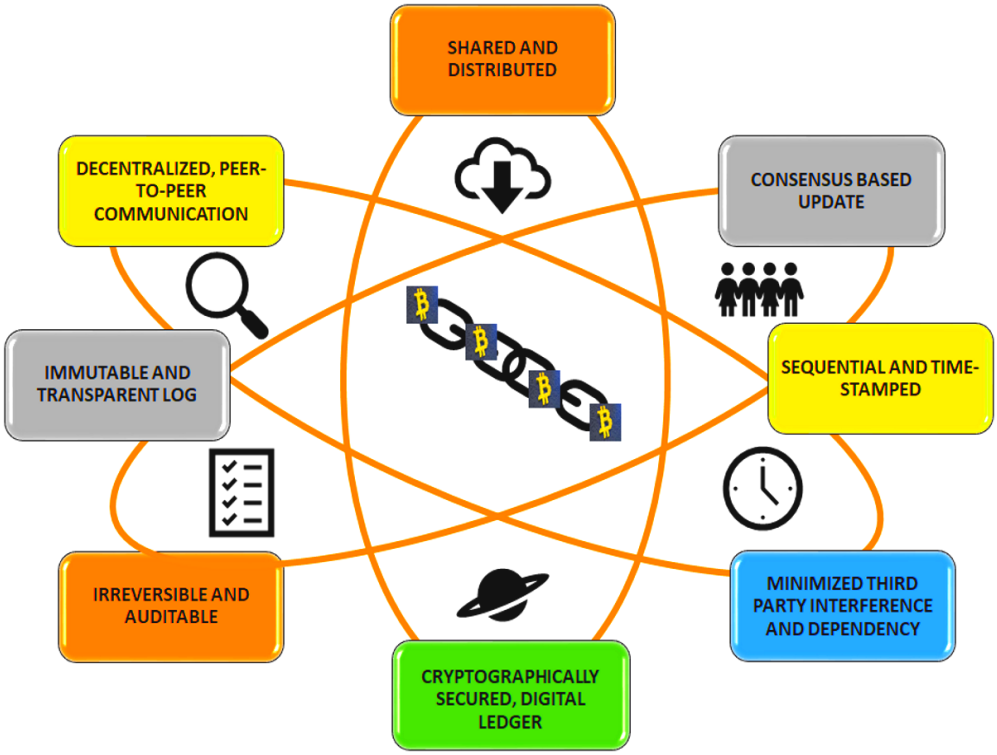


*Figure 3.1 Vital Blockchain characteristics*

## 3.2. Working Model

In this section we explain the core components fabricating the blockchain network setup and their importance. Then we discuss the different phases of blockchain functionality, where these components collaborate in performing

secure communication among distrusted nodes (rogue) by publishing a distributed log of the committed transactions, using a consensus mechanism. Next, we give an overview of the stepwise network operation. The bitcoin blockchain has been taken as an example here to illustrate most of the blockchain functioning.

### 3.2.1. Core Components

The blockchain setup and network operations are built upon the following core components as shown in Figure 3.2:

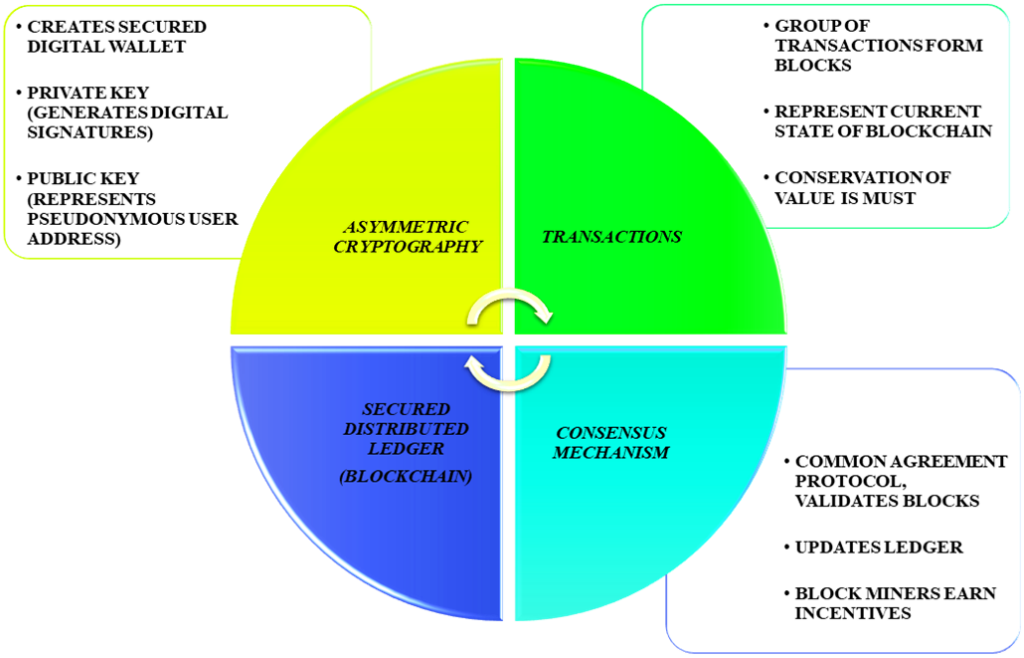


*Figure 3.2 Core components of blockchain*

#### 3.2.1.1. Asymmetric Key Cryptography

The blockchain network utilizes the capabilities of the public key cryptography for secure operations of the blockchain. To perform any exchanges, users other than being on the same platform, need to possess a digital wallet (functioning like a bank account) secured with user's private key, and accessible with appropriate signatures generated using that private key. This wallet's public key serves as the bitcoin address known to everyone, which is advised to change with each transaction for maintaining privacy and anonymity of users. Private keys are used to digitally sign transactions and are kept secret by the user. It is very important to preserve the private key in a secret location and manage in a

such a way that it's not leaked, because considering the nature of blockchain, losses incurred by faulty and fake transactions are irreversible as private key is the only means of user identification.

Although means to recover in case of private key loss are discussed in literature, but it is advisable to keep a backup and frequently change the key-pair to avoid such circumstances. This is because, till the time a new pair is allotted, the old one is functional and it will continue to cause damage and vandalization, which at times, is irrevocable.

#### 3.2.1.2. Transactions

Blockchain enables the sharing and exchange of information among the peer nodes. This exchange takes place by means of files containing transfer information from one node to the other, generated by a source node and broadcasted to the entire network for validation. The current state of blockchain is represented by these transactions, which are continuously generated by the nodes, and then congregated in blocks. Depending upon the application of blockchain, the transactions can represent records, funds, or contracts. In case of bitcoin, each transaction exhibits the transfer of currency from one node to the other. All the nodes are aware of the current balance at each address and maintain a copy the existing blockchain, which is the log containing history of previous transactions. The state of blockchain changes after each transaction, [111] because state exemplifies the current balance in each wallet, which changes post execution of transaction files, when inputs are redeemed, and outputs are produced. With a huge number of transactions generated each second, it is very important to validate and verify the genuine ones and discard the fake ones.

#### 3.2.1.3. Consensus Mechanism

When nodes begin data sharing and exchanging via a blockchain platform, they do not have a centralized party to regulate and resolve disputes or safeguard against security violations. This communication network with distrusted nodes makes it infeasible to perform secure peer-to-peer communication in the absence of a central coordinator and therefore, we need a mechanism to keep track of the flow of funds and ensure an unassailable exchange to avoid any frauds, such as the double spending attacks [112, 113]. All the nodes should agree on a common content updating protocol for this ledger, to maintain a consistent state and blocks should not simply be accepted to be a part of the blockchain, without majority consent. This is called as a consensus mechanism, by which blocks are created and added to the existing ledger for future use. In case of presence of a centralized authority such as a bank, records of each account, balance and transactions are

maintained to avoids any frauds or fake transactions. But in case of bitcoin, recipients after signature verification, might redeem outputs multiple times for use in subsequent transactions as they would seem valid by individual recipients. Thus, solely, for avoiding the double spending, Satoshi was the first one to propose a consensus based decentralized cryptocurrency among non-trusted nodes. This consensus is an agreement amongst the nodes, which involves block mining, wherein miners compete to find the next valid block by computing a cryptographic block hash beginning with 'n' number of zeros. Nodes finding the solution are rewarded with some bitcoins, thereby generating new currency. This hash value is called as the proof of work and if all the transactions and proof-of-work is valid, nodes accept it by updating their copy of the blockchain, otherwise, the block is discarded, and nodes continue to find a valid solution.

These components form the transparent log of transactions called as the blockchain, which is a cryptographically secured shared ledger for anytime reference, among the participants of the distributed network.

### 3.2.2. Phases of Operation

Complete block formation process in blockchain is splitted into two phases:

1. Transaction generation and verification
2. Consensus execution and block validation

#### 3.2.2.1. Transaction Generation and Validation

We explain the complete process of transaction generation, their verification, and claiming ownership of funds under this section.

##### 3.2.2.1.1. Contents

Users connected within the same network have knowledge of each other's address before they begin any transfer. When a new transaction is initiated, it includes input transactions, the amount to be transferred and recipient's bitcoin address. For example, Sheryl needs to transfer 5.0 BTC to Alice, then the transaction executing this transfer contains:

A. *Input Transactions:* These are the source/descendant transactions whose unused transaction outputs (UTXO), serve as an input in this transaction. In other words, it refers to the hash of the transaction which supplies the record that from what source Sheryl earned that 5.0 BTC in her bitcoin

wallet she intends to transfer. These can be one or more transactions whose sum turns up to be 5.0 BTC. Say for example, there are 4 transfers received from multiple sources whose sum is 5.0 BTC and these have already been published in the ledger, then there would be 4 input transactions for the next transfer. The outputs of the transaction depend upon which all places she would split and send these 5.0 BTC.

B. *Amount to be transferred:* The amount transferred is 5.0 BTC in this case

C. *Public key hash of the receiver:* This is Alice's bitcoin address where she would receive the 5.0 BTC. Transactions are uniquely identified by their transaction ID, which is the SHA-256 hash value of the input transaction and public key of recipient as presented in equation 1. This is further encrypted with sender's private key for generating digital signatures to assist recipients in uniquely identifying the source. If any content is changed, it would consequently affect the Transaction ID as well as the signatures, and in case of mismatch the transaction is discarded.

*Transaction_contents = Hash (input_transaction || Public_key_of_recipient)*

*Digital signature = Encrypt (sender_private_key)*

#### 3.2.2.1.2. Confirmation of Transaction

When Alice learns about Shirley's transaction crediting funds to her bitcoin address, she needs to confirm that there is no double spending by Shirley and that the transaction has been confirmed with its existence in a valid block of the ledger. Till the time the transactions are not confirmed, they are not considered trustworthy. Transactions are committed only if, upon reception of the transaction, Alice could verify for the following:

a. The referenced *input's transaction's UTXO is valid* i.e. there is not double spending. Satoshi, to prevent double spending in bitcoin, proposed that the output of a transaction can be redeemed in following one subsequent transaction, and only after its successful verification both via signatures and ledger entry, the output could be redeemed in another transaction.

b. Since only the user authorized to access the UTXO can use it in a subsequent transaction, the recipient checks for the *valid signature* which should match with the UTXO owner signature.

c. The referenced transaction must be *published in a valid block*. The existence of a transaction in a block confirms its validation.

d. *Conservation of value is must*, which means that during the transfers, its mandatory that the sum of input UTXOs equals the sum of output UTXOs, subtracting the amount of coin base transactions. This is called as conservation of value and is the most important in checking a transaction's validity.

Figure 3.3 shows the transaction broadcast and verification among the network nodes.

Bitcoin blockchain consists of many nodes owing to its permission less nature, which leads to loads of transactions simultaneously broadcasted in the network. Hence, it is not necessary that all the miners include this transaction just in the next block they mine and therefore, the next block received by Alice might not contain Shirley's transaction. A block is mined in approx. 10 minutes of time and thus not getting included in the next block causes prolonged delays. But, with a greater number of miners the transaction might be included in more than one blocks also, leading to a greater number of confirmations, thus making it permanent. As more and more blocks would be mined on top of the one containing this transaction, so, after 2-3 hours the transaction becomes *irreversible and immutable*. The details of block validation are elaborated in the next section.

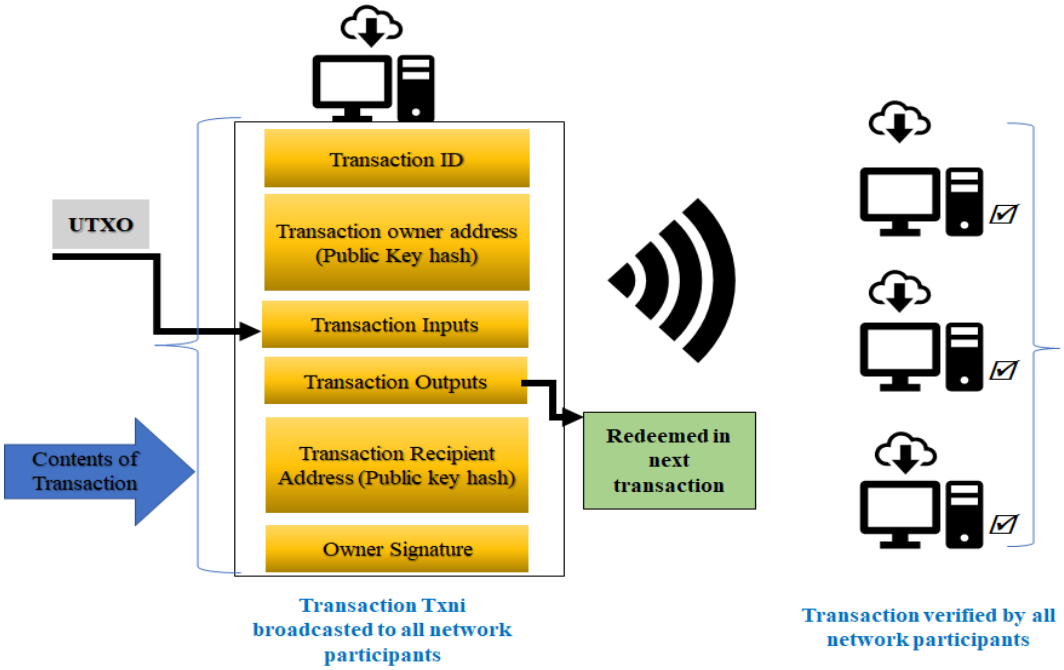


*Figure 3.3 Transaction broadcast and verification*

### 3.2.2.1.3. Claiming Ownership

Every transaction produces an output redeemable by the recipient nodes authorized in the public key hash of the transaction. This public key hash

authenticates users by uniquely identifying them in the network while preserving their privacy. Apart from this pseudonymous identity, users need a private key to control access to their bitcoins. Only those users who can generate valid signatures with their private keys can claim their ownership for redeeming transaction outputs. Thus, a public key hash and a private key are the essentials to enable users redeem funds. The amount redeemable is the amount owned by users, no more, no less.

#### 3.2.2.2. Consensus, Mining, and Block Validation

Nodes, in the absence of a trusted party follow a consensus on how to confirm or discard blocks and transactions with mutual efforts so that there aren't any conflicts at a later stage. This consensus in bitcoin is achieved by 'proof-of-work' which proves how much work has been put in for validating a block. A cryptographic puzzle is to be solved for acceptance of any block and its addition in the shared ledger. This works by nodes accumulating the verified transactions in a block and putting their resources (such as computation power and electricity) to find a value that makes the SHA-256 hash value of this block less than a dynamically varying target value. The block contents include, the arbitrary nonce, hash of the previous block, Merkle root hash of the listed transactions, timestamp and block version. The term 'proof-of-work' refers to this random value, which is found by the miners, by repeatedly hashing the block contents with many such random values to achieve the Cryptographic block hash. The hash should particularly begin with a set number of zeroes for greater security and increasing the block mining period. The nodes to first solve the puzzle and find solution add an additional transaction called as coin base transaction, for claiming the reward points and the block is then broadcasted to the network for verification.

The necessary steps for block validation are summarized as follows:

1. All the transactions contained in the current block are verified by the steps discussed in following section. After individual verification, transaction's chronological order conforming to their occurrences and references is confirmed.
2. The previous block's hash referenced by the current block exists and is valid. This is usually checked from the genesis block.
3. Accuracy of time stamp is verified.
4. The proof-of-work for the current block is valid.

### 3.2.3. Network Operation

The network operation steps are defined as follows by the order of their execution.

a. *Transaction broadcast:* There would be no direct transactions between source-destination, instead all transactions would be announced to the entire network for verification through broadcasting.

b. *Transaction collection and verification:* Nodes verify all transactions as per steps in following section and accumulate them in a block, depending upon the block size, which is 1MB for bitcoin.

c. *Running consensus protocol:* To add this block to the blockchain, nodes put their resources at work and start the mining process to solve the cryptographic puzzle by finding 'Proof-of-work'. Upon solving the puzzle, the block is broadcasted to the entire network.

d. *Block acceptance and chain update:* Upon reception of blocks by nodes, two scenarios can occur:

    1. Either nodes *accept* the block, provided that all transactions contained in it are valid and the computed proof-of-work is correct. Nodes show their approval and acceptance, by adding the block to their copy of the ledger and advancing to find the next valid block, with this block as a predecessor, and taking its hash as the previous hash for the successive block. In case, two miners find a valid solution at the same time, only longest blockchain is considered valid. This is how the blockchain is made tamper-proof and changes once made cannot be reversed.

    2. If the transactions in this block or proof-of-work isn't valid, the block is discarded, and nodes continue to find a valid block.

e. *Earning Incentives:* Miners earn incentives upon successful acceptance of blocks. This is to keep nodes honest and make the system robust.

## 3.3. Classification of Blockchain Systems

The blockchain networks give an opportunity to run decentralized trusted systems secured by appropriate consensus. But, based upon several criterions, the blockchain systems can be classified as public, private and consortium blockchains. These are explained in detail as follows:

### 3.3.1. Public Blockchain

A public blockchain gives an open platform for the people from various organizations and backgrounds to join, transact and mine. There aren't any restrictions on any of these factors. Therefore, these are also called as *'permission less'* blockchains.

Users can simply start by obtaining an address (to uniquely identify them among the nodes), which can change multiple times with proceeding transactions, thus maintain anonymity of the users. Every participant is given full authority to read/write transactions, perform auditing in the blockchain or review any part of the blockchain anytime. The blockchain is open and transparent and there are no specific 'validator nodes. All users can collect transactions and begin with the mining process, to earn mining rewards. The availability of the copy of blockchain synchronized with all the nodes makes it immutable.

Now, with complete decentralization, vastness of network, and an open platform for anyone to join, consensus is achieved by any of the decentralized consensus mechanisms such as proof-of-work, proof-of-stake, etc.

It has advantages of being completely decentralized, permission less, open, transparent, and immutable but simultaneously offers disadvantages of being less efficient and faces scalability drawbacks. The issues of scalability arise in these networks due to many factors, such as:

1. The number of transactions in a block, which are limited to a maximum of 7 per second for bitcoin, 20 per second for Ethereum, which are very less considering the transactions generated by the network participants.
2. The amount of time taken to confirm a transaction.
3. The amount of time taken to reach consensus which is roughly 10 minutes for bitcoin.

### 3.3.2. Private Blockchain

It is a type of blockchain system which is setup to facilitate private sharing and exchange of data among a group of individuals (in a single organization) or among multiple organizations with mining controlled by one organization or selective individuals. It is also called as a permissioned blockchain since, unknown users cannot get access to it, unless they receive a special invitation. Nodes' participation is decided either by a set of rules or by the network in-charge, to control access. This inclines the network more towards centralization, while derogating the elementary blockchain features of complete decentralization, and openness as defined by satoshi in bitcoin blockchain which is a core public network.

In a private blockchain system, once nodes become part of the network, they contribute in running a decentralized network, with each node maintaining a copy of the ledger, and collaborating to reach a consensus for updating, but unlike public blockchain the writes are restricted. Considering the centralization of a selected nodes performing the mining, fake transactions and irreversibility cannot be guaranteed, but their control can be advantageous in situations where it becomes necessary to modify or reverse transactions. Thus, in a private blockchain,

a. Not everyone can review or audit the blockchain. Only a group of authorized nodes as defined by the network in-charge or starter can perform mining.
b. Only nodes who are part of the network have the read/write access. This restricts what is open and transparent in public blockchain.
c. The most important part is the transaction fees. Transactions are cheaper as compared to the public blockchain. Here, limited nodes with high processing power verify the transactions, thus reducing the per transaction fees.

### 3.3.3. Consortium Blockchain

A consortium blockchain can be considered as a *partially private* and *permissioned* blockchain, where not a single organization but a set of pre-determined nodes are responsible for consensus and block validation. These set of nodes decide, who can be part of the network and who can mine. For block validation, multi-signature scheme is used, where a block is considered valid, only if it signed by these set of nodes. Thus, it is a partially centralized system, owing to the control by some selected validator nodes, unlike private blockchain which is completely centralized, and public blockchain which is completely decentralized.
It is decided by the consortium whether read or write permissions would be public or limited to the network participants. Also, the restriction of consensus to a set of nodes, doesn't guarantee immutability and irreversibility, since control of consortium by majority can lead to tampering of the blockchain.
Concluding, we can say that three fundamental questions determine the classification of the types of blockchain. First, who has the right to take part in consensus and block validation. Second, who can read/write transactions and third, who can perform auditing and review.

## 3.4. Consensus Algorithms

A consensus in a decentralized and distributed network with distrusted users is the sole and imperative determinant of the next secure update of their shared state. Consensus ensures the secure and consistent update of the copies with all the participants. The blockchain network takes a previous shared state

and current inputs to produce a new state conforming to a pre-defined set of rules, called as a consensus mechanism. For e.g., the solution of a cryptographic puzzle (producing a hash) in case of bitcoin, for production of a new block, replicated across all the nodes. States in blockchain are composed of transactions, which form blocks, transparently reflecting the current assets (such as currency in case of bitcoin) with each node. With new transactions being generated every second, the values of previous transactions are subject to change, thus altering the current state. The confirmations of state change occur only after agreement among the network participants, determined by the consensus rules, to ensure unambiguity in the new state replicas. We present the various approaches to achieve consensus in a blockchain network.

### 3.4.1. Practical Byzantine Fault Tolerance Algorithm (PBFT)

The PBFT algorithm was proposed by the authors in [114] as a solution to the Byzantine General's problem [115] , which is about conducting a successful attack on a rival city by the Byzantine army. For the Byzantine army to win, first, all the loyal generals work on the same plan and attack simultaneously. Second, no matter what the traitors do, the loyal generals should stick to the decided plan and a small number of traitors should not let the loyal go for a bad plan. Similarly, in blockchain, PBFT works to establish consensus among the participating nodes. Nodes maintain a current state, which upon reception of a new message is fed together with the message received for computations, to help the node reach a decision. This decision is then broadcast to the network. Majority of the decisions determine consensus for the network.

After bitcoin, some of the recently emerged cryptocurrencies such as ripple and stellar use PBFT for their network consensus. Moreover, Hyperledger [116], which is working for developing consortium blockchain systems for businesses utilize PBFT as its underlying consensus mechanism.

### 3.4.2. Proof-of-Work

Proof-of-work was the first decentralized consensus protocol proposed by Satoshi Nakamoto, to achieve consistency and security in the bitcoin network. In bitcoin, currency transfer occurs in a completely decentralized fashion, thus requiring a consensus for authentication and block validation. The nodes in the bitcoin network compete together to calculate the hash value of the next block, which is supposed to be less than a dynamically varying target value, determined

by the consensus rule. Nodes achieving the solution, wait for mutual confirmation by other nodes, before adding the block to the existent blockchain. More than one valid block might be generated, if multiple nodes find an appropriate solution causing a temporary fork(branch) in the network. In such scenarios, all of them are acceptable and nodes closer to the miners accept the solution they receive and forward the same to other peers. The conflict at a later stage is avoided by accepting the 'Longest version' of the chain available at any time. Thus, nodes receiving two valid blocks simultaneously wait for the next block appended to the previous version, and whichever gets longer, it is considered authentic. Nodes work honestly, since they are rewarded with incentives upon finding of the solution, but finding the PW requires too much of computation power and electricity and thus no energy saving.

### 3.4.3. Proof-of-Stake

Proof-of-stake was proposed to overcome the disadvantages of excessive power consumption by POW in bitcoin. Ethereum utilizes POS to achieve consensus in the network. Instead of investing in resources which can perform rigorous computations for hash calculations in POW, POS proposes to buy cryptocurrency and use it as their stake in the network. Their stake is directly proportional to their chances of becoming the block validator, greater the stake, more are the nodes' chances to become part of the validator set. To reach consensus, the block validator is randomly selected and is not predetermined. The nodes producing valid blocks get incentives, but if their block is not included in the existing chain, they also lose some amount of their stake. Ethereum uses the best POS algorithm, called as Casper, which resolves the Nothing-at-Stake problem of naïve POS algorithms. POS suffers from this issue, because nodes can vote for multiple forks to win rewards, because they do not pay any amount of their stake for voting, unlike POW, where going for multiple forks would require distribution of their computation power to go for correct block in both branches.

In [117], different consensus models have been differentiated based upon several factors such as:

a. *Type of blockchain* – It specifies whether the blockchain network is permissioned or permission less.

b. *Transaction rate* – It indicates at what rate are transactions confirmed, which is basically decided by the consensus algorithm. In bitcoin, which employs POW, the transaction rate is only 7 transactions/sec, because POW requires lot of computation time and the block generation time is 10 minutes

c. *Scalability:* A blockchain system is scalable, if it can achieve consensus with number of nodes continuously growing, especially in public blockchain systems.

d. *Participation charges:* For some systems, initially cost of participation is required, say for e.g. with POS, nodes invest in the cryptocurrency, to express their interest in the consensus and block validation, whereas POW requires energy input, which isn't necessary if you simply want to be part of the network and do not wish to mine.

e. *Trust condition:* This determines if the nodes contributing are to be trusted and predetermined, just like in consortium and private blockchain systems or unknown like in public and POW based blockchains.

## 3.5. Applications and Use-Cases

The blockchain has the capacity to revolutionize the security, stability, and transparency of networks in need, provided applied appropriately and only if needed, because it's not a panacea for all security applications. Following are some of the areas where blockchain finds its application and is currently being used owing to its advantages.

**Blockchain in Asset Management** - It is all about securely transferring assets within a business network. An asset could be a physical one like a server, computer or a laptop or an intangible one like software and services. As the assets are transferred across the business network, it's not just within the enterprise, it could be all the way from a part supplier to the manufacturer, to your distribution network and all the way to your final client. What we get blockchain is shared ledger capability which mean we get full visibility from end to end into that business network. Some of the conventional pain points faced by Asset Management Industry are collection of transfer information system, which is split among various systems, conflicting data repository schemas and slow, complex, fragmented process designs and finally no one has a clear view of all the transactional updates happening in the entire process. This complexity can lead to data quality issues, large amount of discrepancies and long cycle times to solve those discrepancies. To tackle this, blockchain was employed right from serialization to being deployed on the floor and focuses only on five key events i.e. manufacturing serialization of assets to initiate the blockchain, receiving and validation of asset, asset capitalization, warranty activation and installation of the asset. Some of the business outcomes include improved transactional settlement time, improved many key operational parameters and reduced number of discrepancies and time required to solve them.

**Blockchain in Real Estate –** The current scenario portrays how cumbersome, opaque and expensive the entire transaction in real estate is and this is mainly because of the involvement of the various middlemen like brokers, government property databases, title companies, escrow companies, inspectors and appraisers and notary publics etc. we must pay them individually, wait for them and finally it becomes like a dependency on them. These middlemen exist because they hold information that you cannot access, or you don't have skills/licenses that are needed to operate in the existing property transaction ecosystem. Public blockchains are a distributed database where anyone can record information, without it being censored, and without needing permission. Equally, anyone can access that information. Blockchain will enable every property, everywhere, to have a corresponding digital address that contains occupancy, finance, legal, building performance, and physical attributes that conveys perpetually and maintains all historical transactions. Additionally, the data will be immediately available online and co-relatable across all properties. The speed to transact will be shortened from days/weeks/months to minutes or seconds. This prevents Fraud Prevention which is a very big loophole in the entire process.

**Blockchain in Finance –** A very important process, which becomes quite expensive and sluggish, due to presence of unnecessary middleman, is the cross-border payments. If a person in New Zealand wants to transfer money to his family in India, who have an account in the local bank, it takes several banks (and currencies) before the money can be collected. Services like Western Union can be used which is faster but again it is too expensive. So, the blockchain can speed up and simplify this process, cutting out the unnecessary middlemen. At the same time, it makes money remittance more affordable. Until now, the costs of remittance were 5-20%. The blockchain reduces the costs to 2-3% of the total amount and provides guaranteed, real time transactions across borders. There are many challenges to this process, but the scope and possibility is yet to be explored and the hurdles can obviously be crossed.

**Blockchain in IoT -** IoT solutions using blockchain can be built to maintain a continuously growing list of cryptographically secured data records protected against alteration and modification. It can set up trust, accountability, and transparency while streamlining business processes. Blockchain can help reduce expense and unpredictability of working edge devices or connecting servers. Blockchain distributed ledger simplifies the development of cost-effective business systems where anything can be tracked and exchanged, without

requiring an essential central control. The adoption of this rising innovation is indicating incredible promise in the IoT space and within the enterprise. For instance, as an IoT connected (RFID) asset with sensitive location and temperature information moves along various points in a warehouse or in a smart home [118] , this information could be updated on a blockchain. This permits all involved parties to share data and status of the package as it moves among different gatherings to guarantee the terms of an agreement are met.

**Blockchain assisting Weddings** - We are aware of the concepts that you can search for a bride or groom online and then physically meet and get to know each other and finally making commitments and involving in a marriage. But what if I say you can do this entire end to end process online, right from finding someone to getting the monetary wedding gifts. Yes, in 2014, the first couple to do this was Joyce and David Mondrus [119]. Those who attended the wedding were shown a QR code that linked to the transaction where the data associated with the wedding was stored. The same concept rather platform can be used to declare one's love in a public, transparent way, in a way that will be enshrined forever.

**Blockchain in Healthcare-** Other than the above, the current trends reveal the applications' areas of blockchain widening to many other sectors, such as smart health care. The authors in [120] propose a unique blockchain based management pf patient's health records. The patient's medical history is stored on a decentralized system, accessible to the treating doctors, and medical insurance providers. Their system named as MedRec, is an immutable medical log of Patients secured by the POW mechanism to facilitate easy sharing with data confidentiality and user authentication.

## 3.6. Challenges

Despite its capabilities and benefits, it has a few disadvantages, the most serious being the scalability problem. The consensus and block validation require the presence of the entire blockchain, i.e. all the transactions that ever happened, thus demanding a lot of storage. The restriction of the block size contributes majorly in the scalability issue. With the limitation of 1MB block size and the delayed consensus process, only 6-7 transactions are confirmed in a second, that too with high transaction fees. If we go for increasing the size of the blocks, it will create an additional delay by decelerating the propagation of the block. To achieve security with reduced block size, a new version of bitcoin blockchain called as Bitcoin-NG was proposed in [121] , which divided the block into two parts to

reduce the propagating size. The first part chooses leader, whereas the other part contained transactions.

Also, forks in typical blockchain networks, cause further delay, while the longest version is awaited by the nodes, to confirm the correct blockchain. But it totally depends on the transaction finalizing time of the consensus i.e. if transactions are committed all in for once and forever or they can be cancelled at a later stage, when new blocks arrive.

Another issue with blockchain is the '51% attack' problem. This problem arises if more than 51% of the nodes collude to generate fake blocks or reverse confirmed transactions. Since greater computation power, leads to quicker generation of the blocks, hence genuine nodes would not be able to compete for a fair version of the blockchain as nodes would only believe the longest version.

## 3.7. Incorporating Blockchain in Proposed Framework

The capabilities and characteristics of Blockchain enable it to make its way in facilitating transparent and immutable security features within VANET. In this section we answer the research questions designed in chapter 1, by providing the blockchain based solution as implemented in the proposed framework.

**Q1. How to identify if messages are indeed coming from an authenticated source?**

**Solution:** Designed a shared distributed ledger, where vehicles would be registered and link to the valid registration can be used to authenticate vehicles on the road. The Distributed ledger, serves as a trusted, decentralized, immutable record of the registration, and revocation of a vehicle.

**Q2. How can the privacy of the users be ensured along with valid authentication (conditional privacy preservation)?**

**Solution:** Developed an algorithm using the blockchain based smart contracts, whereby users' privacy is guaranteed and the ledger storing authentication details can be used for authentication.

**Q3. How to classify a node sending/receiving information as trustworthy or malicious?**

**Solution:** Developed a set of IPFS private nodes which cater the purpose of keeping node's reputation based upon the score evaluated and stored by the smart

contract. Each node referring to this IPFS data can then be the content provider to other nodes looking for the already queried node's information.

**Q4. How to compute a node's reputation without relying on a trusted party and thus providing transparent and valid reputation score?**

**Solution:** Designed a smart contract to capture user's fake and true messages based on a certain verified parameter and automatically calculate the reputation score to be rendered by the nodes on road.

For data sanitization i.e. process of hiding sensitive data before transmission, optimization algorithms are used, whereas for ensuring the access control of this data to reputed nodes, Machine Learning is used with blockchain.

**Q5. How to ensure secured message transmission with minimal computation?**

**Solution:** Designed a data hiding technique which sanitizes the data before transmission. A simple XOR technique is used to perform the sanitization, to ensure minimal computations and no latency in encryption and decryption process. The sanitization works on the sensitive data mostly.

**Q6. How to manage the key used for the sanitization process to prevent data leakage and unwanted access?**

**Solution:** Designed a data management technique using the blockchain technique which manages the keys generated for the sanitization process. This is an immutable storage and records can easily be accessed for desanitization based upon the timestamp.

**Q7. How to have an optimal key for the sanitization process which ensures maximum sensitive data sanitization with minimal key size?**

**Solution:** Designed the objective function which provides the solution for maximum data hiding with optimal key and used optimization technique of Sea-Lion Optimization and Whale Optimization Algorithm to achieve it.

**Q8. How to provide access control and ensure data transmitted by a sender node is only accessible to other trustworthy nodes?**

**Solution:** Designed a trust management system, using Machine Learning, which can classify trustworthy and malicious nodes, based upon certain critical factors such as PDR, RSSI values. This can help prevent attacks caused by 'authenticated' but greedy nodes.

## 3.8. Conclusion

The blockchain is used globally for securing P2P infrastructure with decentralization. This chapter presented a comprehensive review of the blockchain by highlighting the working model of blockchain and subsequently presenting the system features. Consensus algorithms were described with different applications and use cases. Finally, this chapter concluded with how the research question are solved by incorporating the capabilities of blockchain to solve different security challenges in VANET. The proposed framework is presented and discussed in the following chapters.

# Chapter 4

# Vehicle Authentication with Expeditious Revocation

*This Chapter is a work towards contemplating our first research challenge as discussed in Chapter 3 and addressing it using our blockchain based solution. The main and critical issue worked upon is the authentication, authorization, and revocation of vehicles without relying on the centralized infrastructure. The aim is to preserve the privacy of the vehicles while also authenticating them under ordinary and urgent circumstances. A new blockchain-based scheme is introduced which ensures identification of vehicles in the decentralized network which reduces the communication and computation overhead due to the delays caused by the absolute dependency on the Certificate Authority (CA) for authenticating unknown nodes trying to penetrate the network boundaries. This is a private blockchain based scheme, which safely authenticates the OBUs with changing RSU on road after the vehicle has been registered with the CA, also, maintaining their privacy. Also proposed is a quick revocation mechanism which avoids delays in verification of a new entity in the network before authentication. The scheme allows for secure data transfer between the RSU and the group of vehicles in range and further to neighboring RSUs during any emergency encountered.*

## 4.1. Introduction

Privacy and security in Vehicular Ad Hoc Networks (VANET) gained huge prominence after Vehicle Safety Communication (VSC) project [122] , delivering the concept of pseudonym certificates for vehicles and effectively safeguarding the communication within the network for a comfortable and safe driving experience.

While authentication of vehicles becomes the first and most important step, the works done in this direction rely heavily on a trusted party to perform this and the subsequent process, such as identification, revocation, or traceability of a malicious vehicle. Even though they preserve the privacy by incorporating the concept of pseudonyms, but traceability remains a concern where you report to the CA, to find out the actual identity of the vehicle. This centralization has several disadvantages. The cloud servers of the conventional centralized mechanism in VANET serve as an excellent bait for the attackers by functioning as a single point of failure which can lead to certain treacherous situations disrupting the entire network. Also, the malicious messages from suspicious parties or alteration in genuine messages impact the driver's behavior and can cause mishaps jeopardizing the safety of passengers on road. Lack of privacy and security breaches for instance, tracking of a vehicle, impose a restriction on using them for providing personalized services.

In the light of these circumstances, we propose a blockchain based authentication and revocation framework, which not only reduces the dependency on a trusted authority for identity verification, but quickly updates the status of revocated vehicles in the shared ledger visible to the authorities sharing the ledger. In the proposed scheme, vehicles obtain their Pseudo IDs from the CA, which are stored along with their certificate in the immutable authentication blockchain and the pointer enables the RSUs to verify the identity of a vehicle on road. Moreover, the transactional data of a vehicle also enables the Revocation Authorities to go for quick revocation.

## 4.2. Related works

The open access environment catered by VANET instigates open challenges in the field of privacy and security making it unfit for implementation in the real world [123-127]. In this section we would explore these research works in detail, by categorizing them into centralized and decentralized implementations.

### 4.2.1. Centralized Works

[128] utilized a secured group broadcast which made use of the secure key management and proposed security managers that simplify the key transfer handshake mechanism overcoming encumbrances in the domain of privacy and security.

[129] ensured privacy by keeping the identity of a vehicle anonymous and proposed a methodology to trace a vehicle when required by law enforcement agencies. It uses multi-hop communication to transmit an emergency message across groups having more time complexity. There are various studies on VANET dealing with its security issues, threats and challenges in maintaining privacy within the network.

[130] introduced a metric to quantify the level of privacy enjoyed by the vehicles by the frequent change of pseudonyms. Their effectiveness and different methods of implementation were discussed along with a mix model describing the pseudonym change algorithms [37].

In a similar study, pre-shared keys were introduced to implement the authentication of nodes in the network [131]. The improved IBV scheme was proposed in one extensive research, requiring small pairing and point multiplication computations for batch verification which are independent of the number of messages [101].

A similar study focuses on IBS along with pseudonyms in a cloud-based security and privacy-aware information dissemination environment [132]. [38] introduced graph-based resource sharing schemes providing a better network sum rate which is verified using simulation.

In another research, [39] proposed a framework (ACPN) for privacy preservation and non-repudiation in VANET using IBS and IBOOS schemes for authentication between vehicles and RSUs.

[133] focused on security and privacy in VANET and proposed a hybrid method which strengthens the framework using pseudonyms with self-certification thus, eliminating the need for managing them without compromising on the robustness of the system.

To obtain high accuracy and privacy with respect to the vehicle's location, [134] developed a methodology based on dynamic pseudonym generation for mix-zones environment and verified the results using the SUMO simulator.

### 4.2.2. Decentralized works

With the launch of bitcoin blockchain in 2008, the focus of industry and academia shifted towards approaches which could secure the way centralized networks operated. The initial studies incorporating the decentralized, immutable, and robust blockchain propose its implementation in various financial and banking sectors involving secure transactions using smart contracts [135-139] after which its advantages in other sectors were also identified [140].

Some studies focus on implementing blockchain in different areas like the Internet of Things (IoT) devices [141, 142], automotive sector [143], smart home framework [142] and healthcare department [143] providing security, reducing manipulation and forgery by malicious participants and utilizing various features of blockchain like smart contacts and proof-of-work, together or individually. From then on, some researches in VANET focused on methodologies to improve efficiency, guaranteeing privacy and security using the blockchain technology.

[40] introduced a seven-layer secure and decentralized conceptual model for Intelligent Transport System (ITS), discussing the relationship between Blockchain-based ITS and parallel transportation management systems claiming the former to be the future of ITS. After the introduction of autonomous/self-driving vehicles on the road for which efficient and timely communication amongst the nodes is of utmost importance, [41] explored the use of sensing and signaling devices using blockchain public key infrastructure and an inter-vehicle session key establishment protocol. The technological revolution brought by blockchain also imposes certain new challenges like poor scalability, high computational costs due to mining, high bandwidth, and storage requirements. A typical blockchain is depicted in Figure 3.1.

## 4.3. Problem Identification and the proposed solution

When vehicles begin their travel on road, it is important for them to receive periodic traffic updates or be able to access value added services for which the infrastructure should uphold the monumental purpose of user safety. This brings us to the scenarios which can prove fatal for the users if not dealt appropriately on time such as an accident emergency, congestion on the road, obstacle detected on road, etc. Also, transmitting notifications and warnings securely to those who are under threat is important. Keeping all these scenarios into consideration, we derived our problem statement, categorized into the following requirements.

### 4.3.1. Mutual Authentication with Reduced Dependency on CA

To become part of the network and entrust the messages from RSU, mutual authentication must be performed between the On-Board Unit (OBU) and corresponding Road-Side Unit (RSU), but this should not involve complex computations or frequent communications with the CA. Earlier schemes involve the CA to verify user's identity for every critical data received by the RSUs which causes a delay in connection establishment, bandwidth consumption and

increased dependency on the third party. Furthermore, revocation and traceability also rely solely on the CA.

### 4.3.2. Scalability

The framework should reckon with scalability attributable to the vastness of vehicular networks.

### 4.3.3. Privacy Protection

Furthermore, the authentication of users should not incur at the cost of their identity disclosure or perturbing their privacy. When messages are communicated both the message and source authentication should be effectively performed without revealing the actual identity.

### 4.3.4. Expeditions Message Verification and Forwarding Without Network Flooding

When an emergency event occurs such as an accident, traffic jam, meager road conditions or on-going road construction, messages from the vehicles should be forwarded only to the RSUs which would further convey to the appropriate areas who might be affected by the event. This should be accomplished targeting the messages only to the RSUs of these areas rather than broadcasting over the entire region to save time and bandwidth.

### 4.3.5. Message Confidentiality, Integrity and Non-Repudiation

The messages communicated, should be verified for their authenticity and integrity. The security mechanism should prevent unauthorized access by intruders, to avoid any compromise of confidentiality and authentication should prevent repudiation.

### 4.3.6. Reduced Load on the OBUs

The transmission and verification process should also consider confined storage and limited processing capability of the OBUs. The OBUs at any time should not be overloaded with computations or run out of storage.

### 4.3.7. Speedy Revocation Without Additional Overhead

The framework should not just be able to perform authentication, but quickly revocate the malicious vehicles. The vehicles revocated should be easy to identify without circulating an entire Certificate Revocation List (CRL) as it causes lot of overhead. For authenticating as well, RSUs or the in-range vehicles consume plenty of time verifying the CRL before allowing any connections.

Though most of the researches in VANET focusing majorly on the security aspect predominantly addressed authentication and conditional privacy issues, but lack to suffice the scalability, efficient authentication and dissemination of

messages with quick check on revocation and reduce dependency on the centralized authority for major resolutions. In our work, users associated with the CA only in the registration step, rest of the process which includes on-road authentication, verification, and revocation is performed by the RSUs using shared blockchain ledger. Security requirements with user anonymity are fulfilled by the shared ledger which reduces the steps in authentication and secure communication.

## 4.4. System Overview

In this section, we state some assumptions, briefly define the system entities in our network model, system vulnerabilities via the threat model, our problem statement and solution goals.

### 4.4.1. Network model and System Parameters

The network model defines both the physical and abstract entities. The physical entities correspond to the on-road and off-road physical infrastructure formulating the network, enabling wireless/wired communications. These majorly include the CA, RA, Regional Authority (RGA), RSUs, OBUs, Base stations, etc. The abstract entities are applications/software installed with these bodies, that are accountable for managing and coordinating data sharing, updating, verification and data management, such as the authentication and revocation ledger and other software components rendering interfaces to this ledger. While we already explored the fundamental participants i.e. the OBUs and RSUs in Chapter 2, but we discuss in greater detail the functionality of these in our model with new assumptions or specifications. These entities are defined in a greater detail as follows:

#### 4.4.1.1. CA (Certificate Authority)

The first and foremost functionalities are carried out by this authority, devising the foundation of Cryptographic security technique. Vehicles' users are issued identity certificates and essential secret keys corresponding to their certificates by CA, which enables them to communicate with other vehicles' OBUs and RSUs to procure necessary information or transmit emergency messages. These are certificates uniquely identifying every RSU and OBU. The drawback of having RGAs for different areas in a country to issue the key pairs is the

requirement of chaining the certificates, hence we assume a single CA for the task. The scheme utilizes a ledger which is shared between the CA and RSUs, enabling the verification of user's identity as uploaded by the CA and permitting the RSU to request any user data with restricted write rights.

#### 4.4.1.2. RSU

These are static modules located along the roads and highways, working as an intermediary to facilitate communication between the OBUs and the cloud servers. They are equipped with network cards aiding DSRC communications among RSUs and in-range OBUs and connected with the CA via internet sharing a distributed ledger. Also assembled within are tamper-proof devices (such as TPM [28] to store secret cryptographic details such as public keys of neighboring RSUs. Additionally, for our scheme, it generates a group key and group ID, timestamped and shared with the group of vehicles in its range and updated for the new vehicles approaching.

#### 4.4.1.3. OBU

The OBUs are the key devices installed in the vehicles equipped with Wireless transceivers which include IEEE 802.11p (DSRC) radio transceivers facilitating high-speed, short-range, and low-latency communications between OBU-OBU and OBU-RSU. Other wireless modules for IEEE 802.11a/b/g communications might be present. It might also feature a low-cost 4G/LTE module and a wired or wireless interface to connect to the application unit. OBU is supported by the TPM to store the secret keys and ledger details for authenticating the OBU. They have shorter communication range, low computation processing power and storage as compared to the RSUs.

#### 4.4.1.4. Authentication and Revocation Ledger (Blockchain)

CA, RA and the RSUs in an area share this ledger for authenticating, verification, and checking revocated vehicles before granting any authorization rights. CA makes vehicles' registration entries in this ledger by creating new transactions, just like new coins are created in the bitcoin blockchain. The transactions' inputs and outputs are sealed to be accessed by the RA and CA, which have complete rights over the ledger, whereas the RSU can query the ledger with only read rights.

#### 4.4.1.5. Off-Blockchain Storage

This refers to the hash map, which is essentially a user-data store, available and accessible to the CA via an interface. The key-value pairs represent the mapping of Pseudo IDs. TA is hosts this off-blockchain storage in its trusted cloud servers replicated sufficiently across multiple nodes extending high availability.

#### 4.4.1.6. Communication Network

The DSRC communications and the distributed Ledger sharing form pivotal and overriding parts of the entire framework, where both the Ad hoc (V2V, V2I, I2V) domain and the Infrastructure domain [29] rely on these to unpretentiously cater the security needs, thereby enabling secure data transmissions.

### 4.4.2. Assumptions

In this system, the CA is assumed to be a completely trusted, government-owned, automobile division where each vehicle performs the initial registration for being authorized to start on-road. Before registration with the CA for obtaining certificates, we assume that the vehicle obtains a valid vehicle ID (VID) such as an electronic license plate from the Motor Vehicles Division (MVD), which is supplied to the CA further authorization. Thus, registration of a vehicle is accomplished in two-steps, where, the user submits necessary identity documents, essentially their name, address, electronic license plate number, etc to the CA in the first step and acquires cryptographic information i.e. their Pseudo IDs along with corresponding public and private keys and other security parameters in the second step, thus, accomplishing successful registration. We made the following assumptions [30] for our proposed model:

1. Unlike the CA, RSUs are semi-trusted, in virtue of their presence in open, attack-prone environment. Hence, their access rights are restricted to only necessary details, enough to perform successful mutual authentication with the OBUs. They are regularly supervised and examined for any physical breaches, and if compromised, the attack can be tackled and unraveled within a stipulated time. We strengthened the RSU security by embedding TPM (to store confidential security parameters), along with the central DSRC module. The RSUs have significantly greater computation power and storage as compared to OBUs. Additionally, the RSU range exceeds the OBU range as it

supports up to a 1000m whereas OBU transmissions are restricted to a maximum of 300m. RSUs belonging to the same region are connected by means of a wired or wireless connection so as to directly inform and update each other about any crisis via a suitable routing protocol.

2. The in-vehicle storage is equipped with a TPM enabling OBUs to safely forward messages to the nearest RSUs directly or by means a VANET specific routing protocol. At the time of registration, the list of RSUs with their identities, which are also their public keys used in the IBE to initiate on-road communications are stored in the OBUs. During renewal of the registration, these are updated along with other necessary details, to ensure the vehicles can easily contact the proximate RSUs.

### 4.4.3. Threat Model

Raya and Hubaux in [102] elaborated the heterogeneity of attackers who can disrupt the smooth functioning of the network by launching different attacks. They clearly distinguish among these attacks based on the mixed criteria such as network association, methods used, scope of the attack, and motivation causing the attack. From their study, we deduced that attackers can be internal or external, take over local or widespread regions, launch active or passive attacks and these could be for profit and greed or just for fun. Internal attacks are usually more prominent and devastating since they are launched by the authenticated network participants with enough access to cause a breakdown, whereas external attackers collaboratively put in extra efforts for spoofing the network to obtain critical and vital information. The external attacks might not be too successful to obtain secret keys aimed to instigate impersonation or Sybil attacks, but they can easily eavesdrop to procure traffic-related information and link signatures, thus compromising on the user's privacy.

In our scheme, we considered most important threats that are to be resolved in the proposed framework contemplating the primitive requirement of ***latency, throughput, and scalability*** in VANET and rendering end-to-end security.

The most treacherous of all attacks are launched due to inappropriate authentication of the sender and the receiver, inadequate privacy-preserving scheme, and less secure communication channels. Some of the consequent attacks include:

1. impersonation of a legitimate node
2. Sybil attack (using multiple IDs)
3. replaying previous messages

4. fabrication of transmitted messages, and
5. location tracking.

Our model addresses these attacks with reduced overhead, efficient data dissemination and preservation of user anonymity by exploiting blockchain's inherent security features.

### 4.4.4. Cryptographic tools in proposed model

The proposed model is Elliptic Curve Cryptography (ECC) Based PKI, with Elliptic Curve Digital Signature algorithm (ECDSA) as the main building block establishing message authentication and non-repudiation. To make sure senders and receivers take complete ownership of the messages communicated, every message is digitally signed and for Signature generation.

ECC unlike DSA is based on the elliptic curves over prime fields say $F_P$, (where p>3). The curve can be expressed as in equation 1.

$$C_p\,(a, b): y^2=x^3+ax+b(\mathrm{mod}p) \qquad (1)$$

where $a, b \in F_p$ and $4a^2+27b^2 \neq 0$. ECC makes itself a better option by rendering the advantages of greater security with smaller key size, but the level of security is radically determined by the Elliptic Curve Discrete Logarithmic Problem (ECDLP). The ECDLP can be briefly explained as follows:

Consider two points, L and M over $C_p\,(a, b)$. The ECDLP finds an integer $k$ in the field $F_p$, such that L= $k$. M. Considering the computational difficulty of ECDLP, it is impregnable and cryptographically strong, thus making it a choice over other cryptographic tools.

## 4.5. Proposed Model

In our work, we proposed an expeditiously efficient source and message authentication scheme with privacy protection and expeditious revocation. The method is unique due to the introduction of a private blockchain, which majorly contributes in the functioning of the framework by reducing dependency on the CA. The notations used in the system are given in Table 4.1.

The physical entities, i.e. CA, RA, and RSU collaboratively communicate via this shared ledger to achieve the security- for-safety-on-road motive which is explained in the following three phases briefly.

*Table 4.1. Notations*

| Notation | Meaning |
|---|---|
| → | Unicast communication |
| --)) | Broadcast Communication |
| # | An entity stores the data in the data structure following it. |
| * | An entity operates on the data structure/object following it. |
| H () | Hash function |
| [15] $DS_X$ | Digitally signed by X |
| $E_X$ () | Encrypt with X |
| $D_X$ () | Decrypt with X |
| $OBU_i$ | $i^{th}$ On-Board Unit |
| $RSU_i$ | $i^{th}$ On-Road Unit |
| $Cert_x$ | Certificate issued to X |
| Verify () | Function to check integrity and authenticity of a message. |
| $M_i$ | Message |
| Group () | Function to include a vehicle in the group after authentication |
| Query () | Function to search Pseudo ID of the OBU in β |
| $PID_i$ | Pseudo ID if $i^{th}$ OBU |
| B | Authentication and revocation ledger |
| $Ptr_i$ | Pointer to the ledger entry |
| $HPrev_j$ | Previous hash of the block |
| $S_{RSUi}$ | Private key of $i^{th}$ RSU |
| $Tx_i$ | $i^{th}$ transaction of block X in the ledger |
| $TID_{Bi}$ | Transaction ID of $i^{th}$ transaction of block B, given as H(input transaction) |
| MAP () | Mapping function |
| $VID_i$ | Original ID of $i^{th}$ OBU |
| $P_{ki}$, $S_{ki}$ | Public-private key pair of $i^{th}$ OBU |
| $V_i$ | $i^{th}$ vehicle |

### 4.5.2. System Initialization

The protocol focuses on reducing dependency on the CA but doesn't completely deny its importance in the dynamic vehicular networks. During system initialization different participants prepare to get occupied with numerous domain parameters required for later security operations. The CA builds the system for the ECC based PKI, by establishing the system parameters $X=p$, $a$, $b$, $G$, $n$ and $h$ for the curve $C_p$ in the field $F_p$. Here, integer p defines the field $F_p$, $a$ and $b$ are constants defining the curve equation, $G$ is the generator of the cyclic group $Z_p$, $n$ which determines the order of $G$, is a prime number and $h$ is the curve's cofactor given by equation (2).

$$h= (1/n) |C(F_p). \qquad (2)$$

These parameters along with the publicly known hashing functions are stored in the vehicles during registration. Also, the RSUs are supplied with the CA's public key for signature verification in the ledger. CA generates its public key with its private key given by equation (3)

$$P_{CA} = x.\ G \qquad (3)$$

where *x* is the private key of CA.

The blockchain network among the CA, RA and RSUs is setup by their public keys, through which they address and verify each other while storing and retrieving transactions. The genesis block for the authentication and revocation ledger is securely generated. Here, the CA creates new Identities, just like new coins are generated in the bitcoin blockchain. Apart from these, vehicles are assumed to obtain their Vehicles' ID before registration from the Motor Vehicle's Division (MVD).

### 4.5.3. Registration of the Vehicle

The users register with the CA for the first time by submitting their VID obtained from the MVD. The CA verifies the $VID_i$, assigns a Pseudo ID ($PID_i$) and generates an ECC Public-Private key pair namely $Pk_i$ and $Sk_i$. The mapping of the actual identity with the assigned $PID_i$ is stored in a hash map in its database. This ensures easy lookup in case of traceability and revocation of malicious users. The $PID_i$ issued is digitally signed by the CA and forms a transaction of the Block β in the ledger.

*Table 4.2 Registration of the vehicle $V_i$ with CA*

| | | |
|---|---|---|
| **Step 1** | **$V_i \rightarrow$ CA** | ⟨$VID_i$, Other Details⟩ |
| **Step 2** | **CA*$VID_i$** | ⟨Verify ($VID_i$)⟩ |
| **Step 3** | **CA # $T_{Bi}$** | ⟨input→ ($PID_i$)$DS_{CA}$⟩<br>⟨output 1→ (OP_Return "H($Cert_{PIDi}$"))<br>⟨output 2→ Script: Verify (H($PK_{RA}$), $Sig_{RA}$))<br>Value: *$val_0$)* |
| **Step 4** | **CA # β** | Update Ledger with the transaction |
| **Step 5** | **CA → $V_i$** | ⟨$PID_i$, Certificate ($PID_i$, $DS_{CA}$), ECC ($P_{ki}$, $S_{ki}$), $TID_{Bi}$ $Hash\_pointer_{B,}$ $H\_Prev_B$⟩ |
| **Step 6** | **CA # Hashmap** | ⟨MAP ($PID_i$\|\|$VID_i$⟩ |

The input of the transaction can be easily verified as it includes CA's public key hash address and its ECDSA signature. The output of the transaction is the

most important part for identity verification. There are two outputs corresponding to each input for a new vehicle registration. The first output is the Hash value of the certificate embedded in the OP_Return instruction of the output script. For an output script without an OP_return, the output is redeemed with the public-key-hash of the recipient and a signature verification called as '*Pay-to-pubkeyhash*'. The transaction redeeming this output needs to provide an appropriate hash value generated using its public key and signed using the corresponding private key. Thus, for redemption the output script should evaluate to true with the above conditions satisfied and the output being an UTXO. But an output script containing the OP_return has no amount to be redeemed and thus the output script evaluates to be false. This output is only used to verify the authenticity of the certificate by matching it with the one sent by the OBU. The second output assigns a small amount of 0.02$ to the RA, which is redeemed by the RA in case of the vehicle going rogue and thus setting up the 'revocation flag' in the revocation transaction redeeming this amount. Post creation of the transaction, SHA-256 hashing function is used to compute the block's cryptographic hash as given in equation (4) and the ledger is updated.

$$HOB_{\beta i} = H\ (T_{Bi}, HPrev_j) \qquad (4)$$

The result forms the hash previous for the next block which is uploaded to Ledger β shared among the CA, RA and RSUs.

Conforming to the bitcoin transactions, these are also added by the CA in the chronological order and there is no serial number. Each transaction has a transaction Id which unlike the bitcoin transactions is just the hash of the input transaction, digitally signed by the CA. This ensures its verification. The steps of registration are depicted in Table 4.2 with illustration in Figure 4.1.

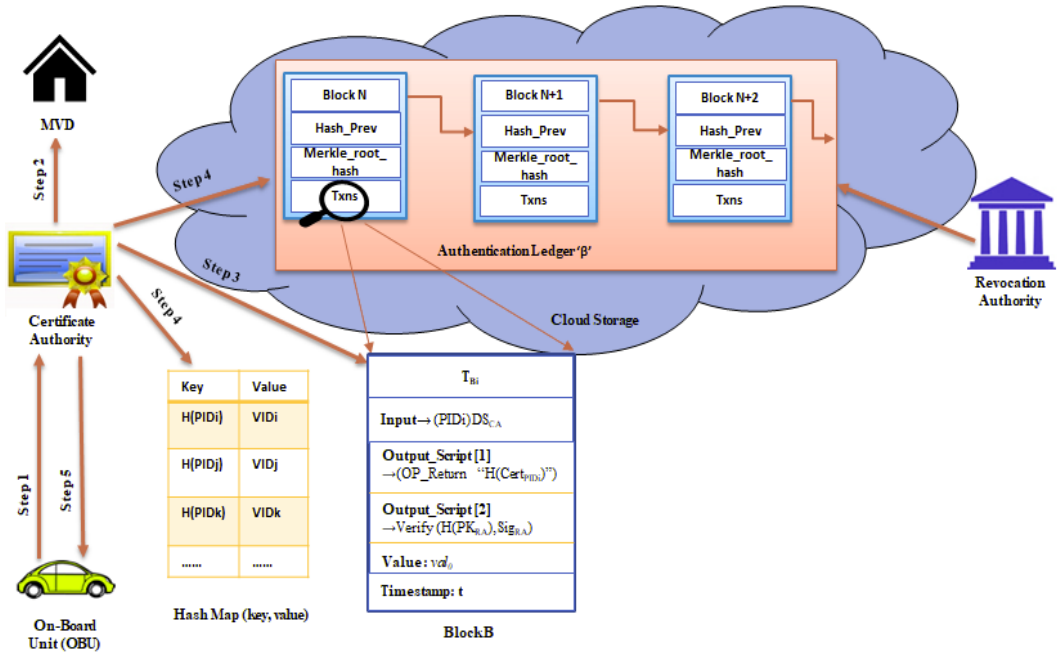

*Figure 4.1 Registration of vehicles at the CA*

But, since this is a private blockchain with no proof of work, but only proof-of-authority and a layer of access control on the top of the shared ledger with a few positive assumptions, transactions can be modified in an extreme case.

The CA then returns Hash_pointerB, assigned PIDi with corresponding certificate, and $TID_{Bi}$ to the OBU. The ECC key-pair ($P_k$ and $S_k$) are stored in the OBU's TPM.

### 4.5.4. Mutual Authentication

When the OBU comes on the road, it authenticates itself with the RSU to become part of the group of vehicles in range of the RSU as shown in Figure 4.2.

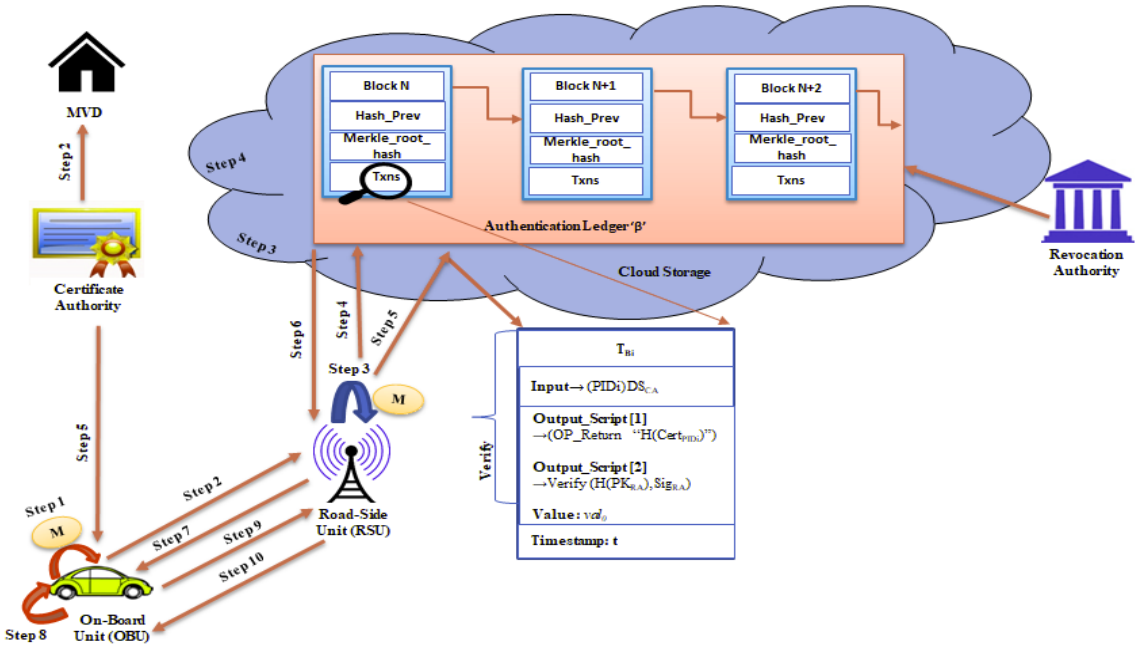


*Figure 4.2 Mutual Authentication of RSU and OBU*

The identity $R_i$ of the RSU, obtained from the CA, serves both as its Identity as well its Public key. When the OBU comes in the range of the first RSU on road, it gets a notification from the OBU since it contains all requisite identity information and certificates of the nearest RSUs. The OBU forms a message M containing its $Hash\_pointer_B$, $TID_{Bi}$ and $Ptr_i$ which is encrypted with Ri using IBE scheme as shown in Table 4.3.

*Table 4.3 Mutual Identity Authentication: OBUs First Encounter with a RSU Or Changing RSU*

| | | |
|---|---|---|
| **Step 1** | **$OBU_i$*$M_i$** | $\langle PID_i, Cert_{PIDi}, E_{Ri}$ (Hash_Pointer$_B$ \|\| $TID_{Bi}$) $\rangle$ |
| **Step 2** | **$OBU_i \rightarrow RSU_i$** | $\langle M_i \rangle$ |
| **Step 3** | **$RSU_i$*$M_i$** | $\langle D_{SRSUi}$ (Hash_Pointer$_B$ \|\| $TID_{Bi}$) $\rangle$ |
| **Step 4** | **$RSU_i$*β** | $\langle$Query(β\|\|$PID_i$) $\rangle$ |
| **Step 5** | **RSU*$T_{Xi}$** | Verify(H($Cert_i$) *stored* = H($Cert_i$) *received*))<br>$val_0 \rightarrow$ not redeemed and Revocation Flag = False,<br>if true go to step 6, else, do not authenticate. |
| **Step 6** | **RSU* $Cert_i$** | $\langle$Extract $P_{ki}\rangle$ |
| **Step 7** | **$RSU_i \rightarrow OBU_i$** | $\langle E_{Pki}$ (Challenge integer N) $\rangle$ |
| **Step 8** | **OBU*(Challenge)** | $\langle D_{Pki}$ (Challenge integer N) $\rangle$ |
| **Step 9** | **$OBU_i \rightarrow RSU_i$** | $\langle E_{Pki}$ (Challenge-Response Integer N+1) $\rangle$ |
| **Step 10** | **$RSU_i \rightarrow OBU_i$** | $\langle$Group ($OBU_i$)$\rangle$ |

The RSU upon receiving the message decrypts it with its private key $S_{RSU}$, and gets the PIDi, corresponding ledger entry and pointer to the block. It queries the blockchain using the $PID_i$ as the index and when found verifies both the outputs for the respective transaction. Once confirmed, the RSU sends a challenge integer to the OBU encrypted with its public key and waits for the response. If the OBU could decrypt the challenge message and send response as the next positive integer, it is authenticated by the RSU. The OBU is provided with the corresponding group key. Now, post authentication, the new vehicle becomes part of the group of vehicles in the range of the RSU and is hence authorized to request any data, send information accumulated from the surroundings or receive emergency alerts from the RSU.

### 4.5.5. Quick vehicle revocation

For revocation, suppose the RSU receives a message from a malicious node and the message content is proved false, then in such scenario, the RSU would

communicate with the RA sending the 'bogus message' as well as the $PID_i$ responsible (Table 4.4).

*Table 4.4 Revocation of Malicious Vehicle*

| | | |
|---|---|---|
| **Step 1** | **$V_i \rightarrow RSU_i$** | ⟨" Bogus Message" ⟩ |
| **Step 2** | **RSU→RA** | ⟨$E_{PKRA}$ ($PID_i$\|\|'Bogus Message') ⟩ |
| **Step 3** | **RA # $T_{Dj}$** | ⟨input→ ($PID_i$ \|\| H ($Cert_{PIDi}$) \|\| ($val_0$) $DS_{RA}$⟩ ⟨output 1→ (OP_Return "H ($Cert_{PIDi}$)", Revocation Flag = True")) ⟩ |
| **Step 4** | **RA # β** | ⟨Update Ledger with the Revocation transaction⟩ |
| **Step 5** | **CA #Hashmap** | ⟨ Search Revoked PID and delete entry⟩ |

This transaction is validated by the CA and the original transaction is verified without adding any linked updates. This ensures that the pointer stored with the OBU remains the source for performing its Mutual authentication with the RSU. Also, the Hash map is updated accordingly. RSUs instead of looking for a CRL can now easily verify the status by a transaction as shown in Figure 4.3.

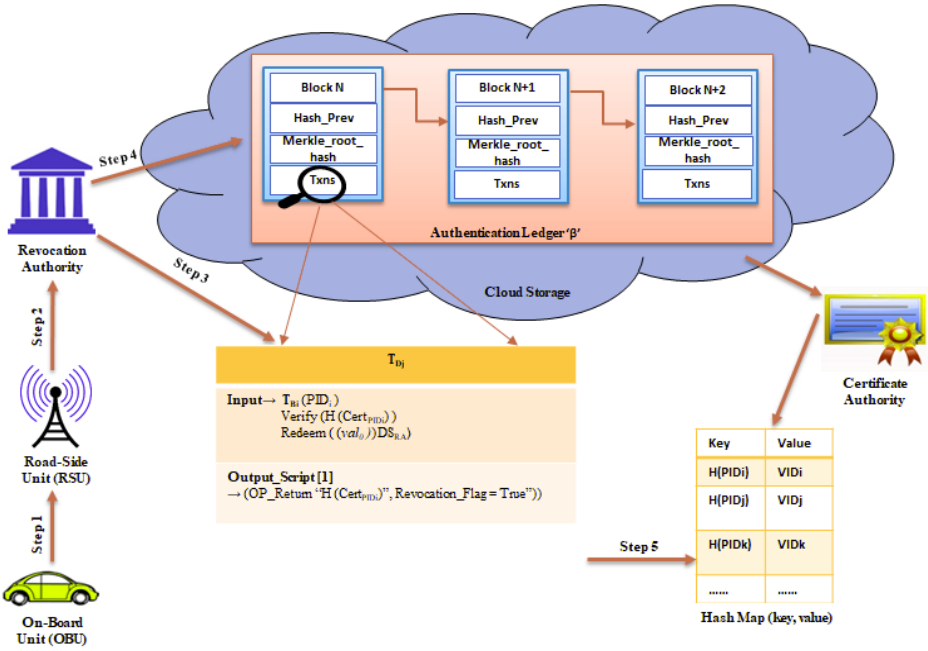


*Figure 4.3 Revocation of Malicious vehicles by the RA*

We assume RSUs to form a Mesh Network and hence easy connectivity and reachability. Upon detection of an event the OBU forms a message which is verified by the RSU and forwarded either to the group of vehicles in range or to RSU of the respective area using an appropriate routing protocol as shown in Table 4.5.

## 4.6. Model Analysis and validation

This section analyses the proposed work w.r.t theoretical and simulation results.

### 4.6.1. Environment Setup

VANET with distinctive topology, are high-speed dynamic networks, that constantly change movement patterns and, association among the vehicles, thus affecting both the traffic scenario and the network formation among the nodes. To demonstrate functionality of the proposed protocol, we used the Veins [32] framework, which supports a range of models to showcase both the road traffic and network simulation.

For network simulation we used OMNeT++ 4.6 (Objective Modular Network Testbed in C++), which is a discrete event simulator. It allows to define both the behavioral and functional characteristics of modules using the inbuilt libraries and procedures written in C++ and the NED language.

The veins framework has the IEEE 802.11P 11p and IEEE 1609.4 DSRC/WAVE integrated in it, which makes it easier to establish the network with pre-established physical layer communication parameters and characteristics like speed limits, lane counts, buildings and turn restrictions. But, to include the functionalities of the network and transport layer and equip the simulation with features for message passing communication and protocols, INET-2.4.0 library is used.

To prototype intermodal traffic systems, SUMO-0.19.0 (Simulation of Urban Mobility) framework is used as the mobility generator to test and optimize the potent and efficiency of the proposed scheme. The simulation is run on a Windows 7 (ultimate -x86) operating system with 8 GB of RAM with simulation parameters listed in Table 4.5.

*Table 4.5 Simulation Parameters*

| **Simulation Parameter** | **Value** |
|---|---|
| Simulation time | 6000s |

| | |
|---|---|
| Frequency | 5.9 GHz |
| Number of nodes | 1-100 |
| Size of ground | 5000m |
| Packet size | 100-200 bytes |
| PHY Layer | IEEE 802.11P |
| MAC Layer | IEEE 1609.4 |
| Data Rate | 18Mbps |
| Measured parameters | Delay, Throughput, and packet delivery ratio (PDR) |

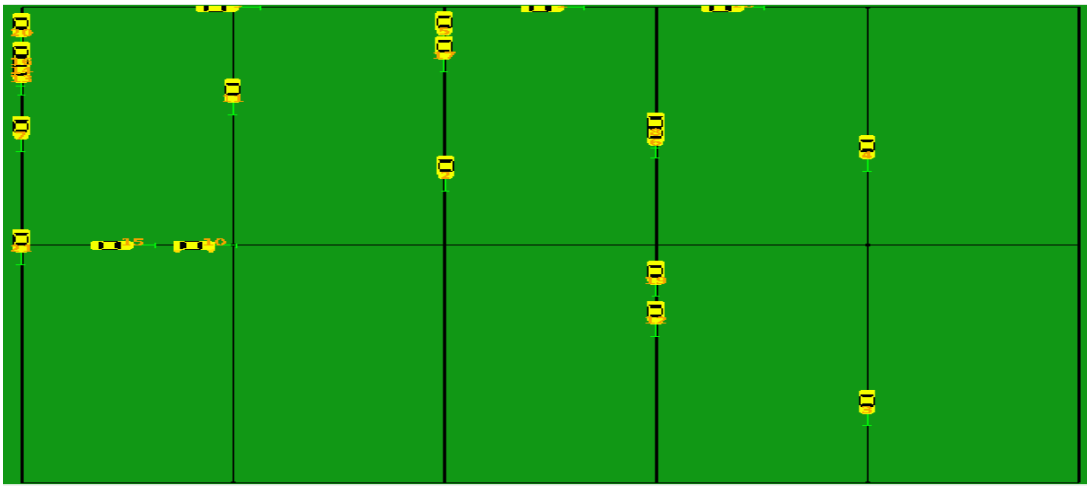

*Figure 4.4 Real-world scenario in sumo-0.19.0*

#### 4.6.1.1. Test Scenario

For testing the functionality of the protocol, we considered a real-world scenario in the Sumo simulator, depicting the lanes with vehicles as given in Figure 4.4. The vehicles in the sumo simulator are shown as the dynamic nodes in the Omnet framework, where we code their functionality and behavior while in movement utilizing the inbuilt libraries and procedures. For our testing, the number of vehicles range from 1- 50, with speeds ranging from 14 to 20 m/s. The parameters of delay, throughput and PDR are considered to showcase how the protocol performs, and the average values over an interval of every 5 vehicles is gathered.

The scenario consists of two RSUs located on road and authenticating vehicles by means of the shared ledger. The application module providing interface for accessing the ledger transactions based on the TID and the block pointer supplied by the corresponding OBU. The above discussed parameters are evaluated for assessing the performance as they could successfully depict how addition of a few fields in the message communication, and encryption and decryption of messages effected the original working. Detailed analysis of the results under these parameters and the mentioned simulation setup are examined in the following subsection.

## 4.6.2. Performance analysis

The protocol performs comparatively well considering the time taken with and without addition of security features. The difference in performance occurs due to the time consumption in executing the security operations, thus establishing the security requirements. The proposed protocol has been analyzed based on three parameters i.e. delay, throughput, and packet delivery ratio (PDR) with unicast communications between the vehicles and RSUs. The graphs show the comparison of the scheme before and after applying the security features of encryption, decryption, verification and authorization for successful authentication and access control. The delay at RSUs increases with the increasing number of vehicles due to the time taken by encryption, decryption, and ledger verification for upholding identity and confirming revocation simultaneously.

### 4.6.2.1. End-to-End Delay and Throughput

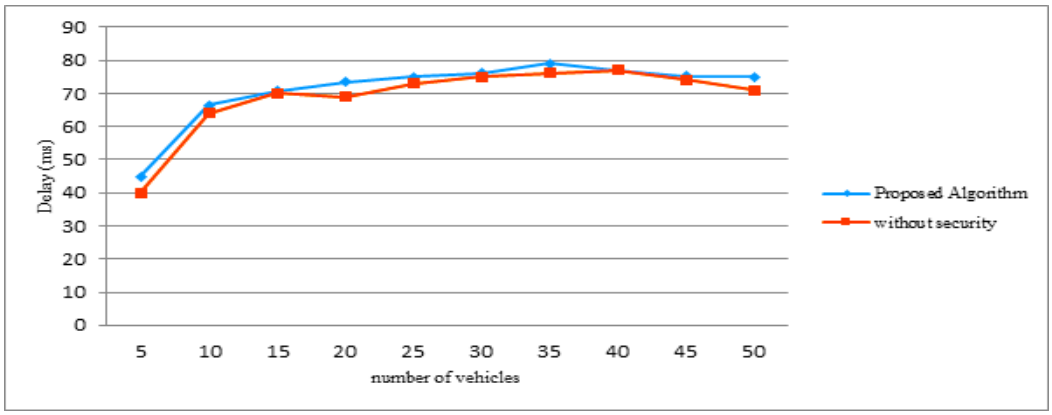


*Figure 4.5 End-to-End Delay vs Number of vehicles*

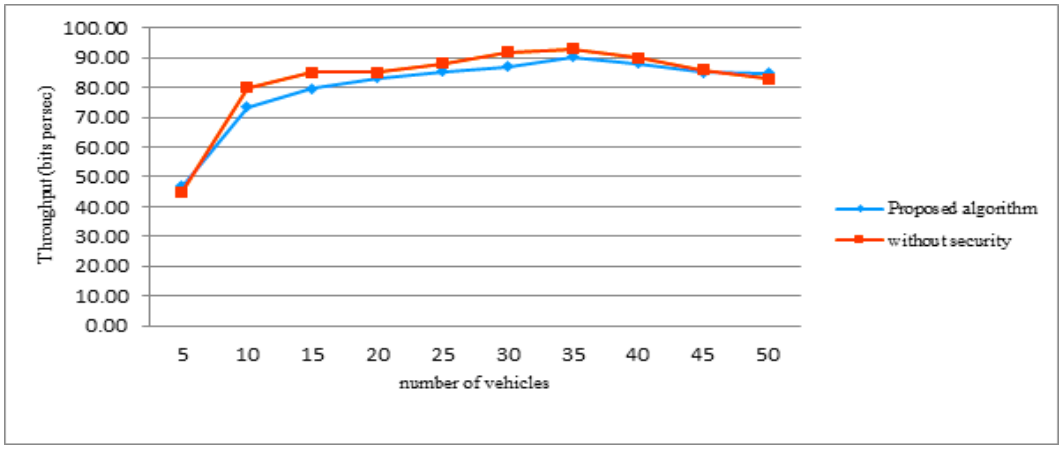


*Figure 4.6 Throughput v/s Number of vehicles*

End-to-end delay is the most important factor in assessing the performance as it evidently depicts how an additional overhead of encryption and decryption increases the delay in processing and response from the receiver i.e., the RSU. We only considered the computation delay which is the time consumed by RSU to decrypt the received message, get the pointer information and PID from the corresponding transaction and generate the challenge message, with encryption using the public key of the PID. The communication delay, which totally depends on the increasing vehicles is also shown in Figure 4.5 and Figure 4.6. However, we haven't analyzed the results as how the delay would be impacted if the speeds of vehicles increase or decrease, but a set of predefined values from 14 to 20m/s in the sumo file are used for evaluation. We noted the delay to be around 45ms for up to 5 nodes, but it increases linearly with nodes advancing from 5 to 10. But post that there is barely any difference in the graphs, considering the minimal amount of time in the ECC encryption and decryption, signature generation and verification, querying the ledger, and verifying the outputs. Thus, we conclude that the slight variation in the two graphs is attributable to these additional steps as depicted in the Figure 4.5.

### 4.6.2. 2. Packet-Delivery Ratio (PDR)

PDR defines the number of packets successfully delivered over the gross packets transmitted. The graph in Figure 4.7 shows the comparison of how many packets are delivered successfully before and after application of the scheme. The packets before encryption have shown a linear rise up to 35 vehicles from 90% to 96% which increases further to 98% as vehicles expand from 35 to 50 vehicles. When we apply the scheme, it is evident from the graph that up to 35 vehicles it is constant at 95%, which starts to drop with increasing traffic on road from 35 t0

50 vehicles. PDR and throughput go hand in hand, but in case of any errors or re-transmissions of packets, the throughput remains same, but PDR is affected.

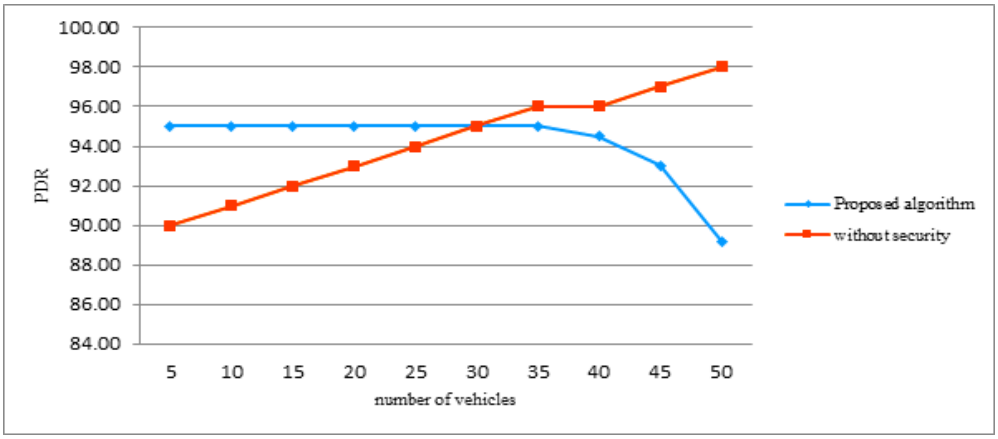


*Figure 4.7 PDR v/s Number of vehicles*

### 4.6.3. Theoretical analysis

In the methodology proposed in [129], RSU uses Diffie-Hellman key-agreement protocol for key establishment whereas in this paper, the TA issues public private key-pair for vehicles using ECC, along with IBE scheme for key establishment. The OBU when enters the vicinity of a new RSU, sends a message to the RSU which is encrypted with the OBU's private key and is then decrypted by the RSU using the former's public key in [129] whereas, in the proposed algorithm, the PID of vehicle, the transaction id and the block pointer are encrypted with the RSU's identity for authentication and the private key of the RSU is further used to decrypt and fetch the contents of the message. The Public key of vehicle is then fetched by the RSU from the block of the ledger and is initially unavailable. The proposed algorithm implements traceability using the concept of hash map and pointer to the ledger and revocation by taking the authenticated transaction as the input and spending the received amount, which sets the revocation flag in the revocation transaction to be true. The CA updates the status as revocated in the hash map. [129] uses a group table for traceability and does not implement revocation. It utilizes the concept of secret keys for message forwarding within the group and hops for communication between the groups. In [129], more time is consumed when the revocation list grows larger.

Issuing of the key-pair by the CA and storing the corresponding PIDi and certificate on the blockchain, assures two things, firstly, when the vehicle communicates with the RSU with these credentials, by confirming with the matching transaction on the blockchain RSU knows they have not been tampered.

Second, it ensures that the vehicles have not been revocated. Our scheme doesn't need the CA to circulate the CRLs for revocation check. This not only reduces the time in verifying the revocated vehicles but leads to quick authentication of vehicles. The mesh network of the RSUs ensures low bandwidth consumption as emergency messages are securely sent to the appropriate areas instead of flooding the network with broadcast messages.

### 4.6.4. Security Analysis

***Security Claim I:*** *Proposed method reduces the dependency on CA thereby reducing the communication overhead in vehicle authentication.*

***Security Proof:*** Unlike traditional methods, whereby the RSU communicates with the CA for identity or pseudonym verification for every communication, in our case we eliminated that dependency by introducing a shared ledger. The dependency on the CA exists, but only for initial System parameters, key generation, and distribution (as we considered a PKI).

In traditional methods, vehicles establish the association with RSU by sending their certificates corresponding to their ID in each communication, but in proposed protocol vehicles only transmit their PID and hash pointers with which the RSU can verify their certificates of existence on the ledger. This reduces the communication overhead with 'no certificates' in communication.

***Security Claim II****: Any external attacker (Ai) neither steal the identity of authenticated node nor alter the packet contents.*

***Security Proof:*** Our protocol is secured against any impersonation attack, which in turn prevents data tampering of the packets and thus provides integrity of data packets. Since we are using the ECC cryptography, to gain access to user keys, he must be able to solve the ECDLP as discussed in section III.D, which is computationally hard enough to make the system secure.

1. An external attacker here, is let's say a new node who tries to penetrate the network, then to gain access to the resources, it must perform successful authentication by communicating the block pointer details, which are not possible to fake, since their existence in the ledger is a proof of existence.
2. The ledger cannot be tampered with as it is cryptographically secure and immutable.

## 4.7. Conclusion

This Chapter discusses a novel and efficient technique of mutual authentication in the VANET environment. The scheme not just authenticates vehicles with reduced dependency on the trusted third party but also preserves their anonymity by not revealing the original identity of users. Despite reducing the communication overhead, the scheme serves to achieve statutory security requirements. It eliminates the need to circulate CRLs by the CA or RSUs, instead mends the status of a vehicle's revocation flag to be true. In the next Chapter, we extend this scheme to find node's trustworthiness by using smart contracts to deal with an emergency scenario, which automatically either updates the ledger for nearby RSUs or sends an alarm to the nearby vehicles depending on the entries of authenticated vehicle database.

Thus, the objectives of the proposed work can be summarized as,

1. Reduced CA dependency
2. Reduced overhead
3. Efficient validation message forwarding
4. Minimal computation at OBU
5. Scalability
6. Source and message authentication
7. Conditional privacy preservation
8. Message integrity, confidentiality, and non-repudiation

# Chapter 5

# IPFS and Smart Contract-Based Vehicle Reputation Classification

*This Chapter is a work towards extending our first research problem, by identifying the issues that persist despite a robust authentication and revocation scheme in place. These issues linger irrespective of the fact that we consider it a network of known 'authenticated' nodes, either because of their greedy or ignorant nature or they might be under the control of a malicious party. In this Chapter we worked towards filling these gaps, and proposing a new solution contemplating our next research challenge as discussed in Chapter 3 and addressing it using our blockchain, smart contracts and IPFS based solution. We worked towards eliminating the need of a centralized party for disseminating and concealing the reputation information. We aim for complete decentralization using blockchain, and smart contracts. The former creates an immutable record of transactions that ever happened amongst the peers, while the later strives to execute a set of instructions upon triggering of an event. We aim to record the messages transmitted (in the form of transactions), as it can be a proven history to ensure non-repudiation and establish a reputation of vehicles based on the validity of messages transmitted and the reputation score maintained. The distributed IPFS network is the storage and retrieval repository used for sharing and storing the reputation of nodes. We analyzed some of the critical requirements of a trust and reputation evaluation model and finally we worked towards fulfilling those in our proposed model. The proposed trust and reputation model stand by to substantiate impregnable requirements in VANET, with proven resolution to decentralization, transparency, reduced latency, dependency on a centralized trust system and more accurate detection of false messages.*

## 5.1. Introduction

Vehicular ad-hoc networks (VANET) are wireless, DSRC [14] enabled networks where each vehicle works both as a network node and a router, thereby facilitating communication between nearby vehicles and standard roadside units (RSU) [7]. For decades, these networks encountered multitudinous security issues. These security and trust issues are attributed to the unique architecture of the network coupled with its dynamic features. For instance, there is intermittent connection and disconnection in the network as nodes travel both in and out of range with one another.

On one hand, the failure to authenticate the different vehicular nodes in the network could lead to the relay of falsified data while on the other, a breach of privacy could lead to unprecedented tracking of vehicles and pose serious threats to human life, especially where accidents result from such activities. But, above all, incorrect assessment of the content delivered by a well-authenticated node can cause trouble and raise issues. This shall lead to no nodes participating in the network owing to trust concerns. Several works in the past decade have been proposed to achieve authentication of nodes, conditional privacy preservation [144], and securing communication, but very less contribution has been made towards evaluating trustworthiness of nodes and data credibility. Trust in nodes specially needs to be evaluated when nodes are authenticated.

Even though users are authenticated, messages are loaded with digital signatures, and certificates, nothing guarantees the trustworthiness of a node within the network due to the absence of any reputed (centralized or decentralized entity) to continuously monitor the functional and behavioral capabilities of the nodes. The self-made decentralized network demands the potentiality to grant each node capability to derive the reputation of every other node. It becomes important that they are self-sufficient.

Over the years, multiple works have been done for accurate evaluation of a vehicle's trustworthiness. These rely on various criteria for assessment. A few models draw reputations from data-based trust model, while others are more focused on entity-based trust model, and role-based trust model [10]. But a definitive trust model should drive upon a hybrid approach to build a vehicle's trust and it should not solely be dependent on a single trusted party. Among all these works, some are centralized, while a recent shift has been observed towards decentralization [8, 47, 81, 86]. In a centralized trust inference, the centralized trusted source manages by gathering multiple inputs and producing an output without any transparency with other vehicles. As per our understanding and the current drawbacks of the trust model, we believe each vehicle should not just have independent rights to query the reputation of a node, but also contribute to its evaluation process, with a clear view of what happens behind the scenes. While many decentralized works have been proposed, they still rely on a centralized

party for disseminating and concealing the reputation information. We aim for complete decentralization using blockchain, smart contracts. The former creates an immutable record of transactions that ever happened amongst the peers, while the later strives to execute a set of instructions upon triggering of an event. We aim to record the messages transmitted (in the form of transactions), as it can be a proven history to ensure non-repudiation and establish a reputation of vehicles based on the validity of messages transmitted and the reputation score maintained. The distributed IPFS network is the storage and retrieval repository used for sharing and storing the reputation of nodes. We analyzed some of the critical requirements of a trust and reputation evaluation model and finally we worked towards fulfilling those in our proposed model.

The proposed trust and reputation model stand by to substantiate impregnable requirements in VANET, with proven resolution to decentralization, transparency, reduced latency, dependency on a centralized trust system and more accurate detection of false messages.

## 5.2. Trust and Reputation model in VANET – Principal Requirements

A message in VANET includes traffic managing instructions, traffic condition, vehicle speed, vehicle position, and other services associated with information that could be deployed for finding alternative routes and seeks out for the nearby service location and so on. However, owing to its distributed, dynamic, and open nature, VANET [51, 60, 96] are subjected to diverse "network security attacks" in recent years.

Particularly, security threats such as wormhole attack, message forging, privacy invasion, and black hole attack are most common in VANET [42-44]. As trustworthy communication is the basis of several applications in VANET, "how to assess and provide data integrity and the trustworthiness of nodes among vehicles" must turn out to be an increasingly significant issue. Numerous solutions were implemented to facilitate secured communication in VANET that falls under two categories: trust scheme and cryptographic technology [45, 46]. The later can provide security in VANET, however, it includes extra power consumption and time delay, thus restraining its applications in dynamic environments particularly under limited energy [47, 48]

As a result, these problems can be dealt with diverse trust approaches that are categorized into three kinds: "(1) vehicle node-based; (2) message-based; and (3) hybrid" [5, 49].

In a complex VANET system, the trust model is a fundamental measure to assess the security of the network. In recent times, merging the "trust management with the mobile model" was extensively deployed. The conventional

trust model of VANET can be categorized into two approaches, the "direct trust model and cooperative computing-based trust model". The former one takes decisions regarding the signals and thus it leads to decision error, whereas the latter cooperates with other nodes and evaluates their trust values [3, 4]. A trust model for the VANET should evaluate trustworthiness based upon the self-observations of the nodes as obtained from either their own sensors or the actions of surrounding nodes. Other than these, the information transmitted by the neighboring nodes should be evaluated. But relying on either one of these is not the sign of a good trust evaluating model. This is true particularly for the latter, as multiple nodes might collude together to send false information, bad-mouth about a reputable node, or state good reputation of a malicious node [104].

Several models and techniques have been presented by different authors in the VANET. These can be categorized as centralized models, de-centralized models, VANET with signature scheme and security and trust-based scheme. To fulfil the security requirements and guarantee trust management in VANET, the following requirements should be mandatorily met

### 5.2.1. Light, scalable, and fast

**Highly dynamic topology:** The VANET environment is highly dynamic owing to the frequently changing topology. The nodes are in touch with each other sometimes just for a fraction of a second. In such scenarios if any messages are to be transmitted and received and acted upon, especially in a crisis, then it requires real-time response. Considering these situations, a distributed approach is the best feasible, rather than depending on a centralized authority to process and store the reputation values of the on-road nodes. Most traffic conditions require to be dealt immediately and hence the model should facilitate a model with minimum processing time and minimum computations.

**Latency issue:** The nodes must be real-time responsive, and therefore this limits the amount of processing and computations that is a node needs to do to compute the reputation score and update the same. The dependent dimensions and attributes for computing the reputation score and evaluating the trustworthiness of node should be minimum to reduce the processing time and reduce the computation load on the OBUs. Thus, the node should not be too dependent on collecting too much of information from the surrounding mobile nodes or static units (such as the RSUs). The amount of time needed in gathering information to assess the trustworthiness of node is directly proportional to the latency in forwarding the received information to other nodes and thus, taking appropriate actions to tackle the situation.

### 5.2.2. Accuracy of Reputation evaluation

**Accurate evaluation:** An accurate algorithm should consider previous history of the node (identity and its behaviors). Even though we want minimum information gathering and computation overhead while computing the reputation evaluation, but it should evaluate the previous history of the node, which can be either gathered either from the neighboring nodes or a trusted party. The algorithm processing the data should take nominal time to inform the node if the received information can be trusted or not.

### 5.2.3. Protection against Collusion attacks/ Fair evaluation

**No-bad mouthing:** Some nodes might just want to spread bad word about other reputable nodes. Even the updating of reputation score by another node should be verified by several nodes. For this a decentralized network/blockchain network with a quick consensus algorithm should be deployed for reputation evaluation. Before a node adds the reputation, score corresponding to a node, it should be verified and then added.

**Collusion attack:** Not just the nodes can bad-mouth for reputable nodes, there might be some nodes, who can collude to contribute in the increased reputation of a malicious or greedy node. This should be completely avoided.

### 5.2.4. Independence of node's movements

As the nodes move along different roads, highways and pathways, the deployed trust model should be accurate irrespective of the paths taken by a node. It should be independent of the route taken and should never presume for a specific path for evaluation.

### 5.2.5. Privacy Preservation

In the process of reputation score evaluation, accepting and forwarding messages, the real identity of the nodes should not be revealed.

### 5.2.6. Reputation Evaluation

We need to keep in account the previous encounters of same nodes, sending messages, but cannot solely rely on this information as most nodes do not even bypass the same nodes often, unless they travel the same path at the same time. In most situations' nodes do not. Therefore, we cannot rely solely on previous encounters with a certain node.

The recommendations of surrounding nodes, both in gathering data trust i.e. whether the data received is trustworthy and the node's reputation who is sending the message is important. But in taking such recommendations, the reputation of the recommending node also must be considered. Hence the total score computing equation needs to consider its reputation factor.

### 5.2.7. Data Trust: How trustworthy is the data?

When a certain information is received, following factors should be considered in evaluating the extent to which it can be trusted:

- The reputation of the node sending the information, which would be evaluated based on a certain parameter as discussed in the following sections.
- How many nodes are sending the similar information over a span of time, and their locations? The ones who have been around particularly during the event-occurrence time can be trusted more.
- How many other nodes are recommending the node sending the information? They can be queried for acquiring the node's reputation, but this must be quick as there cannot be any delay. This must be assessed based on past experiences.

### 5.2.8. Node Trust: How trustworthy is the node?

We just need to be aware of the reputation scores of the nearby neighbouring vehicles.

In our proposed trust and reputation model, the nodes can easily query the reputation of other nodes, in a very transparent way, as each communication is recorded in the distributed ledger. The reputation score is stored in the IPFS network of the VANET nodes, where each reputable node serves as the content provider.

## 5.3. Literature Review

VANET are the most vulnerable kinds of Ad hoc networks, considering not just the dynamic nature but exposure to the various forms of attacks by both insiders and outsiders [102] . Insider attacks are caused by authenticated nodes actively participating in the network. It is important to identify these insider nodes which are behaving maliciously to prevent the consequences of their misbehaviour. The study of multiple misbehaviours in [103], classifies them according to the different intentions and consequent actions on road by the node. There are, therefore, selfish node attacks and malicious attacks. Selfish nodes do not cause any active damage to the network, but they intend to not participate to save their resources and power. Malicious nodes on the other hand can be involved actively in multiple attacks to fulfil a selfish motive, such as sending fake messages of an emergency on a track to get it cleared for itself. Other malicious attacks causing trust issues include message tampering attack, replay attack.

A trust model for the VANET should evaluate trustworthiness based upon the self-observations of the nodes as obtained from either their own sensors or the actions of surrounding nodes. Other than these, the information transmitted by the neighbouring nodes should be evaluated. But relying on either one of these is not the sign of a good trust evaluating model. This is true particularly for the latter, as multiple nodes might collude together to send false information, bad-mouth about a reputable node, or state good reputation of a malicious node [104]. In [10], authors rely on multiple parameters for trust evaluation, particularly the recommendation from the certificate authority or RSU, to reward both the reporting and recommending nodes. The reputation score is also the result of assessment and analysis by the centralized party. The authors in [11] evaluate the trust of both the data and node. Data-trust is evaluated based on the message received and data sensed from multiple vehicles. It is basically to assess how trustworthy the information received is. Node trust is to assess the trustworthiness of node. This has been evaluated based on how good the node is in its functionality and recommendations received from other surrounding nodes.

Evaluation of the different solutions [54, 93, 101-104] highlights a limitation, that, they are all centralized in nature. A key technology that overcomes this centralization limit and assures users of security and trustworthiness is blockchain [105]. The authors note that the technology facilitates the creation of secure environments where the intelligent vehicles can communicate in a peer-to-peer manner.

On the other hand, in [106] a decentralized data credibility system is proposed. This system selects a vehicle from the group of vehicles which is going to validate the received messages and broadcast the rating block. The other

vehicles will then validate the received block using their local knowledge and decide if it should be added to blockchain or not.

The ratings received by the vehicles on observation of the traffic are stored in a block and are chained together using the concept of HASH VALUE. Then, a temporary centre amongst the chain of blocks is selected and broadcasts its rating to others. But, limited by the message's timeliness and vehicle's sensing capacity, the posteriori ratings may have some mistakes.

The proposed system runs on a smart contract embedded in the proposed RepuChain. First, an off-chain reference of the occurred event is created, then the reputation contract facilitates to provide feedback regarding the same. The feedback is positive for the occurrence of the event, with rewards topping up the node's wallet, and updating the reputation score. But, if fake event is detected, the nodes' reputation degrades along with reduction in wallet amount. The contract just like any other smart contract has their own storage, for data reference. The distributed and decentralized storage for maintaining node's reputation is the Inter-Planetary File System (IPFS) [6]. This is also responsible to maintain copies of node's identity certificates. With multiple nodes rendering requisite data in IPFS [6], there is a reduced latency, dependency, and bandwidth consumption for accessing and storing data.

The previous sections highlighted various advantages of IPFS, smart contracts and distributed and decentralized nature while in the latter's case, the technology conceals private details of nodes in the network as they send messages to their peers. Based on these advantages, the current study proposes an algorithm, based on the two technologies, that secures the VANET data and infrastructure.

## 5.4. Background Concepts

As discussed, the model is based upon blockchain, smart contracts and the IPFS distributed storage. We reviewed what blockchain and smart contracts are and how they work in the Chapter 4, but in this section, we would just give a brief overview again and elaborate the role and functionality of the IPFS storage.

### 5.4.1. Blockchain

The blockchain has attained popularity as a decentralized, peer-to-peer, distributed ledger enabling the storage and distribution of data, finance, or other digital assets. Each participant maintains a consistent copy of the transactions that ever occurred in the network, which are added to the chain of blocks after a mutual

agreement among these nodes, as decided by the chosen consensus [8]. Most blockchains serve rewards to the nodes performing the most crucial operation of block mining, as it requires extensive computations to prove the validity of the block. A typical blockchain looks like what is shown is fig 1(Chapter 4).

The blockchain based environments promote the trustworthiness of the network and its data as all peers in the network are involved in verifying the distributed shared data. [145] further add that blockchains are tamper proof as they are often infeasible to modify due to their distributed nature. Such top-notch security features assure users of confidentiality and privacy of their data.

### 5.4.2. Smart Contracts

They are the piece of code running on top of blockchain, containing a set of rules and conditions for executing the code within upon invoking the contract. The contract beforehand contains the parties that can invoke the contract and conditions required to execute the code upon meeting the set conditions.

### 5.4.3. Interplanetary File System (IPFS) storage

The interplanetary file system storms the storage, sharing and database technology with its new distributed, decentralized and 'bit torrent' approach [6]. It plans to overtake the http for retrieval, storage, and update of any resource over the internet in future, owing to 'each node a storage node' mechanism.

While http continues to rule retrieval, storage, and update of resources for nearly about decades now, its disadvantages really started to matter now more than ever with the overflow of data and an increasing number of users.

Following subsections discuss the features, advantages, and disadvantages of this storage which we considered and utilized the capabilities and advantages for our trust and reputation model.

#### 5.4.3.1. Features and advantages of the IPFS storage

**Avoids the breaking links (no duplicates, but availability)**

As we all know each URL gives us access to a resource or data that we are looking for, which is hosted by a server and allows to read, write, or manipulate that same data provided we are authorised to do so. But occasionally we have all experienced the most popular '404' error when we try to visit a website. This occurs due to broken links and unreachability of exact server hosting the data. The

host can decide to remove a certain data or modify the URL, without other user's knowledge and this becomes an issue for dependent users. IPFS resolves this issue by making each node as 'data node'. Instead of reaching out to the centralized server every single time, the IPFS nodes can be queried if they have the file/data, based on the content-hash.

**Offline accessibility**

Offline has become the new online with multiple distributed systems. In IPFS multiple nodes keep the copies of the files/data, and the nearest nodes can be easily queried instead of reaching out the server every time. This makes the data easily available offline.

**Reduced bandwidth consumption with decentralization**

IPFS functioning depends on data content unlike http, which is an IP-addressing protocol. For any file that the owner plans to upload for sharing and storage purpose, is stored with the node within its directory, while the hash of the file along with the node's ID is stored in the Distributed Hash Table (DHT). The DHT stores this key value pair, where key is the node ID and value is the hash of content it provides as shown in fig 5.1. Anyone in the network looking for that file can query for the hash of the document, which provided to the IPFS network is resolved and thus serving the content. This is much simpler as any node which is nearest to the data demanding node can provide the data, unlike http where there is latency, bandwidth consumption and denial of service sometimes, considering centralization.

### 5.4.3.2. Disadvantages of the IPFS storage

While IPFS is meant to revolutionize the whole working of the traditional internet by transforming it into a peer-to-peer, distributed decentralized network, it also suffers from a set of disadvantages , which do not stand in competition to what it offers, but can pose security threats of not handled initially while setting up the network.

**Data deletion issue**

If a data owner wishes to delete data permanently, there is no way to ensure this, as multiple nodes might be keeping a copy of the file. If deletion happens before any other node downloads the file, it can be ensured as permanent deletion, but otherwise no.

**Access control limitation**

The IPFS network is a publicly available network, hence in order to make sure any file is not publicly available, files can be encrypted, which provides access control, but if it needs to be shared with multiple parties again becomes an issue. Solutions such as proxy re-encryption has been proposed to resolve this issue in one of the works, Nucypher [16].

We propose to use private permissioned set of IPFS nodes for registration, where records of user details, time of registration, authority issuing the certificate are recorded, and if modifications, then latest modifications are recorded via. Smart contracts, which would automatically trigger this update, if certain conditions are met, which would be decided while writing these smart contracts. The smart contract ensures only authorized party modifies the content and shares an update on the blockchain in the form of IPFS hash ID.

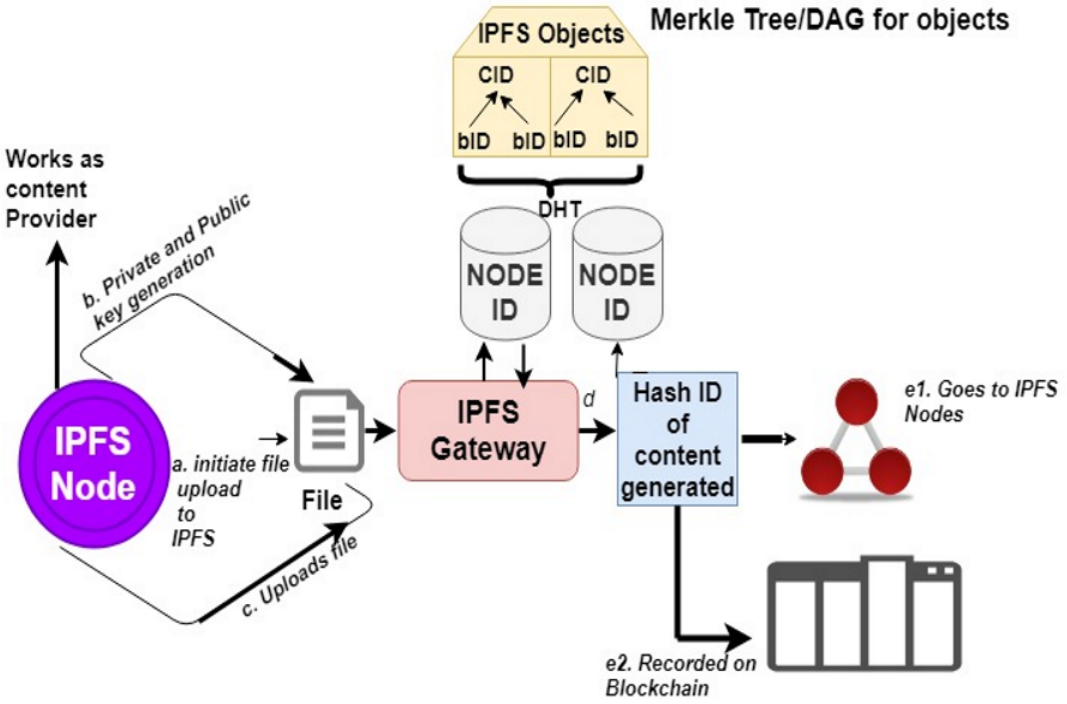


*Figure 5.1 IPFS node uploading data*

## 5.5. Proposed Model

The proposed scheme consists of three phases: registration of vehicles, reputation evaluation (trustworthy message transmission and verification), reputation update and query. The registration of the nodes follows up in a

constrained permissioned environment, where a proof of authority consensus algorithm is used to add vehicles onto the private IPFS network and blockchain. On road the reputed nodes verify vehicles and stores a local copy of recently verified vehicles. This becomes essential as other nodes when wish to query the state of these vehicles do not require to query the IPFS again. The proof of reputation model is used in selecting these reputed nodes from nearby vehicles. There can be more than one of these around the other vehicles. The RSUs are also considered reputed here.

The analogy is like owning a higher number of coins in Bitcoin blockchains where the wealthiest nodes validate new blocks and add them to the chain. However, in this case, proof of reputation model is used to select the most 'reputable' to validate new entries to the blockchain. The process of reputation evaluation and computation is through the deployed smart contract. The flow of interaction between multiple layers is as shown in Figure 5.2.

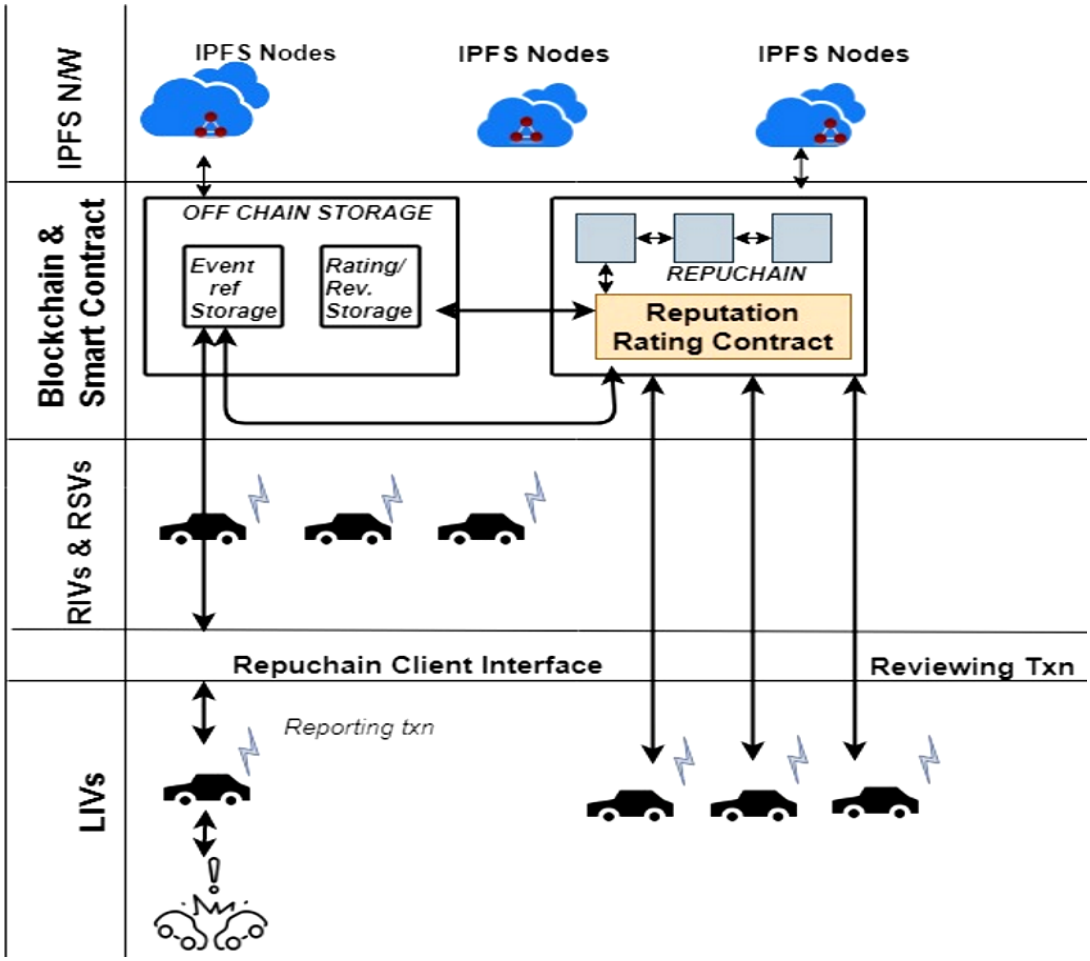


*Figure 5.2 The IPFS, Blockchain and Smart Contract in VANET*

### 5.5.1. Network Composition

The network is a blockchain enabled network w.r.t registration, verification, and reputation management. The entities and data structures building up the network include the following:

#### 5.5.1.1. Entities

1. *Motor Vehicles Division (MVD):* Vehicle owners register with details to obtain the Electronic License Plate no. (ELP).

2. *Law Enforcement Authority (LEA)*: LEA provides the blockchain platform for registration and reputation management, but does not necessarily control it, as we would discuss. The IPFS nodes in the scheme are privately permissioned set of nodes which hold the reputation values of other vehicles. The deployment of smart contracts takes place here for registration and reputation. This ensures traceability of malicious nodes.

3. *Light IPFS vehicles (LIV)*: These are regular vehicles, which registered to the IPFS network, obtained their network parameters, keys and certificate information such as hash ID, asset creation block pointer on the ledger. They are light nodes as they do not have write accessibility to the ledger and the IPFS objects. Due to computation power limitations, they cannot synchronize with the complete blockchain or indulge in mining but can query other IPFS nodes. They are, therefore, the light vehicles.

4. *Reputable IPFS vehicles (RIV)*: The nodes who have established a reputation in the network via proven functionality and honest message delivery as verified by other reputable nodes, come under this category. These have more rights as compared to the LIVs and their recommendations are important in the assessment of reputation of other nodes.

5. *The edge nodes (RSUs)*: The RSUs form the computational layer of the network, where mining of transactions takes place to validate the transactions and add them to the block. Their position in the network layer and functionality comes from their increased computation power and resources as required by the miners.

#### 5.5.1.2. Data Structures

1. *Registration smart contract:* This is included in the registration and authentication ledger, which ensures only valid and authorized users make a new entry, update an old entry with any changes and generate new addresses with these modifications. The transactions are verified by the private permissioned nodes part of MVD and LEA.

2. *Reputation smart contract:* This can be initiated by the LIVs to put their reputation scores in their respective IPFS objects w.r.t surrounding recommendations and truth scores. The reputation of each node is an IPFS object, where any modification is subject to positive reviews from neighbouring nodes and the multi-signature transaction generated by the node and a minimum of RIVs.

3. *The Ledger-Repuchain:* This ledger is solely for the purpose of vehicular management. The nature of the ledger is private and only for vehicular environment. The consensus running on the ledger includes both proof-of-authority and proof-of-reputation.

4. *Off-Chain event information storage:* The emergency event information and details of informing vehicles is stored here.

5. *Reputation review storage:* This stores the different reviews of the vehicles w.r.t to any event reference information. It is used to evaluate the final rating of a vehicles after analysing the reviews.

6. *RepuWallet:* This is user's wallet to manage the public private keys, reputation score and reward points.

### 5.5.2. Assumptions

1. LEA and MVD are assumed to be trusted parties as they are maintaining the set of private IPFS nodes and ensuring the traceability in case of disputes.

2. A second assumption made is that RSUs are the demarcation points for the different networks, that is, only vehicles that are in the proximity of a given RSU can form a network. This allows easier control of blockchain activity and privacy preservation.

Notations for the model are as given in Table 5.1.

*Table 5.1 Notations*

| Notation | Meaning |
|---|---|
| | |
| $E_{ID}$ | Event ID- depends for type of event<br>*01-Accident occurrence*<br>*02-Collision warning*<br>*03-Road blocked* |
| $PID_a$ | Pseudo ID of $a^{th}$ vehicle |
| $RSU_i$ | $i^{th}$ RSU with which a vehicle is associated |
| $l_m$ | Location coordinates as detected by $m^{th}$ entity |
| $t_n$ | Timestamp as recorded by $n^{th}$ entity. |
| $RS_a$ | Reputation score of $a^{th}$ entity |
| $DS_a$ | Digital Signature of $a^{th}$ entity |
| ***ERN*** | Event Reference as generated by the vehicle, using location and associated RSU |
| $RS_a$ | Reputation of node with $PID_a$, computed as<br>*H(NodeID\|\|accumulated_reputationscore)* |
| ***TRS*** | Threshold Reputation Score |
| ***H ()*** | Sha-256 hash function |
| $Txn_i$ | $i^{th}$ transaction generated and broadcasted by a vehicle. |

## 5.6. RepuChain

### 5.6.1. Use Case- Emergency Scenario

In this section we talk about the scenario, types of messages considered, and most importantly the selection of RIVs through our reputation check algorithm.

RIVs are introduced in this proposal to ensure decentralized trust and transparency among the untrusted vehicles. RIVs are the vehicles on road, but with a high reputation score than neighboring nodes. They are selected based upon the number of reputation points gained over a period, which are computed on the truth verifications of different messages sent:

*Message Type 1 ($MT_1$):* These are regular messages which a vehicle would broadcast (in case it loses control due to internal flaws, or bad driving sense) to the neighboring vehicles. These include collision warnings, sudden brakes applied.

*Message Type 2 ($MT_2$):* This is when vehicles spots and emergency and proceeds to broadcasts to the neighboring and probable far away vehicles for caution. This can be an accident, road damage, fallen tree or construction on road, etc.

We are only considering the message broadcasts and not investigating the path traversal of a node to identify if a malicious node delivers or drops a packet on its path, as investigated in [146]. Authors in [146], proposed *watchdog* and *path rater*, to identify and remove malicious nodes, who are part of the network but intentionally silent and not forwarding packets. Our reputation check only works for $MT_1$ and $MT_2$ message broadcasts for evaluating trust, but not detecting or isolating nodes which are not forwarding packets.

Vehicles broadcast the above kinds of messages as per the situation. But it is the neighbors who verify for their authenticity and upload a positive or negative score corresponding to their PIDs. Based upon how many truly verified messages have been received for a vehicle, reputation points are evaluated for the RIVs or LIVs.

Each vehicle has a reputation object in the IPFS which contains relevant information, and the link to the object is stored in the *RepuChain.* The content only contains the reputation score; hence it is stored as it is in the DHT. The link contains the information about which node which hosts the content stored PID and RS. When vehicles receive a message, they query the IPFS nodes. As the LIVs also have rights to download a copy of any vehicle's reputation object, they can easily provide the copy to neighboring vehicles. The vehicles can match the hash to verify if data has been tampered. In this way the vehicles can fairly decide for the reputation of a node without falling for bad-mouthing or colluding attack. Figure 5.3 demonstrates the vehicular node as a *RepuChain* client, and the various interacting modules.

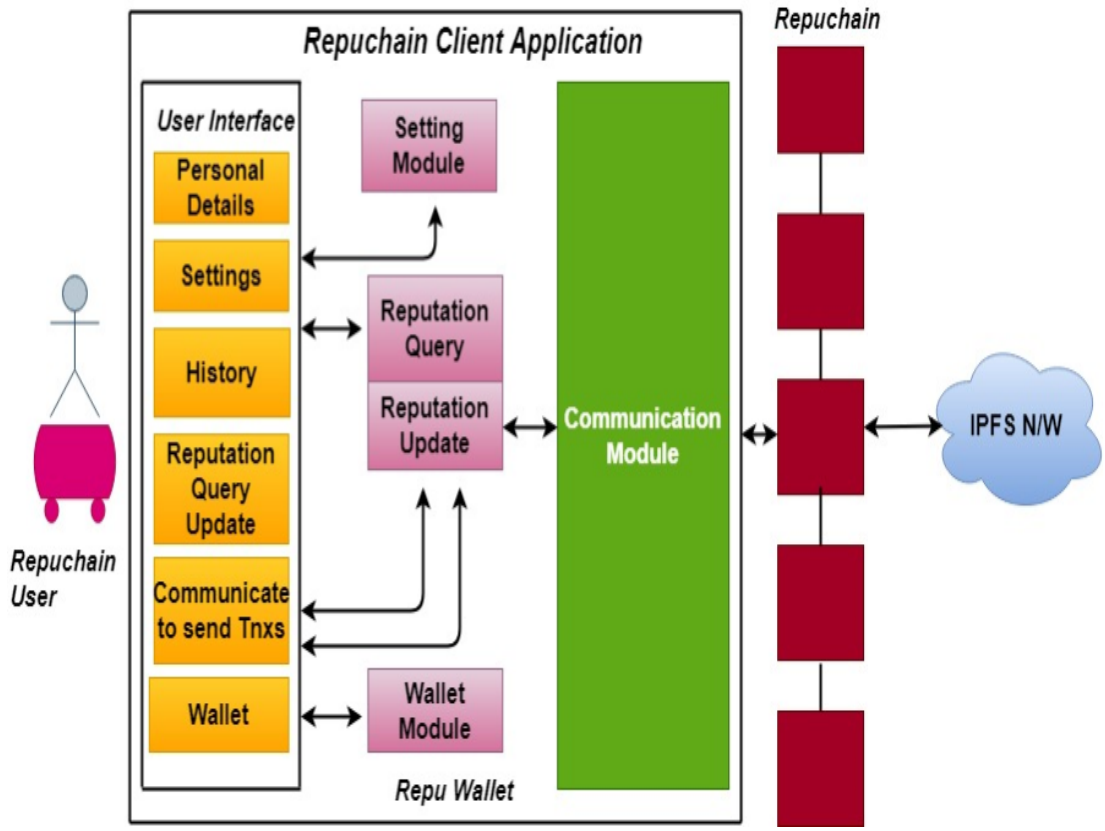


*Figure 5.3 Vehicular node – The RepuChain client*

### 5.6.2. Emergency Detected, reported, and recorded

A vehicle $V_a$ detects an emergency event $E_{ID}$, $MT_{1/2}$ and broadcasts an emergency transaction to the emergency contract with the transaction $Txn_1$ as given in equation (5)

$$\mathbf{Txn_1} = \{PID_a, E_{ID}, MT_1, RSU_i, l_m, t_n, RS_a, DS_a\}. \quad (5)$$

The nearest RIVs and RSUs work towards validating the transaction based upon two criteria –

1. *vehicle's location details '$l_a$' in the past time '$t_a$' and*
2. *querying neighbouring nodes to verify reputation score and if any recent messages received regarding the same event.*
3. *the location as mentioned is associated with the $RSU_i$ near the event. $V_a$'s association is stored with the other RSUs for some stipulated time.*

The location match was the only possibility of verification of the vehicle's message with the reputation score topping trustworthiness of the source. The

RSUs and RIVs query the IPFS network for the reputation score of the vehicle with its $PID_a$ as the search value, and the nearest available node with the block reverting this key, value pair. If $RS_a > TRS$, the message is accepted, else to avoid taking any chances of true message, it is not rejected but added to the cache and more messages regarding the event are waited for a time interval. After validation, block is broadcasted with the event reference details.

The event reference is important as nodes use this to submit a rating later to the *reputation contract.*

The transaction as given in equation (6), generates the event reference number, *ERN* is generated with the $Txn_1$ as input and output includes event reference and details of RIV or RSU whoever verifies and generates the reference number for taking reviews and feedback regarding the same.

$$\mathbf{Txn_2} = \{Txn_{1ID}, \text{EventRefNo}, RIV_i / RSU_i, DS_i\} \quad (6)$$

The nodes accept and take actions according to the event.

The event reference should remain the same, even if multiple vehicles report the event. For this, the nearest RSU association of the event is used to computer event reference number. When multiple vehicles report the same event, the event reference still resolves to same hash as given in equation (7)

$$\mathbf{ERN} = (E_{ID} || RSU_i) \quad (7)$$

The *ERN* should keep track of how many vehicles have reported the same event. For Multiple RSUs coming in the region of the event occurred, as given in equation (8).

$$\mathbf{ERN} = (E_{ID} || RSU_i || RSU_j) \quad (8)$$

The block formation process is as depicted in Figure 5.4**.** The event reference storage is an off-chain storage, which only costs when writes are performed, but not during reads. The process is explained in algorithm I.

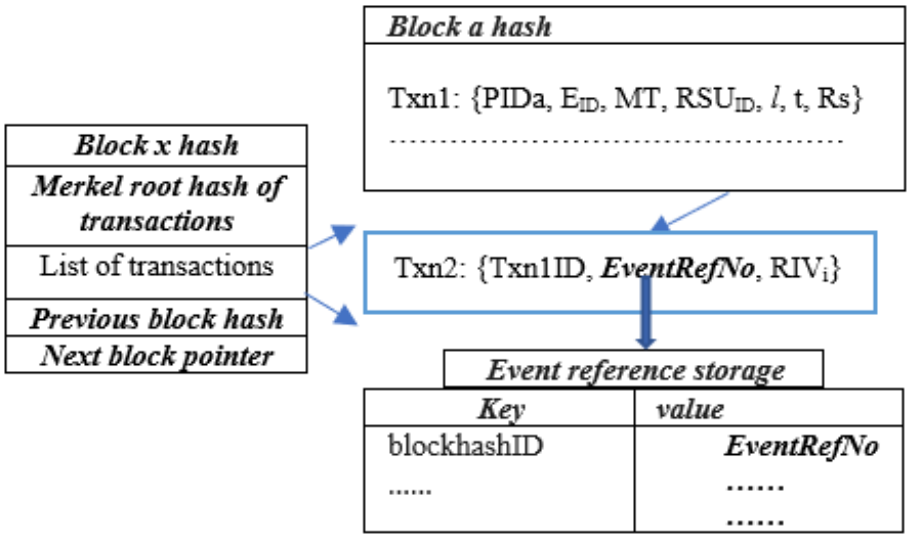


*Figure 5.4 Transaction updating Event reference storage*

**Algorithm I** Emergency event generation and record

**Inputs:** $PID_a$, location $l_i$, current RSU association, $RSU_a$ of the witnessing vehicle. There can be several witnessing and reporting vehicles.

**Outcome:** $E_{ID}$, and *ERN* generation

**Update:** Event reference storage updated

1. **for** each vehicle reporting occurrence of an alarming situation **do**
2. $PID_a$ broadcasts $Txn_1$ with all the information
3. $Txn_1$ received by nearest *RSUs* and *RIVs*
4. **if** (location of reported event == vehicle's last
5. location && last RSU associated can verify location, at time '*t*')
6. **then** validate $Txn_1$ and generate block with new *ERN*
7. **else** reject *Txn1* with warning to reporting vehicle with a probable
8. fake event.
9. **Store** *ERN* in Event reference storage
10. (**key** = *blockhashID*, **value** = *ERN*)
11. **Broadcast** block with the *ERN* to the nearest vehicles
12. **end if**
13. **end for**
14. **EXIT;**

### 5.6.3. Reputation Update- Disseminating feedback

Now, vehicles are required to give feedback regarding this event, and if the feedback falls in the majority category and matches the location of the node, reward points are given in the RepuWallet. The steps are as given in algorithm II.

The feedback is waited for reputation evaluation. The feedbacks invoke the reputation contract, which can only be invoked by vehicle with a good reputation score. The feedback transaction as given in equation (9) goes to the reputation smart contract, which validates the inputs, such as $RS_b$, location $l_x$, and once verified by the RSUs and RIVs, the smart contract updates the reputation score for $V_a$.

$$\mathbf{Txn_3}: \{PID_b, E_{ID}, ERN, l_x, t_{y,} RSU_j, \text{'feedback:1, -1'}, RS_b, DS_b\} \quad (9)$$

Here, $l_x$ = *current vehicle's location,* $RSU_j$= *the same RSU* which falls in region of event.

Now for a positive feedback and event recognition, $V_b$ is rewarded as well with an update of reputation score. The feedbacks are accumulated in the reputation contract storage. The contract utilizes these to update the reputation object of the node in IPFS.

**Algorithm II** Reputation Update Algorithm

**Inputs:** $PID_a$ of the reporting vehicle, $N$ user reviews and ratings $\{R_a, R_b, Rc \ldots R_n\}$, $E_{ID}$, $ERN$, location $l_i$, $l_j$, $l_k$, $l_t$ of $N$ users, last $RSU$ association of these vehicles $\{RSU_1, RSU_2, RSU_3 \ldots\ldots RSU_N\}$ and reputation scores $\{RS_a, RS_b, RS_c, RS_d \ldots\ldots RS_n\}$

**Outcome:** Ratings accepted or rejected based upon location match, reputation score verification and transaction validation.

**Updates:** -Updated reputation Object of $PID_a$
-Updates reputation objects of reviewing vehicles.

1. **for** each vehicle disseminating the review Txns to the *Reputation Contract* on *RepuChain* corresponding to an *EID* and *ERN*, **do**
2. **If** ($E_{ID}$ && *ERN* == valid && location *li* of reviewing vehicle in
3. range)
4. **then** *Txn* -> validated by *RSUs* and *RIVs* && Contract function
5. 1 executed;
6. 
7. **else if** (only *PID* is truly identified, but other parameters not found)
   **then** Contract function 2 is invoked;
   // Vehicles punished with bad mouthing and colluding attack warning.
   **else**
   *Txn* rejected
8. *Contract function1* { // invoked by a valid vehicle with valid inputs
9. *RS* of reviewing vehicle = previous score + 1; {
10. **if** reviewing vehicles rated reported vehicles truthful
11. **then** *RS* of reporting vehicles vehicle = previous score +1;
12. **else**
13. *RS* of reporting vehicles = previous score -1;}
14. }
15. **endif**
16. *Contract function2* { //invoked by identified, but with malicious
17. intention
18. *RS* of invoking vehicle = previous score -1;
19. }
20. **end if**
21. reputation object is modified in IPFS and new *hash value* is generated
22. new block broadcasted which contains updated reputation scores of the
23. reporting and reviewing vehicles
24. **end for**

**EXIT;**

### 5.6.4. Querying Reputation under ordinary situation

If the surrounding vehicles are willing to find out the reputation of a node from a message received (whether alarming or not), then IPFS provides minimum amount of response time owing to its distributed nature.

Unlike in a centralized reputation evaluation and management environment, the nodes' request is routed to the nearest nodes first, and if they have downloaded the copy of the node in question, its reputation score can be forwarded, as shown in algorithm III.

IPFS works with an incentivizing and motivating environment for the nodes. The nodes providing the reputation score of one node, can supply some other verification information, or any other node's reputation score in return. Vehicles supplying blocks of data to other nodes are rewarded by the network, which motivates the network to share as much as possible.

**Algorithm III** Query Reputation Score under normal circumstances

**Description:** If vehicles $V_a$ receives message from $V_b$, which might be suspicious, and $V_a$ wants to query reputation score of $V_b$

Inputs: $PID_a$, $PID_b$, $RS_a$, $RS_b$
Output: Reputation score of vehicles $V_b$, $RS_b$

1. **if** vehicles $V_a$ receives a probable suspicious message from $V_b$
2. **then** Va broadcasts a query messages to nearby nodes,
3. $QM = \{PID_a, RS_a, RS_b,$ *'query for* $RS_b'$, $PID_b\}$
4. **if** nearby vehicles possess block with RSb, then respond with RM
5. $RM = \{PID_l, RS_l, RS_b, blockhash\}$, blockhash is the block with
6. updated reputation score in repuchain.
7. **else** query the actual IPFS network for updated reputation object hash.
8. **end if**
9. **end if**
10. **if** $RS_b > TRS$
11. **accept** message
12. **else**
13. **reject** message.
14. **end if**
15. **end if**
16. **EXIT;**

## 5.7. Model Analysis and Validation

This section discusses the feasibility of the proposed model in the dynamic VANET environment. First, we explain the implementation of the scheme, and assess how many trustworthy nodes are detected and how well the scheme performs in a malicious environment, followed by scrutinizing it theoretically, analysing the latency requirements and then examining it w.r.t security.

### 5.7.1. Implementation and Results

To evaluate the successful working of the reputation evaluation and update algorithm, the functionality of 4 vehicles is recorded and evaluated using MATLAB, analyzed over a period of 90 hours. The graph in Figure 5.5 show how the network preventing colluding attacks, as to how the contract ensures that the rating is evaluated based on true scores as sent by the neighboring vehicles.

Vehicle A participates benevolently in the successful achievement of the network motive. As it disseminates true messages over the period, its reputation score rises in an exponential manner. The increase in reputation score is directly proportional to the rewards in the RepuWallet. For vehicles B, the graph shows a decrement in reputation score after 40-50 hours as fake messages were broadcasted by the node. Vehicles C has not been actively participating to disseminate any true or fake messages and has been a quite spectator, hence a constant nature of his graph. But, for Vehicle D, there has been a rise initially in the score, with a continuous fall after proof of involvement in fake message broadcast, which later improves when the vehicle takes warnings seriously.

The graph in Figure 5.6 shows how the increasing number of malicious vehicles can affect the functionality of network as with more fake messages coming from a location and associated RSU can verify, it becomes hard to discard such messages. But, when number of malicious vehicles are below 40%, it is still easier to distinguish between malicious and trustworthy nodes. Here, a very important role is played by the TRS. It is important to set an accurate value for TRS, so that fake and true messages can easily be distinguished.

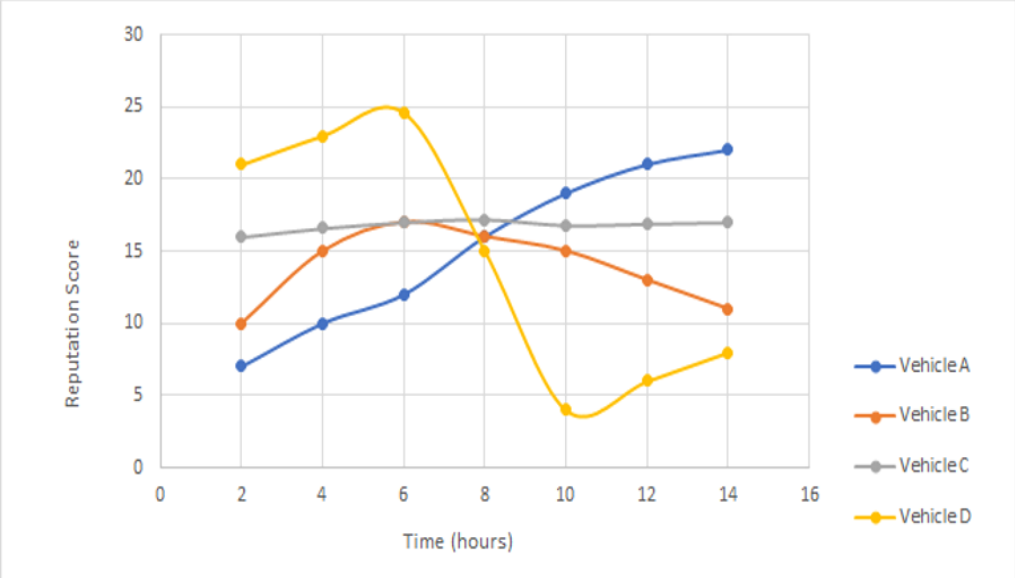


*Figure 5.5 Reputation score update over a period*

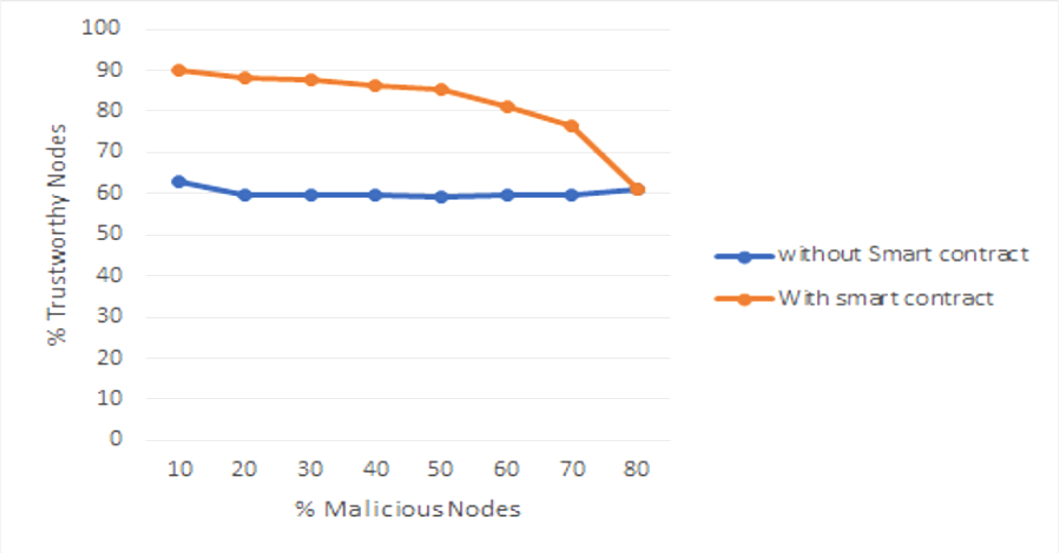


*Figure 5.6 Trustworthy nodes detected with increasing malicious nodes*

### 5.7.2. Theoretical Analysis

In this section, we evaluated our model theoretically, and provided proof for the most important trust requirements claimed to be facilitated by our model.

***Theorem I:*** *A centralized party cannot tamper the rating of a node.*

***Proof:*** The rating of a node is the hash of the file content holding the reputation of the node, *H (NodeID|| accumulated_reputationscore)*. If a centralized party tampers the hash, no querying node can reach the actual value, and would keep discarding messages from such a node. But, since the node itself serves as the content provider and all the modification/deletion transactions are recorded on *RepuChain*, no centralized node would want to lose its reputation by data poisoning.

***Theorem II:*** *The reputation score is available to individual nodes, when queried. There is no centralized dependency.*

***Proof:*** Without any latency and bandwidth consumption, the nearest nodes are contacted first followed by the permanent nodes. The delay hardly varies in the round-trip time for fetching results.

***Theorem III:*** The process of updating a node's reputation is fair and transparent to avoid questioning, and totally prevent colluding or bad-mouthing.

***Proof:*** As discussed in the scheme, each update, and modification is a transaction on the chain. Though older reputation objects might not be on-chain to preserve space and promote scalability, but then they can always be traced for an audit trail.

***Theorem IV:*** The system works with minimum computation and overhead.

***Proof:*** In a blockchain based decentralized environment, validation by the network does not rely on a heavy consensus such as proof-of-work, instead we used proof-of-authority, and proof-of-reputation or PBFT [145] can be used.

### 5.7.3. Security Analysis

The model guarantees message integrity, data poisoning and DDOS attack.

***Security Claim I:*** *Proposed model ensures data integrity and immutability.*

***Security Proof:*** Both blockchain and IPFS strive to achieve data integrity and immutability because of the hash values and pointers safeguarding the content value in IPFS and the blockchain, respectively. Uploading the reputation score involves the input of multiple reviews, and smart contract disables manual inputs. The hash value of a node's reputation object is what represents the content, and the file is maintained with private permissioned IPFS nodes. The multihasht ID of the content (serving as a pointer to the actual content), is stored on blockchain.

***Security Claim:*** *Any external attacker (Ai) neither tamper the reviews or alter the reputation score of any reputed vehicle.*

***Security Proof:*** Multiple vehicles generate review transactions to provide feedback regarding an event occurred. All these are accumulated after verification in the smart contract storage, to calculate the reputation score of the reporting vehicle. Given the pre-coded contract running clearly on If-Then-That logic, it is hard to tamper the reviews or modify the reputation of a node, as there is no centralized control. Also, each transaction as inputs to the smart contracts for event recording or reputation calculation are included in validated block, for transparency.

***Security Claim:*** *The model is secure against DDOS attack and ensures data availability, whenever a node's reputation score is queried.*

***Security Proof:*** The decentralized IPFS DHT storage network as well as blockchain render a transparent, peer-to-peer, immutable and tamper-proof storage. The IPFS storage for files and corresponding pointers to the files in blockchain, facilitate peer-to-peer rendering of data. There are two kinds of data providers in IPFS, one that are temporary, and ones who have downloaded a copy of the file, which is served upon query if the cache is not cleared out. The other kind of providers are the permanent ones, which always host that data as they are the ones owning and providing the data. Due to the multiple copies of data circulating in the network, DDOS becomes impossible.

When the update reputation transaction is created, transaction validation, the smart contract execution, and updating of the reputation object in IPFS takes around 0.050 seconds, whereas querying of the score takes around 0.040 seconds.

***Traceability***

Each transaction is recorded in the blockchain and the smart contract storage evidently sourcing the provenance of the transaction or any update caused by the execution of the smart contract. The transactions are recorded with timestamp, while the smart contracts for the reputation evaluation keep track of the latest update, time of update, sourcing transactions causing the update. All of these ensure traceability in case of any denial, thus providing non-repudiation.

## 5.7.4. Latency

The total delay in the network is a sum of multiple message validations, verifications, processing, and finally cryptographic operations. We discussed the best and the worst-case scenarios in the process of querying and updating the reputation scores.

### 5.7.4.1. Reputation score update:

The complete process of validation of the transaction given by equation (5) after reception by the $RSU_j$ and $RIV_k$, depends on following three steps:

1. Verification of $RS_a$ by querying the other LIVs or RIVs. The query contains key value as hash of the current reputation object file in IPFS and expects the value in return. As discussed and shown in Figure 5.1 the IPFS maintain the DHT as to which node contains which objects/files.
2. *Best case* is when the nearest node already has downloaded a copy of the file or has a cache storage to maintain the node ID and its reputation value (which of course is flushed from time to time).
3. The *worst-case* scenario comes when the copy needs to be downloaded from the IPFS nodes, and the time taken totally depends on the size of the file.
4. Then computation of the EventRefNo is done by the RSU or RIV, as $(E_{ID}||RSU_i)$ The OR operation requires minimal computation. The block after validation is generated with the EventRefNo.
5. Now, the smart contracts take time to verify transactions received for feedback and uses the reviews to update the reputation object of the node and total latency is given by equation (10).

**Total_latency** = $Txn_1\_validation+Txn_2\_validation+Txn_3\_validation$ (10)

#### 5.7.4.2. Reputation score query

The query time totally depends on the number of nodes hopped upon to acquire the required value corresponding to the object hash asked for.
*1.Best Case:* Node is just in the next hop with a copy in cache.
*2.Worst case:* The copy is with none of the nearby temporary IPFS nodes, but instead needs to be downloaded from the IPFS network. This takes time depending upon the file size.

## 5.8. Conclusion

This Chapter progresses to evaluates schemes providing trust in the nodes and the system claiming to provide credible reputation score. Limitations in the existent centralized PKI framework, as well as some of the decentralized works are identified and as a result, a blockchain and smart contract-based solution is envisaged as the best solution. The framework provides decentralization, transparency, immutability and peer-to-peer availability and consistency of every user's reputation value. We evaluated both from the ordinary and alarming situation perspective.

# Chapter 6

# Secure Transmission with Access Control and Key Optimization

*This Chapter is a work towards extending our research and adding the next layer of security. While we already added trust and reputation classification to identify 'greedy authenticated nodes', the focus of this Chapter is providing secured transmission among the vehicular nodes with key optimization and restricting message access to trustworthy nodes.*

*The proposed scheme works under two phases: Secured Message Transmission and Node Trustability Prediction. The security assured message passing is carried out by incorporating the privacy preservation model under the Data Sanitization process before message dissemination. The key used for the sanitization process is optimally tuned by a new hybrid algorithm termed Sea Lion Explored-Whale Optimization Algorithm (SLE-WOA), which is the combination of Whale Optimization Algorithm (WOA) and Sea Lion Optimization Algorithm (SLnO), respectively. The objective function used provides the solution for maximum data hiding with this optimal key. After key computation a simple XOR technique is used to perform data sanitization, by ensuring minimal computations and omitting any kind of latency caused by encryption and decryption processes. The sanitization works on the sensitive data mostly.*

*The blockchain technology is adopted to manage and store the optimal keys generated for the nodes as it would be an immutable storage and records can easily be accessed for desanitization based upon the timestamp. Subsequently, before facilitating any message access, the trustability of the node is evaluated under novel specifics "two-level evaluation process" with a rule-based and machine learning-based evaluation process. Finally, the performance of the proposed model is validated and compared against other conventional methods for certain measures.*

## 6.1. Introduction

The VANET infrastructure in conjunction with the smart vehicles, thus formulating the vehicular network has emerged as a noteworthy scenario in the 5G mobile networks [147-150]. The self-organizing vehicular Ad hoc networks (VANET) currently operate using the DSRC, encompassing vehicles, road-side and centralized infrastructures, where each vehicle functions as a router broadcasting and gathering the circumambient information. The road-related messages are broadcasted to their neighbors by vehicles [151-153], incorporating information in relation to traffic congestions, road conditions, emergency warnings, and so on. On one hand, this offers each vehicle essential and critical knowledge of the traffic situations, thereby enhancing transportation efficiency and safety, yet, it also struggles with multiple issues including, the capability of the network to self-organize within the high mobile network environment, the trustworthiness evaluation of the participating nodes [47, 82, 154-157], their misbehavior detection, their revocation process and CRL management and distribution.

Even though, the neighboring vehicles cannot be completely trusted due to the large variability and mobility of vehicular networks, this is considered as a serious issue if network suffers from the existence of multiple malicious vehicles.

A trust management scheme not only facilitates the vehicles to decide on the trustworthiness [105, 158, 159] of the received messages, but also aids the network operators to decide on the punishments or rewards on appropriate vehicles. Generally, a vehicle's trust value is evaluated based on its past behavior's ratings produced by pertinent nodes, but several works have considered multiple other factors in estimating a nodes' trustworthiness. Existing trust management systems can be classified into two groups, i.e., centralized, and decentralized [47]. In the centralized trust management schemes, the entire ratings are processed and stored within a centralized server, for instance, the cloud server, which computes, stores, manages and provides with each node's reputation score. This suffers from more disadvantages than advantages, considering that it is single point of failure and provides no transparency. Also, since the decision to trust other nodes and the received messages is to be made by any vehicle in a short delay, considering the short contact time on road, hence, the centralized schemes will not always please the meticulous QoS [160, 161] needs in vehicular networks.

In the decentralized trust management schemes, the occurrence of trust management tasks is made either within the vehicle or in the RSU. Therefore, the interactions with network infrastructures are reduced because of the local management of trust values. Decentralization also leads to more transparency and less dependency on a centralized server to evaluate trustworthiness of any node.

Also, to incorporate privacy inherent with the trust scheme, data sanitization policies, procedures and requirements are mentioned in many data

protection and privacy regulations and guidelines. The optimization concept [162-164] plays a major role in making the sanitization more promising.

Recently, blockchain technology, which is considered as the distributed and decentralized computing paradigm (that underpins the Bitcoin cryptocurrency), has played a major role towards making networks independent and decentralized. These include many of the self-organized and self-managed applications such as in VANET, as it is believed to have the capacity and capability to solve more critical problems of information dissemination, providing security and facilitating transparency in VANET. Moreover, this technology grants both security and privacy in P2P networks. In VANET, blockchain is used to maintain the ground truth of information for vehicles so any vehicle can access event information' history in the public blockchain [82].

As we had already designed a reputation system described in the previous Chapter, which considered an emergency scenario to compute reputation scores. But we have not restricted the data access. We are dependent on the Light IPFS vehicles to only transmit to RSUs and other reputed IPFS vehicles which then verify authenticity of the message, but as discussed it only applies to emergency messages. Also, an IPFs network suffers from multiple disadvantages which are being worked upon and our work relied on the assumption of it being a private network, but the data once circulated cannot be completely omitted.

In our machine learning based scheme, we guarantee access control with each message, based upon the node's trustworthiness. Also, we avoid the computationally extensive encryption decryption process and use a simple XOR function to hide the sensitive data. Also, with machine learning we get the cost and time benefits, along with quality and accuracy of results, by simply training our Neural Network with standard values to obtain node classification.

We aim here to establish a trust management system with underlying data privacy with the following research objectives:

- We proposed a new trust management system in VANET comprising two major stages named as 'Secured Message Transmission' and 'Node Trustability Prediction'.
- The assurance of secured message transmission via blockchain technology is given by integrating the privacy preservation model under the Data Sanitization process.
- The key used for the sanitization process is tuned optimally using a new hybrid algorithm named SLE-WOA, which combines the theory of WOA and SLnO algorithms.
- After this, the node trustability is computed in terms of novel terms "two-level evaluation process" via rule based and machine learning-based evaluation process.
- Finally, the performance of the implemented model is validated over other state-of-the-art methods under certain measures.

*Table 6.1 Nomenclature*

| Abbreviation | Description |
|---|---|
| 5G | Fifth Generation |
| DSRC | Dedicated Short Range Communications |
| CRL | Certificate Revocation List |
| RSU | Roadside Unit |
| QoS | Quality-of-Service |
| P2P | Peer-to-Peer |
| BARS | Blockchain-based Anonymous Reputation System |
| JSSDT | Joint Spectrum Sensing and Data Transmission |
| IGHSOM | Improved Growing Hierarchical Self-Organizing Map |
| CL-PKS | Certificateless Public Key Signature |
| V2I | Vehicle-To-Infrastructure |
| HTM | Hybrid Trust Model |
| MDS | Misbehavior Detection System |
| PoW | Proof of Work |
| MN | Mobile Node |
| RSU | Roadside Unit |
| OBU | On Board Units |
| KCA | Known Ciphertext Attack |
| CPA | Chosen Plaintext Attack |
| CCA | Chosen Ciphertext Attack |
| SOM | Self-Organizing Map |
| KPA | Known Plaintext Attack |
| GHSOM | Growing Hierarchical Self-Organizing Map |
| PDR | Packet Delivery Ratio |
| PFR | Partnerships for Renewables |
| RSSI | Received Signal Strength Indicator |
| VANET | Vehicular Ad Hoc Networks |
| CR-VANET | Cognitive Radio VANET |
| IDS | Intrusion Detection System |
| V2V | Vehicle to Vehicle |
| WOA | Whale Optimization algorithm |
| MCC | Mobile Cloud Computing |
| NPV | Net Present Value |

## 6.2. Literature Review

Secure message dissemination along with appropriate trust management, and authentication is the critical requirement of VANET. Several works in the past have contributed towards addressing these issues and have propitiously accomplished it either using a centralized or decentralized approach. However,

each of these has some unperturbed advantages with undeniable limitations. These are discussed as follows, with their reviews in the following sub-section.

In 2019, [82] proposed a novel blockchain model to determine the crucial message dissemination problems in VANET. Further, a local blockchain for real-world event message exchange was created amongst the vehicles in the boundary of a country. This scheme is assumed to be a novel kind of blockchain appropriate for VANET. Subsequently, a public blockchain was presented that stored the message trustworthiness and node trustworthiness within a distributed ledger for secure message dissemination. But it required plenty of computing power and most of the malicious miners could capture the network and gain dominance, thereby causing the decentralized approach a failure.

In 2019, [47] introduced a decentralized trust management scheme based on blockchain technology in vehicular networks. In this work, Bayesian Inference method was used by vehicles for validating the received messages from neighboring vehicles. A rating scheme was generated by vehicles when a message received by nodes, based upon justification for every source vehicle. Further, the trust value offsets of all vehicles in the network were computed using the data added to the blockchain by the RSUs. The ratings uploaded from vehicles were packed within a "block" by the RSU, and every RSU subsequently added their "blocks" to the trust blockchain. The experimental analysis revealed that the implemented structure is feasible and effective in calculating, storing and collecting trust values in vehicular networks. Even though it made an attempt to utilize and exploit the characteristics of blockchain, it could only produce posterior distributions that were heavily influenced by the priors and it often came with a high computational cost, especially in models with many parameters.

In 2018, [79] implemented BARS for establishing a privacy-preserving trust technique for VANET. In this scheme, blockchain was used as the underlying technology for the implementation of the certificate and revocation transparency. Further, to avoid the forged message distribution, a new algorithm named reputation evaluation was introduced that relied on indirect opinions about vehicles, but direct historical interactions. Later, the BARS evaluation was performed using a set of experiments to evaluate the validity, security, and performance. The outcomes demonstrated better establishment of the trust model with conditional anonymity, transparency, robustness, and efficiency for VANET. The most important limitation of BARS is that it is expensive, time-consuming, and difficult.

In 2019, [51] presented a general work to learn about trust management for improving the data transmission and spectrum sensing processes in CR-VANET. Further, a novel JSSDT attack was proposed in the data transmission process, where an attacker could be reported for fake sensing data and packet drops. Afterward, a unified trust management structure was proposed in CRVANET for both processes. Based on this scheme, a weighted consensus-based spectrum sensing structure was introduced for preventing the spectrum sensing

process. The analysis thus implied the efficiency of the introduced trust-based security structures. Weight selection is a crucial step in this method because the entire performance relies on the weights included in the spectrum sensing model. Inappropriate weights could lead to uncertainty in the performance achievement.

In 2019, [165] established a new IDS for wireless and dynamic networks, such as VANET. The IDS was mainly incorporated with a new algorithm including feature extraction and classifier based on IGHSOM in VANET. Two core characteristics were extracted in the proposed algorithm that involved the differences in traffic flow and their positions. The traffic flow was evaluated by the distance range among vehicles, whereas the position was evaluated using a semi-cooperative and voting filter mechanism. Further, two new classification mechanisms were used for relabeling the GHSOM units and for validating the GHSOM balance structure. The experiment showed the advantage of implemented IDS based on stability, accuracy, message scales, and processing efficiency. The hierarchical relations had a lack of representation and the detection time demanded more improvement.

In 2019, [166] introduced an effective CL-PKS approach based on bi-linear pairing to offer conditional privacy-preserving authentication for V2I communication in VANET. In order to accelerate the verification process, the CL-PKS approach was backed by the batch signature verification and it aggregated the signature verification functions. Additionally, the blockchain technology was incorporated over the CL-PKS approach for the efficient implementation of revocation transparency of pseudo-identities before signature validation. Thus, this approach provided better protection and security against a diverse attack with less computational cost, but V2V communication needed the CL-signature model as part of the design process. It also increased network congestion and the performance was bad for long distances between source and destination.

In 2018, [167] presented a novel security model based on vehicular behavior analysis. Moreover, an HTM and MDS were defined to assign a trust metric for each vehicle. The vehicle classification was made based on these trust metrics. The evaluation in terms of performance for HTM and MDS were performed using Groovenet Simulator. The outcomes showed effectiveness of the implemented approach not only upon selecting trustworthy vehicles and monitoring their behaviors, but further on classification and deactivation of malicious ones. But the constraints like specific frequent attacks and intergroup interaction needed more improvement.

In 2019, [168] designed a new decentralized architecture named blockchain-based VANET based on blockchain technology. This process was comprised of four main phases: SBMs upload, blockchain set-up, vehicle registration, and blockchain record. To prevent the location and identity privacy, UGG, IPP, and LPP algorithms were proposed depending on k-anonymity unity and dynamic threshold encryption within the phases of SBMs upload. Further two indicators were introduced namely, connectivity and average distance for

quantifying the availability of k-anonymity unity. Experimental evaluation was performed validating the efficiency of blockchain-based VANET which showed superiority in terms of providing identity and location privacy, but it needed more energy even though it was not a huge distributed computing system. Also, it did not provide local network security.

Table 6.2 explains the features and challenges of the state-of-the-art model on blockchain-based VANET models.

*Table 6.2 Features and Challenges of State-Of-The-Art models on Blockchain-based VANET*

| Author [citation] | Methodology | Features | Challenges |
|---|---|---|---|
| Shrestha *et al.* [22] | PoW consensus mechanism | • Efficiently used in VANET without storage overhead<br>• Effectively handles the trustworthiness | • Needs enhancement to deal with crucial event message dissemination |
| Yang *et al.* [13] | Bayesian inference model | • Effective and feasible for decentralized trust management<br>• Maintains a reliable and consistent database | • Joint assurance of privacy preservation and trust management is needed |
| Liu *et al.* [23] | BARS | • Better transparency and conditional anonymity<br>• Improved robustness and efficiency | • Vulnerable to various attacks |
| He *et al.* [24] | Unified trust management | • Enhanced data transmission<br>• Better effectiveness | • Needs enhancement over the security issues with virtualization and software-defined networking |
| Liang *et al.* [25] | I-GHSOM | • Quick and accurate detection of attacks<br>• Fast extraction of distinct features from the message by vehicle | • Needs further improvement in overhead and detection time |
| Ali *et al.* [26] | CL-PKS | • Reduces the computational cost<br>• Perform efficiently in V2I communication | • Designing of CL-signature model for V2V communication is needed |

| | | | |
|---|---|---|---|
| Hasrouny *et al.* [27] | HTM | • The better capability of vehicles to identify the effect of malicious users<br>• Improved trustworthiness | • Future work required to consider the constraints like specific frequent attacks and intergroup interaction |
| Li *et al.* [28] | Blockchain-based VANET | • Increased data processing time<br>• High efficiency in privacy protection and system time | • Relies on trusted centralized entities |

## 6.3. Background Concepts

The model is based upon blockchain, Machine Learning and the hybridization of two optimization algorithms – Sea Lion Optimization (SLnO) and Whale Optimization Algorithms (WOA). To generate an optimized key which is used for the sanitization process, we used a hybrid algorithm combining the SLnO and WOA.

We reviewed what blockchain is how it works in the Chapter 4, but in this section, we would just give a brief overview of the original optimization algorithms and our proposed hybrid algorithm.

### 6.3.1. Sea Lion Optimization Algorithm

SLnO [169] algorithm is a renowned optimization algorithm, which is developed, based on the hunting behaviour of Sea lions. The sea lions have posed a few attractive features inclusive of fast movement, clear vision, and superior hunting property. Sea lions further have interesting sensitive features named 'whiskers', which support them to determine the correct prey position. These whiskers are useful for sea lions to express the position, shape, and size of prey. When considering their hunting behaviour, the main phases of attack in sea lions are:

1. Tracking and chasing of prey as detected by their whiskers.
2. Pursuing and encircling the prey by calling other members of their subgroups to join them.
3. Attack the prey.

#### 6.3.1.1. Mathematical Modelling

The SLnO algorithm is arithmetically defined in four phases called as tracking, social hierarchy, attacking and encircling prey.

**Detecting and tracking phase**

The whiskers support a sea lion to sense the existing prey and detect their position. This is done while the direction of whiskers is against the water wave's direction, even though, the vibration of whiskers is less as its orientation is on the same present orientation.

Sealion discovers the prey's position and invites other members to join its subgroup for chasing and hunting the prey. The leader among that sea lion is the one who calls others, but it is the other members of the group who then identify and update the position of the prey. This algorithm assumes the target prey as the one that is closer to the optimal solution or presents the best solution. This behaviour is arithmetically expressed as per Equation (11), in which the distance among the sea lion and target prey is defined as $\overrightarrow{Dis}$, the vector position of sea lion and target prey is indicated as $\vec{S}(t)$ and $\overrightarrow{M}(t)$, respectively, $t$ is the present iteration and the random vector is expressed as $\vec{G}$.

$$\overrightarrow{Dis} = \left| 2\vec{G}.\overrightarrow{M}(t) - \vec{S}(t) \right| \qquad (11)$$

In the subsequent iteration, the sea lion shifts over the target prey to get closer. The arithmetical modelling of this behaviour is expressed using Equation (12), in which the next iteration is given by $(t+1)$ and $\vec{H}$ gets decreased gradually over an iteration course to 2 from 0.

$$\vec{S}(t+1) = \overrightarrow{M}(t) - \overrightarrow{Dis}.\vec{H} \qquad (12)$$

**Vocalization phase**

Sea lions can survive both in land and water. On comparing the sea lions sound, the sound in air is moved four times faster than the sound in water. While on prey hunting, the communication of sea lions is made via several vocalizations. Furthermore, they pose the capability of identifying the sound both on and under water. Hence, after identifying the prey, the sea lion invites the other members for encircling and attacking the prey. This is arithmetically computed as per Equation (13), (14) and (15), in which the speed of the leader's sound is depicted as $\overrightarrow{S_{leader}}$, the sound speed in water and air is symbolized as $\overrightarrow{P_1}$ and $\overrightarrow{P_2}$.

$$\overrightarrow{S_{leader}} = \left| \left( \overrightarrow{P_1}(1 + \overrightarrow{P_2}) \right) / \overrightarrow{P_2} \right| \qquad (13)$$

$$\overrightarrow{P_1} = \sin\theta \quad (14)$$

$$\overrightarrow{P_2} = \sin\phi \quad (15)$$

**Attacking phase**

In the exploration phase, two stages are exploited under the sea lions hunting behaviour and are exhibited as follows:

***Dwindling encircling approach:***

This approach is based on $\vec{F}$ value in Equation (12). Largely, $\vec{F}$ value is decreased progressively via a course of iteration from 2 to 0. This decreasing factor directs the sea lion to forward on and encircle the prey.

***Circle updating position:***

The bait ball of fishes is chased and attacked by sea lion from edges and is stated as per Equation (16), in which the distance among the search agent (sea lion) and best optimal solution (target prey) is given as $\overrightarrow{M}(t) - \vec{S}(t)$ the absolute value is computed as $|\ |$ and the random number is explained as $l$ and it falls between -1 to 1.

$$\vec{S}(t+1) = \left|\overrightarrow{M}(t) - \vec{S}(t).\cos(2\pi l)\right| + \overrightarrow{M}(t) \quad (16)$$

**Prey Searching**

Based on the best search agent in the exploration part, the position update of the sea lion is formulated. The search agent's position update within the exploration phase is exploited in compliance to the chosen random sea lion. It is further said that the SLnO algorithm performs a global search agent and identifies the global optimum solution, while $\vec{F}$ is larger than 1. This is explained using Eq. (17) and (18).

$$\overrightarrow{Dis} = \left|2\vec{B}.\overrightarrow{S_{rnd}}(t) - \vec{S}(t)\right| \quad (17)$$

$$\vec{S}(t+1) = \overrightarrow{S_{rnd}}(t) - \overrightarrow{Dis}.\vec{H} \quad (18)$$

## 6.3.2. Whale Optimization Algorithm

WOA [170] is a renowned optimization concept based on humpback whales' bubble-net feeding behaviour. The mathematical demonstration of WOA is exhibited in the following:

**Shrinking encircling mechanism**

The prey's current position is identified at the time of hunting course by whales. After that, the prey is encircled by them. The target prey is assumed as the recent best solution; next to this, the position gets updated for attaining the optimal solution. The whale's encircling behaviour is explicated as per Equation (19) and (20).

$$\vec{F} = \left| \vec{W}.\vec{S}^{*}(t) - \vec{S}(t) \right| \quad (19)$$

$$\vec{S}(t+1) = \vec{S}^{*}(t) - \vec{H}.\vec{F} \quad (20)$$

In this, the present iteration is depicted as $t$, the best solution's position vector is signified as $S^{*}$, the coefficient vectors are expressed as $H$ and $W$, and the vector's position is portrayed by $S$, then element-by-element multiplication is enabled based on "." Function and the absolute value is stated as $|\ |$. $S^{*}$ needs to be updated if they exist in the best solution. The vectors $H$ and $W$ are evaluated as per Equation (21) and (22).

$$\vec{H} = 2\vec{s}.\vec{x} - \vec{s} \quad (21)$$

$$\vec{W} = 2\vec{x} \quad (22)$$

In this, the $s$ value addresses a gradual reduction that lies between 2 to 0 and a random vector $x$ is designated to have the range [0,1].

**Spiral Updating position**

The position update among the prey and humpback whale is computed numerically using the spiral equation in Equation (23) and (24).

$$\vec{F} = \left| \vec{S}^{*}(t) - \vec{S}(t) \right| \quad (23)$$

$$\vec{S}(t+1) = \vec{F}'.e^{dz}.(\cos 2\pi z) + \vec{S}^{*}(t) \quad (24)$$

In this, the logarithmic spiral's shape is explained based on $d$ and is considered to be a constant, and the random number is exploited by $z$ and is spread out constantly between -1 to 1. The numerical modelling of probability

estimation is performed using Equation (25), in which every feasible path for encircling is denoted as $pb$.

$$\begin{aligned} \vec{S}(t+1) &= \vec{S}^{*}(t) - \vec{H}.\vec{F} \qquad if\ pb < 0.5 \\ \vec{S}(t+1) &= \vec{F}'.e^{dz}.(\cos 2\pi z) + \vec{S}^{*}(t)\ \ if\ pb \geq 0.5 \end{aligned} \tag{25}$$

Moreover, the random value $H$ plays its major role in the global updating of the search agent. Equation (26) and (27) defines the mathematical formulation of this WOA theory. In Equation (27), $\vec{S}_{rad}$ is decided as an arbitrary value from the whales during the current try-out run.

$$\vec{F} = \left|\vec{W}.\vec{S}_{rad} - \vec{S}(t)\right| \tag{26}$$

$$\vec{S}(t+1) = \vec{S}_{rad} - \vec{H}.\vec{F} \tag{27}$$

## 6.4. Proposed Hybrid Algorithm (SLE-WOA)

The WOA is a recently developed nature-inspired approach that imitates the hunting characteristics of humpback whales, whereas the SLnO algorithm is initiated based on the sea lions' hunting behaviour in nature. Both these algorithms have attained better performance in numerous terms yet suffer from premature convergence which impacts them to get trapped in local optima. Hence, this paper tries to implement a new improved algorithm by hybridizing these two algorithms (WOA + SLnO). For this, the SLnO concept is incorporated inside the WOA algorithm and is thus named as SLE-WOA. Here, the exploration phase of a sea lion in Equation (18) is considered for this hybridization. In the conventional WOA algorithm, when the probability $pb < 0.5$, two conditions are evaluated, one is if $|H| < 1$, where , the position update is computed using Equation (19) and on other conditions $|H| \geq 1$, the position update is computed based on Equation (24). In this proposed work, the modification is formulated over the condition $|H| \geq 1$, where the update equation of WOA is replaced by the sea lion equation given in Equation (16). The flowchart of the proposed SLE-WOA approach is depicted in Figure 6.1.

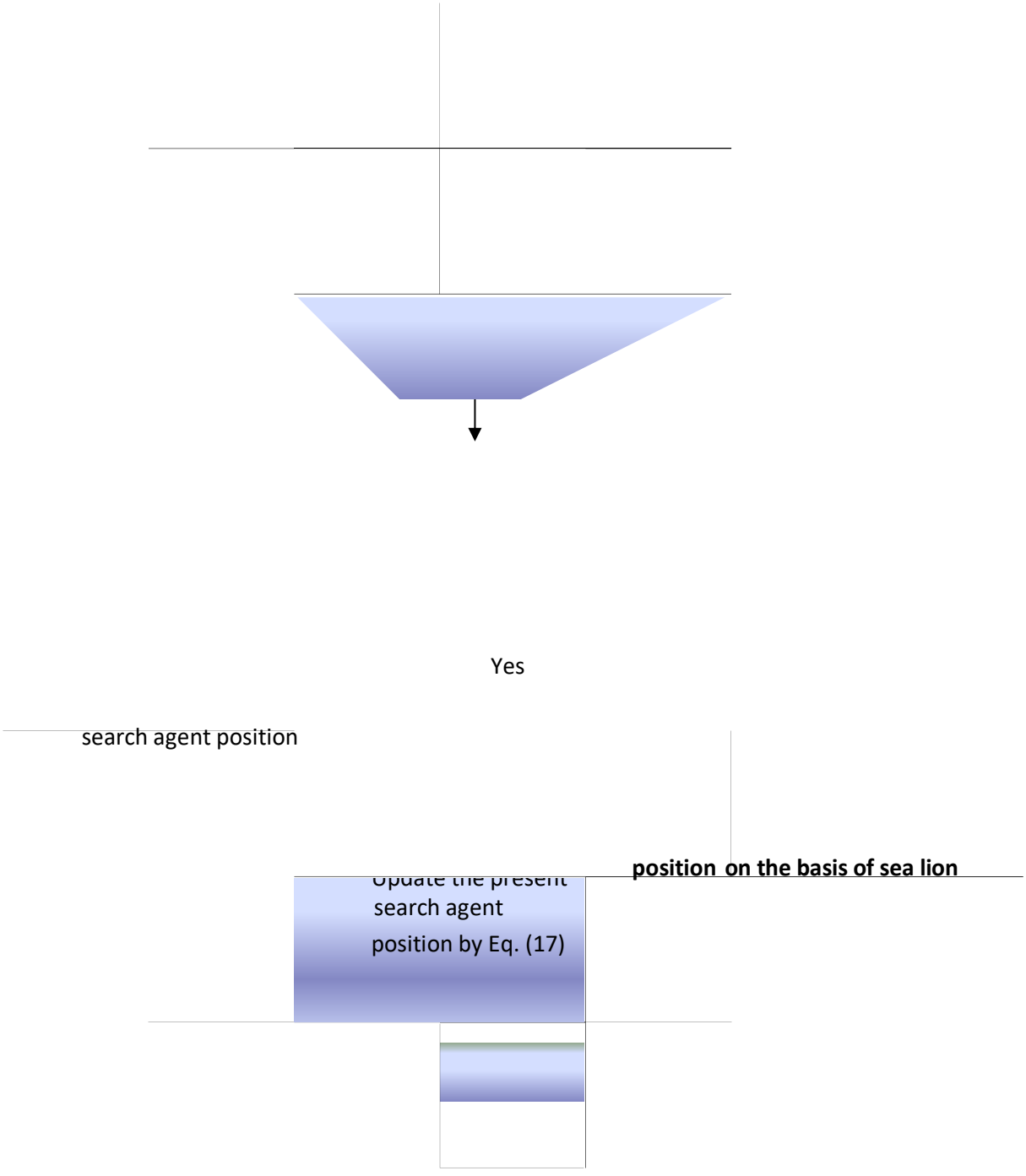


*Figure 6.1 Flowchart of Proposed SLE-WOA Algorithm*

## 6.5. System Model

This section explores the system model of the proposed SLE-WOA. As seen in Figure 6.2 data is sanitized before transmission. From sanitization, the block chain storage is assisted to access model generated by the nodes. The VANET model consists of nodes that attempts to access messages. A node then defines several properties as credentials. From the node, the requested message is sent to the access model. If the authentication is successful, then the desanitization takes place otherwise the above process is repeated until the authentication is successful. The sanitization and desanitization are done using the optimal key.

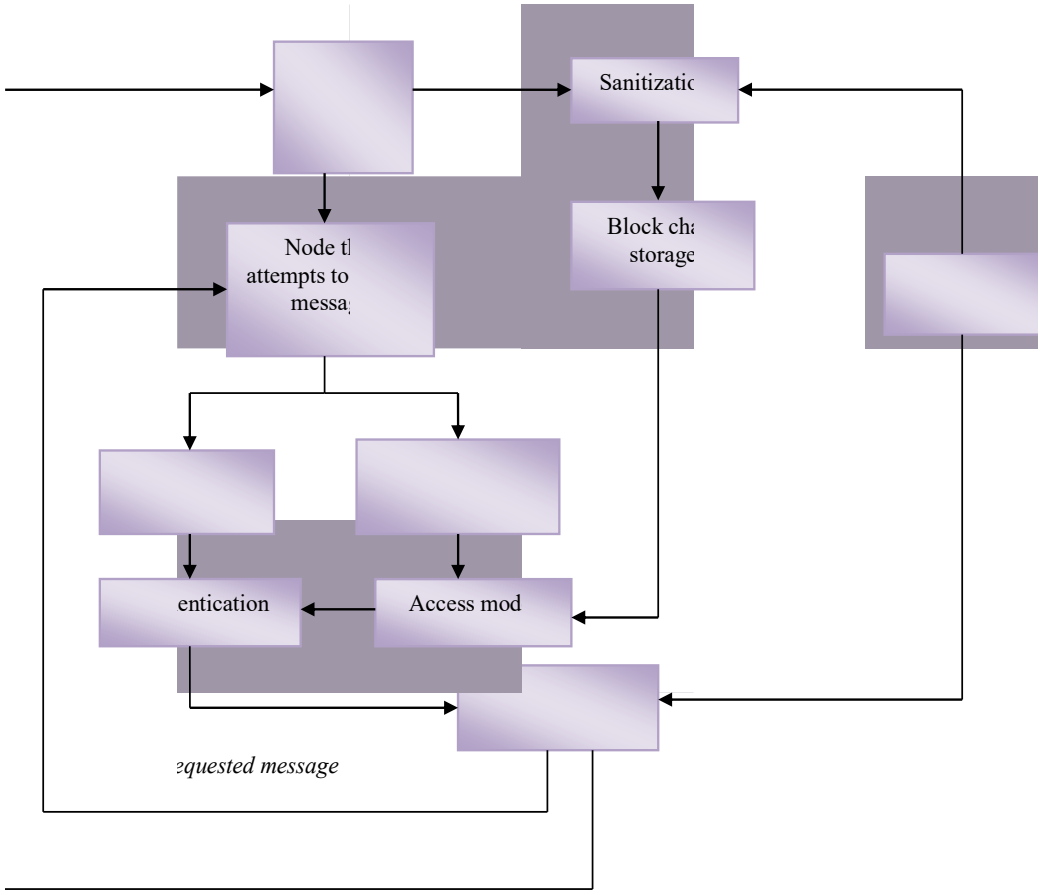


*Figure 6.2 The system model of the proposed SLE-WOA*

## 6.6. Overall design and architecture of proposed framework

Our proposed scheme considers the vehicles moving under different RSUs. As the core work focuses on secured VANET, message transmission is critically required to be safe. Hence, rather than passing the message in its original form, it is sanitized before transmission. The sanitization process assures the privacy of data transmission while communication, as explained in the subsequent section.

For sanitization process, the key is a major requirement. This process begins with a source willing to broadcast a message, consequently making a key generation request to the respective RSU. This key generation optimistically takes place through an optimization algorithm, which is further explained in the next section. The RSU then maintains this key using blockchain technology, and the sanitized data is broadcasted among vehicles.

Now, when the receiver is trying to access this message, it requests for the corresponding key from the in-range RSU. Before granting the key, RSU makes a trust evaluation to decide whether the node is authenticated and trustworthy or not. For this, a new logic of two-level trust evaluations is proposed in this paper, and it is given in the further sections.

At each timestamp, vehicle mobility alters the RSU coverage, and thereby the key request for the sanitization process happens accordingly to the in-range RSU. Moreover, all the RSUs are connected to the centralized server to which the keys (in the form of blocks) get shared. Figure 6.3 depicts the proposed architecture of trust evaluation based on VANET communication.

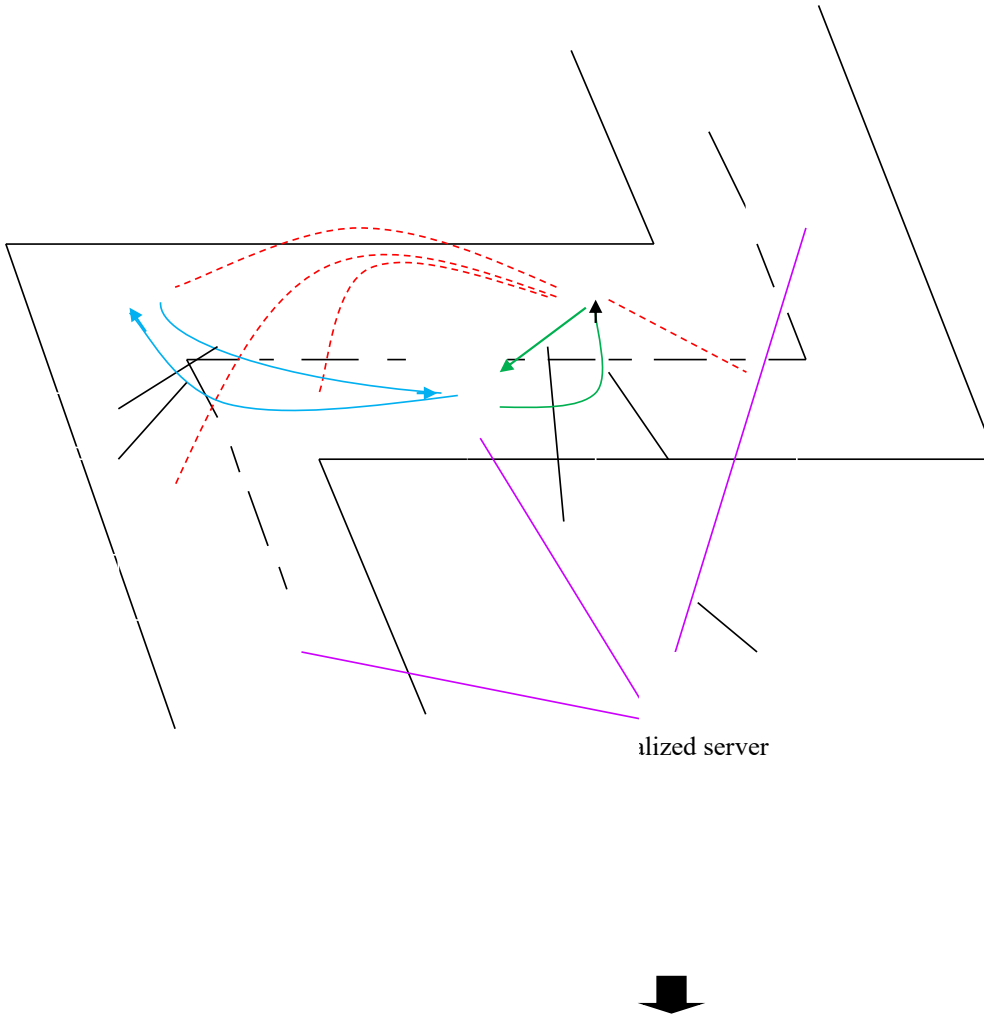


*Figure 6.3 Proposed architecture of Trust evaluation based VANET communication*

## 6.6.1. Data Sanitization for Secured Message Transmission

### 6.6.1.1. Optimal Key Generation

Sanitization is considered as the data hiding process, in which sensitive data is sanitized using a key , which plays a major role in this sanitization process. It is arithmetically defined in Equation (28). and its length is stated as, key length= [Number of records ×1].

(28)

As the key should be optimal, this paper introduces a new hybrid optimization algorithm for generating the optimal key in RSU. The hybrid algorithm used for the key generation is the hybridized form of SLnO and WOA.

For instance: let us consider the data as $d_1 : [2 \quad 1 \quad 3]$, in which '1' is the sensitive data to be sanitized, and the respective key is predicted as '2'. This key value '2' is XOR-ed with the sensitive data to generate sanitized data.

The key generation process is made in two phases under the sender and RSU, based on fitness function in Equation (29). The process of optimal key generation is as follows: Initially, the sender requests a key from their in-range RSU. Subsequently, the optimization process using the proposed hybrid algorithm takes place at both sender and RSU which is as follows:

***Population Initialization***

Once the key request is received, the RSU provides a random key to the Sender.

***Fitness Evaluation***

The Sender evaluates the fitness (objective) to finalize the optimal key and the fitness score is sent back to the RSU**.**

***Updating***

If the fitness is attained, that key is kept as the optimal key and provided to the sender, but if required fitness is not attained, the key is updated and sent again to the sender for evaluating fitness and obtain the new fitness score. This process continues, until an optimal key is provided to the sender. Figure 6.4 delineates the key generation process using the proposed algorithm.

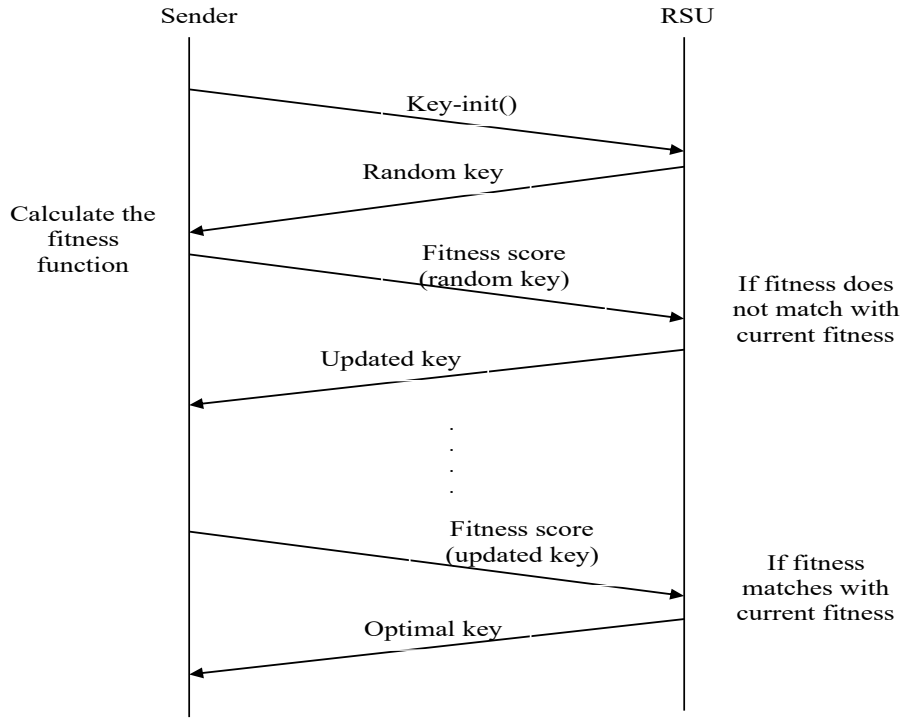


*Figure 6.4 Optimization-based Key generation process*

#### 6.6.1.2. Key Storage using Blockchain

We used blockchain technology to store the key into respective RSUs. Let us assume a scenario, vehicle is under mobility, and at each interval of Ts=5, it transfers a message and hence requests a key from the respective RSU for sanitization process. As per Figure 6.4. when Ts=5, request , which is stored in block 1 of RSU 1. Then the key is also shared to neighbourhood RSU, RSU 2. When Ts=10, is under RSU 2, and during message transmission, it requests the key from RSU 2 which then provides the same as well. Thereby, is stored along with as shown in Figure 6.5. The Scenario of Key storage using blockchain technology is shown in Figure 6.5. Then the generated key by RSUs is shared with a centralized server.

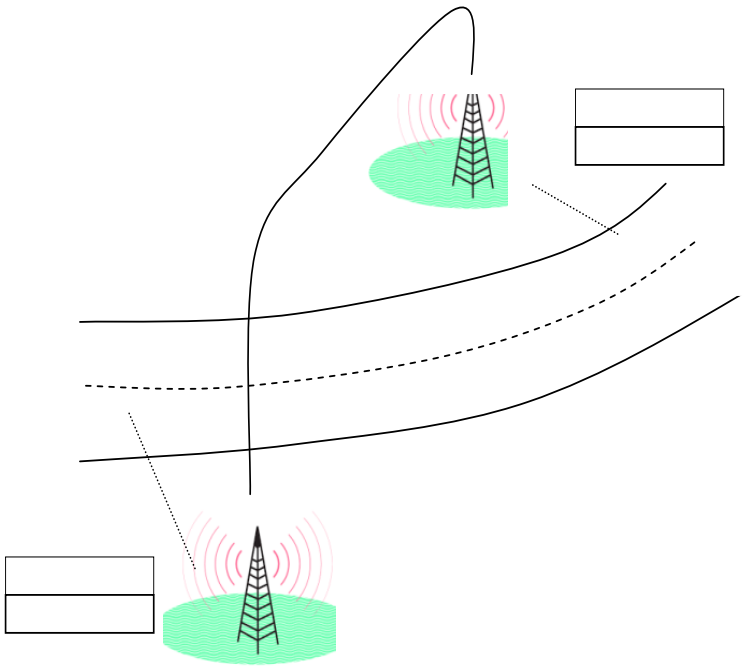

*Figure 6.5 Scenario of Key storage using BlockChain Technology*

#### 6.6.1.3. Derivation of Optimal Key: Objective Function and Solution Encoding

The objective function of the proposed VANET simulation approach is presented as per Equation (29), derived from Equation (30), (31), (32). The solution encoding that is given as input to the proposed model which is illustrated in Figure 6.6.

$$Obj = \mathrm{m} \tag{29}$$

where,

(30)

(31)

$$DR = abs(original\ data - sanitized\ \ data) \tag{32}$$

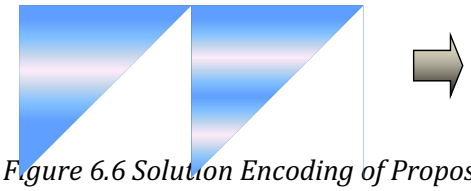

*Figure 6.6 Solution Encoding of Proposed model*

### 6.6.2. Data Accessing by Receiver: Proposed Trust Evaluation for Access Control

Once the sanitized message is broadcasted, and the receiver vehicles are trying to access the data, they need the relevant key to access the original data. Hence, a recipient vehicle sends a key request to the corresponding RSU. However, RSU makes the trust evaluation to decide "whether to provide the key to this requesting vehicle?", for which, we introduced a new trust evaluation process in this paper. With this trust evaluation process, if receiver is proven to be authenticated, it gets the key to access the original data and restores it, but, if the RSU discovers any maliciousness and uncovers that the requesting vehicle as unauthorized, it straightforwardly neglects its request.

To make the evaluation strong, the process progresses with two levels:

**(1) Rule-based evaluation (Level 1)**

**(2) Neural Network-based trust evaluation (Level 2)**

In this process, the receiver is firstly examined under an evaluation process which leads to uncover whether the node (vehicle) is an intruder or not. This is continued by integrating some rule-based evaluation, which is comprehensibly

explained below. If any condition under this rule-based evaluation is unsatisfied, the evaluation process is then advanced to next level, i.e. the NN model, which decisively classifies whether the node being assessed is authorized or not. Figure 6.7 explains the architecture of the proposed trust evaluation model.

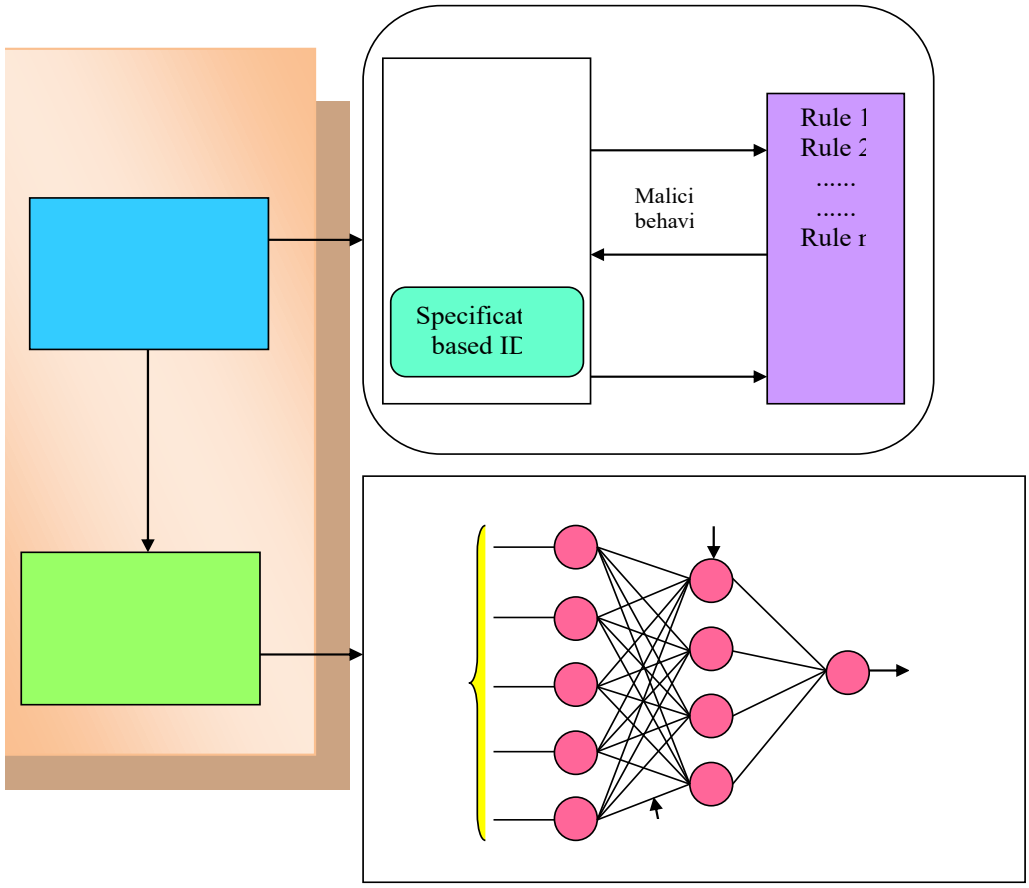


*Figure 6.7 Architecture of Proposed Trust Evaluation Process*

### 6.6.2.1. Rule Based Evaluation

Here, the trustability of nodes are evaluated using rules defined for the expected vs received values of PDR, PFR and RSSI values. For the node which is under assessment of trustworthiness, if the PDR, PFR and RSSI values reach beyond the threshold values , and , then the node is said to be malicious with the specified attack. Algorithm 2 explains the detection rules for various attacks.

nput: PDR, PFR RSSI values of nodes – *Node*)

if $\begin{pmatrix}(PDR_{ID-Node} > \delta_{PDR}) \,\&\, (PFR_{ID-Node} > \delta_{PFR}) \,\&\, \\ (RSSI_{ID-Node} > \delta_{RSSI})\end{pmatrix}$ /*the node is subjected to DoS attack*/

send $Vote\_Message(attack, ID-Node)$ to RSU

else

send verification (ID-Node's RSSI, PDR, and energy level values, PDR of ID-Node's neighbouring nodes) message to RSU

end

#### 6.6.2.2. NN-Based Evaluation

If the condition under the above rule-based evaluation (Level 1) is unsatisfied, the evaluation process is then advanced to next level (Level 2), i.e. the NN model, which is already trained using some standard PDR, PFR, and RSSI values, thus enabling it to classify whether the node under examination is authorized or not. Thus, at the time of testing, the trustability of node is easily predicted. The NN model [171] is as follows:

Eq. (33), (34) and (35) explains the network model, in which $i$ denotes the hidden neuron, $\hat{w}_{(ik)}^{(o)}$ depicts the output weight from $i^{th}$ hidden neuron to $k^{th}$ layer, $IN_{(n)}$ portrays the input neuron's count, $HI_{(n)}$ signifies the hidden neuron's count, $\hat{w}_{(\tilde{b}i)}^{(HI)}$ exhibits the bias weight to $i^{th}$ hidden neuron, $\hat{w}_{(li)}^{(HI)}$ delineates the weight from $l^{th}$ input to $i^{th}$ hidden neuron, $\hat{w}_{(\tilde{b}k)}^{(o)}$ expresses the output bias weight to $k^{th}$ layer, and $NF$ terms as the activation function. $\overline{OU}_k$ is stated as the network output, predicted output and it is demonstrated in Equation (34), $OU_k$ is portrayed as actual output.

$$\overline{HO}^{(HI)} = NF\left(\hat{w}_{(\tilde{b}i)}^{(HI)} + \sum_{l=1}^{IN_{(n)}} \hat{w}_{(li)}^{(HI)}\left(Inputfeatures\right)\right) \tag{33}$$

$$\overline{OU}_k = NF\left(\hat{w}_{(\tilde{b}k)}^{(o)} + \sum_{i=1}^{HI_{(n)}} \hat{w}_{(ik)}^{(o)} \overline{HO}_i^{(HI)}\right) \tag{34}$$

$$ER^* = \underset{\left\{\hat{w}_{(\tilde{b}i)}^{(HI)}, \hat{w}_{(li)}^{(HI)}, \hat{w}_{(\tilde{b}k)}^{(o)}, \hat{w}_{(ik)}^{(o)}\right\}}{\arg\min} \sum_{k=1}^{O_{(n)}} |\, OU_k - \overline{OU}_k \,| \tag{35}$$

## 6.7. Model Analysis

### 6.7.1. Simulation Setup

The proposed trust management system is implemented in MATLAB. The dataset used for evaluating the trustability of the node is the KDDcup dataset. Then some analysis is also performed to prove the betterment of proposed work:

- The analysis of proposed work is carried out for certain attacks like KCA and CCA attacks, KPA and CPA attacks along with rejection ratio and key sensitivity, respectively.
- Next, the analysis of the NN classifier is performed over other state-of-the-art classifiers like SOM [172] and GHSOM [173] with respect to sensitivity, specificity, accuracy, and precision, FPR, FDR, FNR, MCC, F1-score and NPV.
- The analysis gets extended by comparing the implemented hybrid algorithm to other classical models like WOA [170], SLnO [169], GA [174] and DA [175].
- Followed is the analysis for the proposed and Conventional Models, such as WOA [170], SLnO [169], GA [174], and DA [175] by considering KPA and CPA attack.
- Further, the performance of the NN Model in Trustability Prediction is performed over the classifiers like SOM [172], GHSOM [173], and NN [171] with respect to Accuracy, Sensitivity, Specificity, Precision, FPR, FNR, NPV, FDR, F1_score, and MCC.

### 6.7.2. Analysis of Rejection Ratio

Figure 6.9 shows the count of nodes that get rejected by the proposed work under both the rule based and NN based scenario. The formulation of the rejection ratio is defined in Equation (36). Moreover, the analysis (number of rejections) is made for each time stamp. While analysing, more rejections have been done under NN based trust evaluation. More particularly, at the 4$^{th}$ timestamp, $T_s$=20, 100% of the nodes that are subjected to the NN model for trust prediction are rejected, which shows that these nodes are malicious. Similarly, the rejection ratio at each time stamp is plotted in the graph.

$$\text{Re}\,jection\ ratio = \frac{No\ of\ rejections}{No\ of\ attempts} \qquad (36)$$

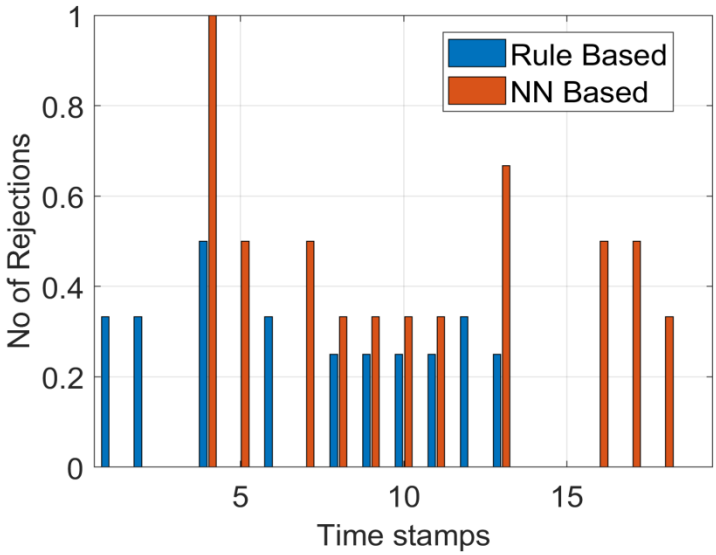


*Figure 6.8 Analysis of Rejection Ratio: Level 1 and Level 2*

### 6.7.3. Analysis on KCA and CCA attack

This section explains the robustness of proposed work against KCA and CCA attack. In the known ciphertext attack, the attacker has the access merely to a set of ciphertexts yet has some knowledge of the plaintext. Under this analysis, it is reported that the implemented model is robust against the KCA attack. In this, the analysis is performed by varying the percentage of plaintext data and the outcomes are obtained, that are symbolized in Table 6.3. The proposed SLE-WOA algorithm, by varying the plaintext as 5% has proven its robustness against the KCA attack with less possibility of retrieving the original data.

Now, "a CCA is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key". In our work, the analysis is carried out by varying the percentage of ciphertext data and the outcomes obtained are given in Table 6.4. By varying the ciphertext to different percentage levels, the proposed model is proven for its efficiency over avoiding CCA attack.

*Table 6.3 Analysis on KCA attack: Proposed over Conventional Models*

| Varying the plaintext | WOA [170] | SLnO [169] | GA [174] | DA [175] | SLE-WOA |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| per_5 | 0.72171 | 0.94183 | 0.74796 | 0.81475 | 0.71012 |
| per_10 | 0.7862 | 0.95587 | 0.79836 | 0.80685 | 0.78312 |
| per_15 | 0.78387 | 0.95203 | 0.79205 | 0.80255 | 0.77692 |
| per_20 | 0.78532 | 0.94731 | 0.81127 | 0.80674 | 0.77895 |
| per_25 | 0.82122 | 0.9574 | 0.84862 | 0.83123 | 0.81308 |

*Table 6.4 Analysis on CCA attack: Proposed over Conventional Models*

| Varying the ciphertext | WOA [170] | SLnO [169] | GA [174] | DA [175] | SLE-WOA |
|---|---|---|---|---|---|
| per_5 | 0.74726 | 0.93655 | 0.82058 | 0.78959 | 0.71805 |
| per_10 | 0.77919 | 0.94739 | 0.82984 | 0.79913 | 0.73357 |
| per_15 | 0.83901 | 0.95472 | 0.86073 | 0.85565 | 0.78566 |
| per_20 | 0.86913 | 0.95923 | 0.87249 | 0.88676 | 0.8209 |
| per_25 | 0.87897 | 0.96325 | 0.87299 | 0.89539 | 0.85283 |

### 6.7.4. Analysis on KPA and CPA attacks

This section explains the robustness of proposed work against KPA and CPA attack. The ciphertext and its respective plaintext in known-plaintext attacks can be easily accessed by the attacker. The major goal is to predict the secret key (or the secret key count). Under this analysis, it is observed that the implemented approach is greatly robust against the KPA attack, as the attacker cannot gain the original data. From Table 6.5, it is observed that the attacker could access only 71% of original data and thus it failed in its attempt to get the original data. Similarly, during CPA, the attacker can decide the plaintext records randomly for encryption and based on that, achieves the respective ciphertext. He tried to purchase the secret key for encryption or alternatively generate an approach that might permit him to decrypt some ciphertext messages that are encrypted utilizing this key (with no detail about the secret key). Table 6.5 shows how the proposed algorithm is robust to CPA attack when compared to other conventional models. During this attack, only 70% of the original message is acquired by the attacker.

*Table 6.5 Analysis on KPA and CPA attack: Proposed and Conventional Models*

| | KPA | CPA |
|---|---|---|
| WOA [31] | 0.72171 | 0.77448 |
| SLnO [30] | 0.94183 | 0.9055 |
| GA [34] | 0.74796 | 0.73534 |
| DA [35] | 0.81475 | 0.75548 |
| SLE-WOA | 0.71012 | 0.71106 |

### 6.7.5. Key Sensitivity Analysis

In this section, the robustness of the sanitization key is investigated by varying the sanitization key to 5%, 10%, 15%, and 20%, respectively and attempted to recover the original data (Table 6.6). The resultant data is compared to the original data. While analyzing, it is observed that the implemented sanitization model can produce only 17% of original data with 10% of the key variation. However, the key with a variation of the conventional method has retrieved 40% of original data. A similar analysis is made for all the remaining variations. Table 6.6 shows the key sensitivity analysis.

*Table 6.6 Key sensitivity analysis*

| | WOA [170] | SLnO [169] | GA [174] | DA [175] | SLE-WOA |
|---|---|---|---|---|---|
| per_5 | 0.34343 | 0.3942 | 0.45439 | 0.47096 | 0.23084 |
| per_10 | 0.23832 | 0.41433 | 0.31735 | 0.4506 | 0.17537 |
| per_15 | 0.24754 | 0.41131 | 0.3149 | 0.43664 | 0.16612 |
| per_20 | 0.25011 | 0.37802 | 0.32338 | 0.41904 | 0.15964 |
| per_25 | 0.29927 | 0.40266 | 0.31205 | 0.40839 | 0.16066 |

### 6.7.6. Analysis of Classifier

The proposed work uses the NN model for predicting the trustability of nodes, and the performance of the classifier is analysed over other state-of-the-art methods like models SOM and GHSOM. In fact, the analysis is carried out under both positive and negative measures. From Table 6.7, it is observed that the prediction accuracy of NN is 92%, whereas the conventional methods show poor performance with less accuracy.

$$Accuracy = \frac{(TP + TN))}{(TP + TN + FP + FN)} \quad (27)$$

Similarly, the FPR by NN is least 0.08 when compared with other models, which shows that it is 16.33% and 15.1% superior to SOM and GHSOM, respectively. The performance evaluation formula is defined in Eq. (28).

$$perf\ \% = \frac{proposed - conventional}{conventional} \times 100 \quad (28)$$

*Table 6.7 Performance of NN Model in trustability Prediction*

| | SOM [172] | GHSOM [173] | NN [171] |
|---|---|---|---|
| Accuracy | 0.74576 | 0.89831 | 0.92308 |
| Sensitivity | 0.38889 | 0.85714 | 1 |
| Specificity | 0.90244 | 0.90385 | 0.91837 |
| Precision | 0.63636 | 0.54545 | 0.42857 |
| FPR | 0.097561 | 0.096154 | 0.081633 |
| FNR | 0.61111 | 0.14286 | 0 |
| NPV | 0.90244 | 0.90385 | 0.91837 |
| FDR | 0.36364 | 0.45455 | 0.57143 |
| F1_score | 0.48276 | 0.66667 | 0.6 |
| MCC | 0.34442 | 0.63185 | 0.62736 |

Further, the overall trustability prediction results in Table 6.8 show that, as the rule based and NN based models are combined to evaluate the trustability of node, the proposed trust management system is strong enough to control the malicious activity in the network, which is proven using certain positive and negative measures.

*Table 6.8 Overall Performance Analysis*

| | Rule-based | NN-based | Overall performance |
|---|---|---|---|
| Accuracy | 0.83051 | 0.92308 | 0.88136 |
| Sensitivity | 0.57143 | 1 | 0.7 |
| Specificity | 0.86538 | 0.91837 | 0.91837 |
| Precision | 0.36364 | 0.42857 | 0.63636 |
| FPR | 0.13462 | 0.081633 | 0.081633 |
| FNR | 0.42857 | 0 | 0.3 |
| NPV | 0.86538 | 0.91837 | 0.91837 |
| FDR | 0.63636 | 0.57143 | 0.36364 |
| F1_score | 0.44444 | 0.6 | 0.66667 |
| MCC | 0.36268 | 0.62736 | 0.5957 |

### 6.7.7. Representation of Key management in RSU via Blockchain technology

Figure 6.10-6.14 show how the optimal key generated by RSUs is stored in blocks. This shows the mobility of the vehicle at each time stamp and the key generation in each RSU (RSU 1, 2, and 3) for the requesting vehicle. Moreover, this section reveals how the generated optimal keys are maintained in each RSU through blocks (both proposed and conventional models).

| RSU 1 | |
|---|---|
| Key 5 | <4,1,1,3,5> |
| Key 4 | <1,3,6,3,5> |
| Key 3 | <2,5,1,7,7> |
| Key 2 | <4,6,3,1,1> |
| Key 1 | <3,5,5,3,1> |

| RSU 2 | |
|---|---|
| Key 13 | <1,1,7,6,3> |
| Key 12 | <4,3,2,3,9> |
| Key 11 | <1,5,1,7,3> |
| Key 10 | <1,7,8,1,1> |
| Key 9 | <3,8,1,1,6> |
| Key 8 | <6,2,7,1,1> |
| Key 7 | <5,2,1,7,6> |
| Key 6 | <3,3,2,1,5> |

| RSU 3 | |
|---|---|
| Key 19 | <2,3,3,3,1> |
| Key 18 | <1,3,2,4,3> |
| Key 17 | <4,2,1,4,7> |
| Key 16 | <1,3,3,6,4> |
| Key 15 | <2,1,9,4,7> |
| Key 14 | <3,1,5,4,4> |

*Figure 6.9 Optimal key generated by RSUs using WOA*

| RSU 1 | |
|---|---|
| Key 5 | <1,3,2,1,1> |
| Key 4 | <1,1,3,1,7> |
| Key 3 | <3,1,1,1,1> |
| Key 2 | <1,1,1,1,1> |
| Key 1 | <3,1,1,1,1> |

| RSU 2 | |
|---|---|
| Key 13 | <1,3,1,1,1> |
| Key 12 | <1,3,1,3,1> |
| Key 11 | <1,1,1,1,2> |
| Key 10 | <1,3,1,1,1> |
| Key 9 | <1,1,1,1,3> |
| Key 8 | <1,1,1,1,2> |
| Key 7 | <1,1,1,3,3> |
| Key 6 | <1,1,1,1,2> |

| RSU 3 | |
|---|---|
| Key 19 | <1,1,1,1,2> |
| Key 18 | <1,7,1,3,1> |
| Key 17 | <1,1,1,5,1> |
| Key 16 | <1,1,2,3,1> |
| Key 15 | <1,1,1,2,1> |
| Key 14 | <1,1,1,1,1> |

*Figure 6.10 Optimal key generated by RSUs using SLnO*

| RSU 1 | |
|---|---|
| Key 5 | <8,5,5,3,3> |
| Key 4 | <6,5,1,2,7> |
| Key 3 | <1,1,1,5,3> |
| Key 2 | <5,1,1,3,2> |
| Key 1 | <6,1,1,3,1> |

| RSU 2 | |
|---|---|
| Key 13 | <3,2,1,2,7> |
| Key 12 | <6,2,2,2,7> |
| Key 11 | <1,3,3,3,8> |
| Key 10 | <3,1,2,5,5> |
| Key 9 | <7,3,5,1,3> |
| Key 8 | <1,2,6,2,2> |
| Key 7 | <1,3,5,4,3> |
| Key 6 | <6,5,7,1,1> |

| RSU 3 | |
|---|---|
| Key 19 | <3,6,2,7,1> |
| Key 18 | <2,7,2,1,8> |
| Key 17 | <4,6,6,6,6> |
| Key 16 | <3,4,2,5,4> |
| Key 15 | <1,3,3,2,6> |
| Key 14 | <3,4,3,3,5 |

*Figure 6.11 Analysis on optimal key that is generated by RSUs using GA*

| RSU 1 | |
|---|---|
| Key 5 | <1,5,7,3,4> |
| Key 4 | <1,7,5,1,1> |
| Key 3 | <3,6,3,6,6> |
| Key 2 | <5,2,7,7,5> |
| Key 1 | <2,1,3,3,1> |

| RSU 2 | |
|---|---|
| Key 13 | <8,3,3,1,7> |
| Key 12 | <1,3,1,1,1> |
| Key 11 | <2,3,1,5,3> |
| Key 10 | <3,6,5,3,3> |
| Key 9 | <1,4,3,7,5> |
| Key 8 | <3,5,3,7,6> |
| Key 7 | <7,3,3,6,3> |
| Key 6 | <1,3,3,1,5> |

| RSU 3 | |
|---|---|
| Key 19 | <7,7,1,2,3> |
| Key 18 | <1,3,7,2,9> |
| Key 17 | <2,3,6,1,6> |
| Key 16 | <3,3,1,3,3> |
| Key 15 | <3,6,1,4,1> |
| Key 14 | <3,3,5,3,3> |

*Figure 6.12 Optimal key generated by RSUs using DA*

| RSU 1 | |
|---|---|
| Key 5 | <2,2,1,1,5> |
| Key 4 | <4,1,4,2,2> |
| Key 3 | <3,2,1,4,7> |
| Key 2 | <4,2,1,2,7> |
| Key 1 | <2,2,7,1,2> |

| RSU 2 | |
|---|---|
| Key 13 | <2,5,7,4,2> |
| Key 12 | <2,2,4,1,5> |
| Key 11 | <5,4,2,6,1> |
| Key 10 | <1,2,2,5,1> |
| Key 9 | <3,3,1,4,3> |
| Key 8 | <6,3,9,1,7> |
| Key 7 | <7,1,1,3,6> |
| Key 6 | <5,1,7,5,2> |

| RSU 3 | |
|---|---|
| Key 19 | <3,6,7,7,6> |
| Key 18 | <2,4,2,5,1> |
| Key 17 | <1,1,6,6,3> |
| Key 16 | <3,4,4,6,1> |
| Key 15 | <1,7,1,9,5> |
| Key 14 | <2,3,2,2,3> |

*Figure 6.13 Optimal keys generated by RSUs using Proposed SLE-WOA Algorithm*

## 6.8. Conclusion

The research focuses on developing a novel and efficient technique of mutual authentication, revocation, trust, and privacy in the VANET environment. In the first research work, we proposed a scheme that not just authenticates vehicles with reduced dependency on the trusted third party but also preserves their anonymity by not revealing the original identity of users. Despite reducing the communication overhead, the scheme serves to achieve statutory security requirements. It eliminates the need to circulate CRLs by the CA or RSUs, instead

mends the status of a vehicle's revocation flag to be true. In the next phase of our research, we evaluated the schemes providing trust in the nodes and the system claiming to provide credible reputation score. Limitations in the existent centralized PKI framework, as well as some of the decentralized works have been identified and as a result, a blockchain and smart contract-based solution is envisaged as the best solution. The framework provides decentralization, transparency, immutability and peer-to-peer availability and consistency of every user's reputation value. We evaluated the proposed scheme both from ordinary and alarming situation perspective. The nodes have their pseudo IDs obtained after registration, which provide privacy to some extent, but they do not prevent location tracking. In the next phase, we worked on identifying trustworthy nodes, with a combined approach using Machine Learning and Blockchain where we use an optimized key to sanitize data thus providing privacy and data is only shared with nodes fulfilling the classification of being a trustworthy node. This research work has introduced a novel trust management system in VANET with two main phases: Secured Message Transmission and Node Trustability Prediction. The security assured message passing incorporates the privacy preservation model under the Data Sanitization process. Furthermore, the optimization concept plays as a major role, in which the key utilized for the sanitization process is optimally tuned using a novel hybrid algorithm named SLE-WOA, which is the combination of WOA and SLnO algorithms. Subsequently, the trustability of the node is computed based on the "two-level evaluation process" i.e., rule based and machine learning-based evaluation process. The performance and authenticity of the proposed model is validated against other classical models considering multiple performance evaluation measures. The result thus analyzed is, that the proposed sanitization method with respect to the key sensitivity analysis can produce only 17% of original data with 10% of the key variation. However, the key with a variation of the conventional method has retrieved 40% of original data. This substantiates the proposed model, thus fulfilling the essential requirement of privacy-preserving secure message transmission with established trust management in the network.

# Chapter 7

# Conclusion and Future Work

*Vehicular Ad hoc Networks (VANET) are emerging as a promising technology of the Intelligent Transportation systems (ITS) due to its potential benefits for travel planning, notifying road hazards, cautioning of emergency scenarios, alleviating congestion, provisioning parking facilities and environmental predicaments. But the security threats hinder its wide deployment and acceptability by users. This thesis presented major components required to secure the dynamic vehicular Ad hoc networks. These components are discussed, implemented, and tested in the last three Chapters (Chapter 4 to Chapter 6) of this thesis. In this Chapter, we conclude our thesis by shedding light on the major contributions made and the expected research outcomes followed by a consideration of possible future works presented.*

## 7.1. Conclusions

With numerous VANET advantages, comes the security risks and disadvantages given the open nature of the vehicular communications. The security solutions require a centralized party to work as a trusted intermediary in establishing secure communication between the Road-Side Units (RSUs) and On-Board Units (OBUs). In this thesis, we study the major security requirements of VANET and understand the need of moving towards decentralization of the traditional VANET and reducing dependency on a centralized party to achieve the critical security requirements i.e. authentication and revocation, trust and reputation, secured transmission with access control and key management.

As discussed in previous Chapters, we proposed a security framework that reduces the dependency on the centralized party while rendering the primitive security requirements of VANET. This framework guarantees that the self-sustained and self-organized vehicular network allows not just for easy identification/authentication of the vehicles without any intermediary but also, establishes transparency in the computation of trust and reputation among the

communicating nodes, and ensures secured communication by restricting access to only reputed nodes.

Below is a summation of the proposed work.

The research focusses on developing a novel and efficient technique of mutual authentication, revocation, trust, privacy, and access control in the VANET environment.

In **Chapter 4**, first component of the scheme is proposed, which is authentication and revocation. This scheme not just authenticates vehicles with reduced dependency on the trusted third party but also preserves their anonymity by not revealing the original identity of users. Despite reducing the communication overhead, the scheme serves to achieve statutory security requirements. It eliminates the need to circulate CRLs by the CA or RSUs, instead mends the status of a vehicle's revocation flag to be true.

In **Chapter 5**, the trust and reputation component is discussed. The schemes providing trust in the nodes and the system claiming to provide credible reputation score are evaluated. Limitations in the existent centralized PKI framework, as well as some of the decentralized works have been identified and as a result, a blockchain and smart contract-based solution is envisaged as the best solution. The framework provides decentralization, transparency, immutability and peer-to-peer availability and consistency of every user's reputation value. The proposed scheme is evaluated both from ordinary and alarming situation perspective. The nodes have their pseudo IDs obtained after registration, which provide privacy to some extent, but they do not prevent location tracking.

In **Chapter 6**, Identification of trustworthy nodes, with a combined approach using Machine Learning and Blockchain is worked upon. Here, an optimized key is used to sanitize data, thus providing privacy. Data is only shared with nodes fulfilling the classification of being a trustworthy node. This research work has introduced a novel trust management system in VANET with two main phases: Secured Message Transmission and Node Trustability Prediction. The security assured message passing incorporates the privacy preservation model under the Data Sanitization process. Furthermore, the optimization concept plays as a major role, in which the key utilized for the sanitization process is optimally tuned using a novel hybrid algorithm named SLE-WOA, which is the combination of WOA and SLnO algorithms. Subsequently, the trustability of the node is computed based on the "two-level evaluation process" i.e., rule based and machine learning-based evaluation process. The performance and authenticity of the proposed model is validated against other classical models considering multiple performance evaluation measures. The result thus analyzed is, that the proposed sanitization method with respect to the key sensitivity analysis can produce only 17% of original data with 10% of the key variation. However, the key with a variation of the conventional method has retrieved 40% of original data. This

substantiates the proposed model, thus fulfilling the essential requirement of privacy-preserving secure message transmission with established trust management in the network.

## 7.2. Contributions to the ITS Field

The research proposes a blockchain based security framework for solving security challenges regarding vehicular communication in Intelligent Transport Systems (ITS).

1. It uses the distributed ledger technology (DLT), to enable easy verification of vehicles details by the RSUs and facilitate their authentication and quick revocation while travelling on road, without relying on the trusted authorities.
2. It uses IPFS storage and smart contracts for updating vehicle's reputation score after reception of emergency information from them and then analyzing it along with feedback from other neighboring vehicles regarding the same event. The decentralized IPFS storage transparently provides node's reputation scores to other nodes in real time manner without depending on a centralized party.
3. It ensures the protection against impersonation, sybil and replay attacks, thus providing authentication and quick revocation.
4. It ensures secured message transmission by providing data sanitization before transmission by using optimized keys and managing the keys using blockchain to easily supply them for desanitization. The blockchain storage ensures immutability and chronological storage of data.
5. It ensures accurate classification of nodes as trustworthy and malicious by making use of Machine Learning and thus providing access control by restricting message access to only trustworthy vehicles

This research concentrates on designing a blockchain based security service which can provide higher level of security in ITS while introducing a decentralized technique for protection against the above stated attacks.

## 7.3. Research Outcomes

Expected outcomes in relation to the research objectives as discussed in Chapter 1 are following:

This research delivers a blockchain based security solution to Intelligent Transport Systems. The solution relies on distributed ledger and smart contract technologies to provision security such as on-dynamic authentication, quick revocation, establishing trust in the source, maintaining message confidentiality and privacy, and the most important of all decentralization of the network.

We classified the research outcome as:

1. **Reduced CA dependency**
2. **Reduced overhead**
3. **Efficient validation before message forwarding**
4. **Minimal computation at OBU**
5. **Scalability**
6. **Source and message authentication**
7. **Conditional privacy preservation**
8. **Node classification- Trustworthy/Not-trustworthy**
9. **Transparency in reputation evaluation**
10. **Data Privacy and sanitization**

## 7.4. Future Works

Based on the work presented in this thesis, our main objective is to design and develop a new decentralized security framework for the VANET. As we address the major components of the network model, there are still other smaller components that require investigation. The possible areas where the research can be directed in the future are as below.

In the proposed framework pseudonyms are used to provide user privacy and protect against any kind of location tracking by intruders. While we use pseudo Ids to maintain user anonymity, the process of updating and renewing needs improvement.

We used distributed ledger for storing the pseudo Id which is used by the vehicles to identify themselves while they communicate on road, but unlike the bitcoin blockchain where each and every transaction by a user uses a different address/Id, we have used a single one, which is regularly updated but not very frequently which is important.

This is particularly to avoid any kind of location tracking. If users continue to use one pseudo id for a longer period, it becomes easier for intruders to track the movement of the node. The beacon and emergency messages transmitted from the node can be tracked down easily and malicious activities can be conducted after the location is disclosed.

We considered some standard blockchains, i.e. bitcoin and Ethereum, but we can consider the other blockchains such as Hyperledger and Stellar or Corda, as we have a private blockchain network in the VANET scenario.

We studied the different blockchains but have not considered each of their benefits with respect to our scheme. But it becomes essential to utilize the best blockchain to gain the maximum speed and performance with scalability.

Further improvements can be made by implementing and testing the proposed model in real-world scenario to obtain better performance and results.

# Bibliography


[1] A. Auer, S. Feese, S. Lockwood, and B. A. Hamilton, "History of intelligent transportation systems," United States. Department of Transportation. Intelligent Transportation ..., 2016.

[2] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," 2013.

[3] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Vehicular Communications,* vol. 13, pp. 1-12, 2018.

[4] C. Kalaiarasy and N. Sreenath, "An incentive-based co-operation motivating pseudonym changing strategy for privacy preservation in mixed zones in vehicular networks," *Journal of King Saud University-Computer and Information Sciences,* 2018.

[5] S. Oubabas, R. Aoudjit, J. J. Rodrigues, and S. Talbi, "Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme," *Vehicular Communications,* vol. 13, pp. 128-138, 2018.

[6] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561,* 2014.

[7] N. Malik, D. Puthal, and P. Nanda, "An overview of security challenges in vehicular ad-hoc networks," in *2017 International Conference on Information Technology (ICIT)*, 2017: IEEE, pp. 208-213.

[8] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine,* vol. 7, no. 2, pp. 18-21, 2018.

[9] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consumer Electronics Magazine,* vol. 7, no. 4, pp. 6-14, 2018.

[10] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 674-679.

[11] N. Malik, P. Nanda, X. He, and R. Liu, "Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2019: IEEE, pp. 34-41.

[12] N. Malik, P. Nanda, X. He, and R. P. Liu, "Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology," *Wireless Networks,* pp. 1-20, 2020.

[13] A. Festag, "Standards for vehicular communication—from IEEE 802.11 p to 5G," *e & i Elektrotechnik und Informationstechnik,* vol. 132, no. 7, pp. 409-416, 2015.

[14] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE,* vol. 99, no. 7, pp. 1162-1182, 2011.

[15] A. Festag, "Cooperative intelligent transport systems standards in Europe," *IEEE communications magazine,* vol. 52, no. 12, pp. 166-172, 2014.

[16] A. Intl, "Standard specification for telecommunications and information exchange between roadside and vehicle systems-5 GHz band Dedicated Short Range Communications (DSRC)," *Medium Access Control and Physical Layer specifications, E2213-03,* 2003.

[17] I. W. Group, "IEEE standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std,* vol. 802, no. 11, 2010.

[18] R. A. Uzcátegui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications magazine,* vol. 47, no. 5, pp. 126-133, 2009.

[19] D. B. Johnson and A. J. Menezes, "Elliptic curve DSA (ECDSA): an enhanced DSA," in *Proceedings of the 7th conference on USENIX Security Symposium*, 1998, vol. 7, pp. 13-23.

[20] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications,* vol. 37, pp. 380-392, 2014.

[21] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security,* vol. 15, no. 1, pp. 39-68, 2007.

[22] H. Lu and J. Li, "Privacy-preserving authentication schemes for vehicular ad hoc networks: a survey," *Wireless Communications and Mobile Computing,* vol. 16, no. 6, pp. 643-655, 2016.

[23] R. Baldessari *et al.*, "Car-2-car communication consortium-manifesto," 2007.

[24] S. Chen *et al.*, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Communications Standards Magazine,* vol. 1, no. 2, pp. 70-76, 2017.

[25] T. ETSI, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," *Tech. Rep. ETSI TR 102 6382009,* 2009.

[26] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems,* vol. 50, no. 4, pp. 217-241, 2012.

[27] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications,* vol. 1, no. 2, pp. 53-66, 2014.

[28] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*, 2002: Springer, pp. 251-260.

[29] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE wireless communications,* vol. 13, no. 5, pp. 8-15, 2006.

[30] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks," *IEEE Transactions on Wireless Communications,* vol. 8, no. 2, pp. 736-745, 2009.

[31] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV)*, 2005: Maryland, USA, pp. 1-6.

[32] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *2012 6th International Conference on Signal Processing and Communication Systems*, 2012: IEEE, pp. 1-9.

[33] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *European Wireless*, 2002, vol. 2.

[34] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy,* vol. 2, no. 3, pp. 49-55, 2004.

[35] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications,* vol. 44, pp. 1-13, 2014.

[36] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANET security challenges and solutions: A survey," *Vehicular Communications,* vol. 7, pp. 7-20, 2017.

[37] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology,* vol. 66, no. 4, pp. 3235-3248, 2015.

[38] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, 2007, pp. 19-28.

[39] I. Memon, Q. Ali, A. Zubedi, and F. A. Mangi, "DPMM: dynamic pseudonym-based multiple mix-zones generation for mobile traveler," *Multimedia Tools and Applications,* vol. 76, no. 22, pp. 24359-24388, 2017.

[40] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016: IEEE, pp. 2663-2668.

[41] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," *arXiv preprint arXiv:1704.02553,* 2017.

[42] Y. Lai, Y. Xu, F. Yang, W. Lu, and Q. Yu, "Privacy-aware query processing in vehicular ad-hoc networks," *Ad Hoc Networks,* vol. 91, p. 101876, 2019.

[43] I. A. Kamil and S. O. Ogundoyin, "A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5G smart grid slice," *Sustainable Energy, Grids and Networks,* vol. 20, p. 100260, 2019.

[44] M. A. Habib *et al.*, "Security and privacy based access control model for internet of connected vehicles," *Future Generation Computer Systems,* vol. 97, pp. 687-696, 2019.

[45] H. Xia, S.-s. Zhang, Y. Li, Z.-k. Pan, X. Peng, and X.-z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology,* vol. 68, no. 7, pp. 7108-7120, 2019.

[46] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized trust evaluation in vehicular Internet of Things," *IEEE Access,* vol. 7, pp. 15980-15988, 2019.

[47] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 1495-1505, 2018.

[48] M. Arshad *et al.*, "Beacon trust management system and fake data detection in vehicular ad-hoc networks," *IET Intelligent Transport Systems,* vol. 13, no. 5, pp. 780-788, 2018.

[49] J.-M. Chen, T.-T. Li, and J. Panneerselvam, "TMEC: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles," *IEEE Access,* vol. 7, pp. 148913-148922, 2018.

[50] N. Ullah, X. Kong, Z. Ning, A. Tolba, M. Alrashoud, and F. Xia, "Emergency warning messages dissemination in vehicular social networks: A trust based scheme," *Vehicular Communications,* vol. 22, p. 100199, 2020.

[51] Y. He, F. R. Yu, Z. Wei, and V. Leung, "Trust management for secure cognitive radio vehicular ad hoc networks," *Ad Hoc Networks,* vol. 86, pp. 154-165, 2019.

[52] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "Active vehicle: a new approach integrating AmI technology for trust management in VANET," *International Journal of High Performance Computing and Networking,* vol. 11, no. 4, pp. 291-303, 2018.

[53] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular Ad hoc Networks (VANETs)," *Computer Networks,* vol. 121, pp. 152-172, 2017.

[54] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of network and computer applications,* vol. 35, no. 3, pp. 934-941, 2012.

[55] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Vehicular Communications,* vol. 9, pp. 254-267, 2017.

[56] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access,* vol. 5, pp. 25408-25420, 2017.

[57] J. Wang, Y. Zhang, Y. Wang, and X. Gu, "RPRep: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs," *International Journal of Distributed Sensor Networks,* vol. 12, no. 3, p. 6138251, 2016.

[58] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Communications Magazine,* vol. 53, no. 8, pp. 42-47, 2015.

[59] A. VishwaVidyapeetham, "A Blockchain and IPFS based framework for secure research record keeping," *International Journal of Pure and Applied Mathematics,* vol. 119, no. 15, pp. 1437-1442, 2018.

[60] N. Fan and C. Q. Wu, "On trust models for communication security in vehicular ad-hoc networks," *Ad Hoc Networks,* vol. 90, p. 101740, 2019.

[61] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers & Electrical Engineering,* vol. 40, no. 6, pp. 1981-1996, 2014.

[62] X. Li, J. Liu, X. Li, and H. Li, "A reputation-based secure scheme in vehicular ad hoc networks," *International Journal of Grid and Utility Computing,* vol. 6, no. 2, pp. 83-90, 2015.

[63] P. T. N. Diep and C. K. Yeo, "A trust-privacy framework in vehicular ad hoc networks (VANET)," in *2016 Wireless Telecommunications Symposium (WTS)*, 2016: IEEE, pp. 1-7.

[64] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications,* vol. 7, no. 3, pp. 229-242, 2014.

[65] J. Zhang, C. Chen, and R. Cohen, "A Scalable and Effective Trust-Based Framework for Vehicular Ad-Hoc Networks," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.,* vol. 1, no. 4, pp. 3-15, 2010.

[66] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks," *Ad Hoc Networks,* vol. 37, pp. 122-132, 2016.

[67] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Computer Communications,* vol. 71, pp. 50-60, 2015.

[68] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Computer Networks,* vol. 134, pp. 78-92, 2018.

[69] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for VANETs," in *2010 10th IEEE International Conference on Computer and Information Technology*, 2010: IEEE, pp. 832-837.

[70] J. Cui, W. Xu, Y. Han, J. Zhang, and H. Zhong, "Secure mutual authentication with privacy preservation in vehicular ad hoc networks," *Vehicular Communications,* vol. 21, p. 100200, 2020.

[71] A. Ltifi, A. Zouinkhi, and M. S. Bouhlel, "Trust-based scheme for alert spreading in VANET," *Procedia Comput. Sci,* vol. 73, pp. 282-289, 2015.

[72] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation management in vehicular ad hoc networks," in *2010 International Conference on Multimedia Technology*, 2010: IEEE, pp. 1-5.

[73] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Securing vehicular networks: a reputation and plausibility checks-based approach," in *2010 IEEE Globecom Workshops*, 2010: IEEE, pp. 1550-1554.

[74] O. Abumansoor and A. Boukerche, "Towards a secure trust model for vehicular ad hoc networks services," in *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, 2011: IEEE, pp. 1-5.

[75] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers & Electrical Engineering,* vol. 43, pp. 33-47, 2015.

[76] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "PPREM: privacy preserving REvocation mechanism for vehicular ad hoc networks," *Computer Standards & Interfaces,* vol. 36, no. 3, pp. 513-523, 2014.

[77] L.-Y. Yeh, Y.-C. Chen, and J.-L. Huang, "PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks," *Computer Communications,* vol. 34, no. 3, pp. 447-456, 2011.

[78] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *IFIP international conference on distributed applications and interoperable systems*, 2017: Springer, pp. 206-220.

[79] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access,* vol. 6, pp. 45655-45664, 2018.

[80] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "Bars: a blockchain-based anonymous reputation system for trust management in VANETs," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018: IEEE, pp. 98-103.

[81] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018: IEEE, pp. 1499-1506.

[82] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital Communications and Networks,* vol. 6, no. 2, pp. 177-186, 2020.

[83] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, 2018: IEEE, pp. 161-166.

[84] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 4660-4670, 2018.

[85] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *IFIP International Conference on ICT Systems Security and Privacy Protection*, 2016: Springer, pp. 398-411.

[86] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 6, pp. 949-962, 2013.

[87] O. Hasan, L. Brunie, and E. Bertino, "Preserving privacy of feedback providers in decentralized reputation systems," *Computers & Security,* vol. 31, no. 7, pp. 816-826, 2012.

[88] S. Tangade and S. S. Manvi, "Trust management scheme in VANET: Neighbour communication based approach," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 2017: IEEE, pp. 741-744.

[89] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence Theory and Practice,* vol. 5, 2010.

[90] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE systems journal,* vol. 8, no. 3, pp. 749-758, 2013.

[91] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *2006 3rd Annual International Conference on Mobile and Ubiquitous Systems-Workshops*, 2006: IEEE, pp. 1-8.

[92] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016: IEEE, pp. 1050-1055.

[93] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 17, no. 4, pp. 960-969, 2015.

[94] R. Kaur, T. P. Singh, and V. Khajuria, "Security issues in vehicular ad-hoc network (VANET)," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018: IEEE, pp. 884-889.

[95] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking,* vol. 2009, no. 1, p. 125348, 2009.

[96] W. Liang, J. Long, T.-H. Weng, X. Chen, K.-C. Li, and A. Y. Zomaya, "TBRS: A trust based recommendation scheme for vehicular CPS network," *Future Generation Computer Systems,* vol. 92, pp. 383-398, 2019.

[97] N. Yang, "A similarity based trust and reputation management framework for VANETs," *International Journal of Future Generation Communication and Networking,* vol. 6, no. 2, pp. 25-34, 2013.

[98] H. Xia, S.-s. Zhang, B.-x. Li, L. Li, and X.-g. Cheng, "Towards a novel trust-based multicast routing for VANETs," *Security and Communication Networks,* vol. 2018, 2018.

[99] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 1-6.

[100] M. C. Ramon and D. A. Zajac, "Cybersecurity Literature Review and Efforts Report," *Prepared for NCHRP Project,* pp. 03-127, 2018.

[101] J. Zhang, "A survey on trust management for VANETs," in *2011 IEEE International Conference on Advanced Information Networking and Applications*, 2011: IEEE, pp. 105-112.

[102] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 11-21.

[103] P.-W. Yau and C. J. Mitchell, "Security vulnerabilities in ad hoc networks," in *Proceedings of the 7th International Symposium on Communication Theory and Applications*, 2003, pp. 99-104.

[104] S. Buchegger and J. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," 2003.

[105] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Computer Networks,* vol. 145, pp. 219-231, 2018.

[106] Z. Yang, K. Zheng, K. Yang, and V. C. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, 2017: IEEE, pp. 1-5.

[107] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats [future directions]," *IEEE Consumer Electronics Magazine,* vol. 6, no. 4, pp. 24-27, 2017.

[108] R. Grinberg, "Bitcoin: An innovative alternative digital currency," *Hastings Sci. & Tech. LJ,* vol. 4, p. 159, 2012.

[109] C. Mohan, "Blockchains and databases: A new era in distributed computing," in *2018 IEEE 34th International Conference on Data Engineering (ICDE)*, 2018: IEEE, pp. 1739-1740.

[110] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering,* vol. 30, no. 7, pp. 1366-1385, 2018.

[111] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems,* vol. 107, pp. 841-853, 2020.

[112] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—how to make bitcoin a better currency," in *International conference on financial cryptography and data security*, 2012: Springer, pp. 399-414.

[113] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, 2019.

[114] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017: IEEE, pp. 557-564.

[115] V. Buterin, "A Next Generation Smart Contract & Decentralized Application Platform (2013) Whitepaper," *Ethereum Foundation*.

[116] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 906-917.

[117] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, 2015: IEEE, pp. 104-121.

[118] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 203-226.

[119] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *OSDI*, 1999, vol. 99, no. 1999, pp. 173-186.

[120] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, "Performance analysis of hyperledger fabric platforms," *Security and Communication Networks,* vol. 2018, 2018.

[121] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1085-1100.

[122] N. H. T. S. Administration, "US department of transportation," *Motor Vehicle Safety Standard,* no. 208, pp. 74-14, 1999.

[123] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *European Workshop on Security in Ad-hoc and Sensor Networks*, 2007: Springer, pp. 129-141.

[124] L. Zhu, C. Chen, X. Wang, and A. O. Lim, "SMSS: Symmetric-masquerade security scheme for VANETs," in *2011 Tenth International Symposium on Autonomous Decentralized Systems*, 2011: IEEE, pp. 617-622.

[125] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in edge-of-things," *Future Generation Computer Systems,* vol. 85, pp. 190-200, 2018.

[126] D. Puthal, "Lattice-modeled information flow control of big sensing data streams for smart health application," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 1312-1320, 2018.

[127] K. Gai and M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," *IEEE Transactions on Industrial Informatics,* vol. 14, no. 8, pp. 3590-3598, 2017.

[128] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal,* vol. 4, no. 6, pp. 1832-1843, 2017.

[129] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications,* vol. 4, pp. 30-37, 2016.

[130] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms-ideal and real," in *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*, 2007: IEEE, pp. 2521-2525.

[131] Q. G. K. Safi, S. Luo, C. Wei, L. Pan, and G. Yan, "Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs," *Computer standards & interfaces,* vol. 56, pp. 107-115, 2018.

[132] Y. J. Li, "An overview of the DSRC/WAVE technology," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, 2010: Springer, pp. 544-558.

[133] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *Journal of Financial Perspectives,* vol. 3, no. 3, 2015.

[134] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications,* vol. 10, no. 4, pp. 983-994, 2017.

[135] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International workshop on open problems in network security*, 2015: Springer, pp. 112-125.

[136] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*, 2016: IEEE, pp. 839-858.

[137] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in *International conference on financial cryptography and data security*, 2016: Springer, pp. 79-94.

[138] M. Pilkington, "Blockchain technology: principles and applications," in *Research handbook on digital transformations*: Edward Elgar Publishing, 2016.

[139] N. Kshetri, "Can blockchain strengthen the internet of things?," *IT professional,* vol. 19, no. 4, pp. 68-72, 2017.

[140] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access,* vol. 4, pp. 2292-2303, 2016.

[141] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine,* vol. 55, no. 12, pp. 119-125, 2017.

[142] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 2017: IEEE, pp. 618-623.

[143] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016, pp. 1-10.

[144] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems,* vol. 20, no. 2, pp. 760-776, 2018.

[145] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things,* vol. 1, pp. 1-13, 2018.

[146] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255-265.

[147] A. Kumar and M. Gupta, "A review on activities of fifth generation mobile communication system," *Alexandria Engineering Journal,* vol. 57, no. 2, pp. 1125-1135, 2018.

[148] A. Mukherjee and D. De, "Femtolet: A novel fifth generation network device for green mobile cloud computing," *Simulation Modelling Practice and Theory,* vol. 62, pp. 68-87, 2016.

[149] C. Feijóo, J. L. Gómez-Barroso, and S. Ramos, "Techno-economic implications of the mass-market uptake of mobile data services: Requirements for next generation mobile networks," *Telematics and Informatics,* vol. 33, no. 2, pp. 600-612, 2016.

[150] A. Habbal, S. I. Goudar, and S. Hassan, "A Context-aware Radio Access Technology selection mechanism in 5G mobile network for smart city applications," *Journal of Network and Computer Applications,* vol. 135, pp. 97-107, 2019.

[151] W. Benrhaiem and A. S. Hafid, "Bayesian networks based reliable broadcast in vehicular networks," *Vehicular Communications,* vol. 21, p. 100181, 2020.

[152] O. Urra and S. Ilarri, "Spatial crowdsourcing with mobile agents in vehicular networks," *Vehicular Communications,* vol. 17, pp. 10-34, 2019.

[153] R. A. Osman, X.-H. Peng, and M. Omar, "Adaptive cooperative communications for enhancing QoS in vehicular networks," *Physical Communication,* vol. 34, pp. 285-294, 2019.

[154] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," *Future Generation Computer Systems,* vol. 101, pp. 843-864, 2019.

[155] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Misbehavior detection and efficient revocation within VANET," *Journal of Information Security and Applications,* vol. 46, pp. 193-209, 2019.

[156] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications,* vol. 19, p. 100179, 2019.

[157] J. Kang, D. Lin, W. Jiang, and E. Bertino, "Highly efficient randomized authentication in VANETs," *Pervasive and Mobile Computing,* vol. 44, pp. 31-44, 2018.

[158] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *cognitive systems research,* vol. 55, pp. 153-163, 2019.

[159] P. Cirne, A. Zúquete, and S. Sargento, "TROPHY: Trustworthy VANET routing with group authentication keys," *Ad Hoc Networks,* vol. 71, pp. 45-67, 2018.

[160] J. Zhao, Z. Wu, Y. Wang, and X. Ma, "Adaptive optimization of QoS constraint transmission capacity of VANET," *Vehicular Communications,* vol. 17, pp. 1-9, 2019.

[161] A. Debnath, H. Basumatary, A. Tarafdar, M. K. DebBarma, and B. K. Bhattacharyya, "Center of mass and junction based data routing method to increase the QoS in VANET," *AEU-International Journal of Electronics and Communications,* vol. 108, pp. 36-44, 2019.

[162] P. P. Jadhav and S. D. Joshi, "WOADF: Whale optimization integrated adaptive dragonfly algorithm enabled with the TDD properties for model transformation," *International Journal of Computational Intelligence and Applications,* vol. 18, no. 04, p. 1950026, 2019.

[163] K. Revathi and N. Krishnamoorthy, "The performance analysis of swallow swarm optimization algorithm," in *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015: IEEE, pp. 558-562.

[164] R. Remmiya and C. Abisha, "Artifacts removal in EEG signal using a NARX model based CS learning algorithm," *Multimedia Research,* vol. 1, no. 1, pp. 1-8, 2018.

[165] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing,* vol. 75, pp. 712-727, 2019.

[166] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *Journal of Systems Architecture,* vol. 99, p. 101636, 2019.

[167] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET," *Wireless Networks,* vol. 25, no. 8, pp. 4639-4661, 2019.

[168] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer-to-Peer Networking and Applications,* vol. 12, no. 5, pp. 1178-1193, 2019.

[169] R. Masadeh, B. A. Mahafzah, and A. Sharieh, "Sea Lion optimization algorithm," *Sea,* vol. 10, no. 5, 2019.

[170] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Advances in engineering software,* vol. 95, pp. 51-67, 2016.

[171] Y. Mohan, S. S. Chee, D. K. P. Xin, and L. P. Foong, "Artificial neural network for classification of depressive and normal in EEG," in *2016 IEEE EMBS conference on biomedical engineering and sciences (IECBES)*, 2016: IEEE, pp. 286-290.

[172] C.-C. Hsu, S.-H. Lin, and W.-S. Tai, "Apply extended self-organizing map to cluster and classify mixed-type data," *Neurocomputing,* vol. 74, no. 18, pp. 3832-3842, 2011.

[173] W.-S. Tai and C.-C. Hsu, "Growing Self-Organizing Map with cross insert for mixed-type data clustering," *Applied Soft Computing,* vol. 12, no. 9, pp. 2856-2866, 2012.

[174] J. McCall, "Genetic algorithms for modelling and optimisation," *Journal of computational and Applied Mathematics,* vol. 184, no. 1, pp. 205-222, 2005.

[175] M. Jafari and M. H. B. Chaleshtari, "Using dragonfly algorithm for optimization of orthotropic infinite plates with a quasi-triangular cut-out," *European Journal of Mechanics-A/Solids,* vol. 66, pp. 1-14, 2017.