Journal of Ubiquitous Computing and Communication Technologies (ISSN: 2582-337X)
www.irojournals.com/jucct/

Self-Healing Blockchain Mesh (SHBM): A Secure and Autonomous Cyberattack Prevention System for Vehicles

Sathyabama A R.[1], Jeevaa Katiravan[2], Kanishka S.[3], Lavanya H.[4]

[1]Assistant Professor, [2]Professor, [3, 4]Student, Information Technology, Velammal Engineering College, Chennai, Tamil Nadu, India

E-mail: [1]sathya.it1@gmail.com, [2]Jeevaakatir@gmail.com, [3]kanishkaskumar2004@gmail.com, [4]lavny27@gmail.com

Abstract

Developing autonomous vehicles improve transportation by reducing human involvement and traffic management. Autonomous vehicles depend on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications for transmitting real-time data such as speed, braking position and road conditions. It handles major cyberattacks such as modified communications, data spoofing, denial of service attacks and unauthorized access that cause accidents, traffic congestion and safety risks. The previous work focuses on cloud servers, roadside devices and delayed response time to privacy attacks. The proposed study develops a decentralized cybersecurity framework for autonomous vehicles to handle these challenges. In this work, each autonomous vehicle will be connected to a smart node on a blockchain-based mesh network allows authorized communication without the need for centralized control. The blockchain ensures data integrity, transparency and authenticity by using permanent records, digital communications and cryptographic keys for modifications. This study contains a self-healing methodology for detecting problems, disconnecting damaged cars and an automated repair mechanism. The results suggest that SHBM improves centralized architectures for future smart transportation systems in terms of attack detection, recovery time, scalability, reliability and road safety.

DOI: https://doi.org/10.36548/jucct.2026.1.004
Received: 24.12.2025, received in revised form: 29.01.2026, accepted: 16.02.2026, published: 28.02.2026

Keywords: AVs, Cybersecurity, Blockchain, V2V, Self-healing, Decentralized architectures, Intelligent Transport systems, Isolation Forest, Long Short Term Memory (LSTM).

1. Introduction

Autonomous vehicles (AVs) are dependent on sustained Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication makes secure driving in real-time. The communications will help vehicles by sharing the data about the speed, position, road dangers and traffic conditions. However, when AVs are connected, more vulnerable systems are attacked. One hacked vehicle can transmit incorrect data, interrupt traffic and could lead to massive collisions. Traditional security solutions utilize cloud servers or roadside devices are lack of data resulting in delayed responses and vulnerable to online attacks. In order to handle these issues, the proposed Self-Healing Blockchain Mesh (SHBM) is presented as a decentralized, secure and smart communication model suitable for autonomous transportation networks.

The Self-Healing can be defined as the ability of the network to automatically identify a vehicle in a compromised condition, effectively remove V2V communication and return to normal operations within a predetermined recovery period without the intervention of a human operator. SHBM integrates the blockchain technology, mesh networking and dynamic cryptographic key cycling provides a secured, low-latency and highly robust communication mesh network. In SHBM, the automobiles develop a distributed mesh network allows each node (vehicle) to connect directly with other nodes without utilizing a central server. The combined blockchain record validates all message transfers, ensures that no incorrect and damaged data can be transmitted into the network.

The system will also facilitate advanced capabilities like in the case of a cyberattack, the system will rapidly identify abnormal behavior, isolate a compromised vehicle and activate self-healing recovery will restore safe vehicle operation within a time. The system also supports a multi-vehicle attack handling ability, auto creation of an emergency-free zone and a real-time security dashboard alert vehicles and authorities on the level of threats. SUMO simulation and real-time visual evaluation with OpenCV prove that the system is effective in the real-life traffic conditions, allowing more reliable and safer transportation networks which are scalable and can be used in the future.

1.1 The Evolution of Autonomous Vehicle Security

Now, the cybersecurity is used in autonomous vehicles as an advanced method. In early AVs had independent control systems with low connection which reduced their exposure. Secured real-time communication and decentralized safety were in high demand after AVs were introduced to support collaborative driving and business engineering. For beginners, security included authentication and encryption. The autonomous vehicle (AV) system proposed in the modern world should be able to recover rapidly on their own and include decentralized architectures in addition to provide real-time intrusion detection functions. The Intelligent Transportation Systems (ITS) has increased the efficiency of driving and the safety, but the enhanced connectivity added complexity and susceptibility to cyberattacks for AV networks. The growth of similar challenges is used by massive hacking attacks similar as the remote Jeep Cherokee breach and the Tesla autopilot exploit. As a result, experimenters are currently investigating into security results using AI.

1.2 Autonomous Vehicle Cybersecurity Challenges

The lack of operation indicates that the most effective systems focus on detecting problems but are unable to prevent or solve problems when they develop. Errors in a standard design frequently fail due to difficulties in central control. V2V communication is challenging because it is impossible to verify data transfers in a decentralized and inconsistent method. Insufficient response to violations and the constant change of current procedures, increases the probability of crashes as a result of violations. Privacy attacks in large data transfers should be protected and verified to help against the spread of fake data. Scalability issues in traditional architectures are unable to handle the increasing demands of bigger antiviral networks. Legal and storage limits may be difficult to secure individual data in compliance with changing requirements. The following concerns highlight the significance of using decentralized, self-healing security mechanisms to safeguard AV networks.

1.3 Secure AV Communication Using Blockchain-Based Solutions

The application of blockchain enables the following features to increase the security of AVs:

- Secure V2V Communication to prevent unwanted variability, transactions are stored in non-modifiable and digitally connected formats.
- Decentralized Anomaly Discovery AVs may detect risks that are part of the AV network without the need for central systems.
- Rapid Self-Healing with the help of recorded data on the blockchain allows it simple to conduct tests and follow rules for people with authorization may communicate.

1.4 Proposed SHBM Framework

SHBM develops an autonomous cybersecurity solution to minimize cyberattacks using blockchain, self-healing algorithms and real-time V2V security. The major steps are:

- **Normal Operation:** AVs employ blockchain-based V2V communication to securely communicate position, speed, and status data [1].
- **Cyberattack Detection:** When anomalous behavior is seen, the compromised antivirus software is automatically recognized.
- **Rerouting and Isolation:** The antivirus software has been introduced to avoid a crash and the attacked vehicle has been securely transferred to a safe lane.
- **Self-Healing:** The antivirus requires to be alerted. It utilized blockchain to communicate regarding the attack. So, the self-healing process will make the vehicle to securely run on the lane.

2. Literature Survey

The below table 1 includes a systematic literature review of current research publications to summarize them by providing primary focus, methodology and application domain made the proposed study of secure and self-healing vehicular network systems.

Table 1. Systematic Review of Research Works

Ref. No	Author(s) / Year	Primary Focus Area	Methodology / Technology	Key Contribution	Application Domain
2	Kusari et al., 2021	Autonomous Vehicle Testing	SUMO simulator enhancement	Improves simulation-based testing and validation	AV simulation & validation

3	Kurva, 2025	Data Integrity	Blockchain	Ensures secure and tamper-proof AV data	AV cybersecurity
4	Mugundh, 2025	Network Security	Deep Learning, DDoS Detection	Detects DDoS attacks in 6G AV networks	AV network security
5	Ming et al., 2021	Path Planning	Survey of algorithms	Comprehensive taxonomy of AV path planning	Autonomous navigation
6	Javaid et al., 2016	Intrusion Detection	Deep Learning	DL-based NIDS framework	Network security
7	Khaledian, 2020	Anomaly Detection	Stacked Learning	Ensemble-based anomaly detection approach	Cybersecurity
8	Avnet, 2025	V2V Communication	Communication overview	Explains V2V architecture and benefits	Connected vehicles
9	Yahoo Finance, 2022	Market Analysis	Industry report	Market trends and growth of V2V	Automotive industry
10	Logistics Viewpoints, 2025	Freight & Safety	V2V Communication	Role of V2V in logistics and safety	Transportation & logistics
11	Ye & Li, 2017	Resource Allocation	Deep Reinforcement Learning	DRL-based V2V resource allocation	Wireless V2V networks
12	Sun et al., 2015	Low-Latency V2V	D2D Communication	Reliability-aware V2V communication	Vehicular networks
13	Li et al., 2021	Cooperative Localization	V2V-assisted localization	Improves vehicle positioning accuracy	Connected vehicles
14	Kousaridas et al., 2021	V2X Infrastructure	5G & Edge Computing	Enables low-latency V2X services	Smart transportation
15	Smith, 2017	Traffic Optimization	Autonomous driving concept	Single AV mitigating traffic jams	Traffic management
16	Chandola et al., 2009	Anomaly Detection	Survey	Foundational taxonomy and methods	Data mining & security
17	Kumar & Sharma, 2014	V2V Communication	ZigBee Protocol	Low-cost V2V communication model	Vehicular communication

18	Hartenstein & Laberteaux, 2008	VANETs	Tutorial survey	Foundational VANET concepts	Vehicular networking
19	Zhang et al., 2020	Cellular V2X	Deep Reinforcement Learning	Mode selection & resource allocation	C-V2X systems
20	Ray et al., 2024	5G V2V Systems	mmWave at 28 GHz	Real-world 5G V2V system realization	Smart vehicles
21	Zhang et al., 2025	Vehicle Platooni	Event-triggered control	Cooperative tracking under delay	Platoon control
22	Mande Ramachandran, 20	6G V Challenges	Survey	Identifies issues in future V2X	Future vehicular networks
23	Su et al., 2022	Content Distribution	Joint V2I–V2V Scheduling	Efficient mmWave content delivery	Vehicular networks

3. Proposed System

The proposed technique will protect autonomous vehicles from cyber threats using V2V communication and blockchain recovery. There are automobiles in the model at different speeds and share data with each other. When the automobile is hacked (for example, by changing the speed or lane), it becomes red and continues flashing. A combination of Random Forest and LSTM is utilized to identify anomalies. When nearby automobiles are detected, they turn orange and reduce their speeds in order to avoid collisions. The compromised vehicle is transferred to the side road. The vehicle's original and unmodified data are preserved on a decentralized blockchain network. This data is securely collected using the Smart Automobile Contract Algorithm, and the automobile becomes stable using the proposed work. When the automobile is found, it becomes green and continues to run. The blockchain keeps track of everything that occurs. SHBM provides real-time detection, safe rerouting, rapid recovery and secure V2V communication to prevent accidents and increase trust. Figure 1 shows the proposed architecture incorporates real-time detection, distributed ledger and recovery modules to achieve autonomous vehicle communication security. Figure 2 represents the flow diagram of the proposed work.

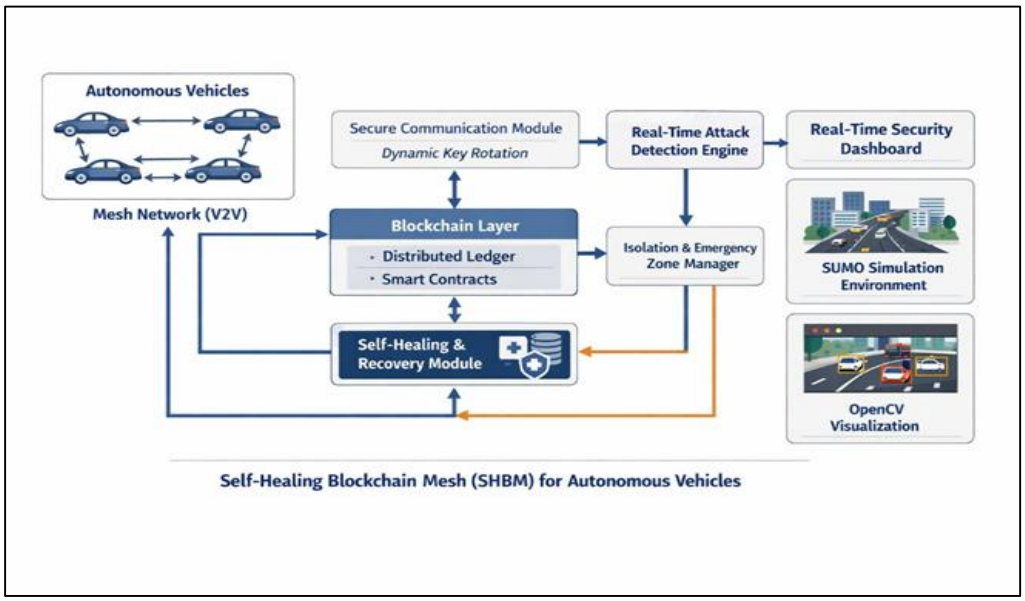

Figure 1. Self-Healing Blockchain Mesh (SHBM) Architecture

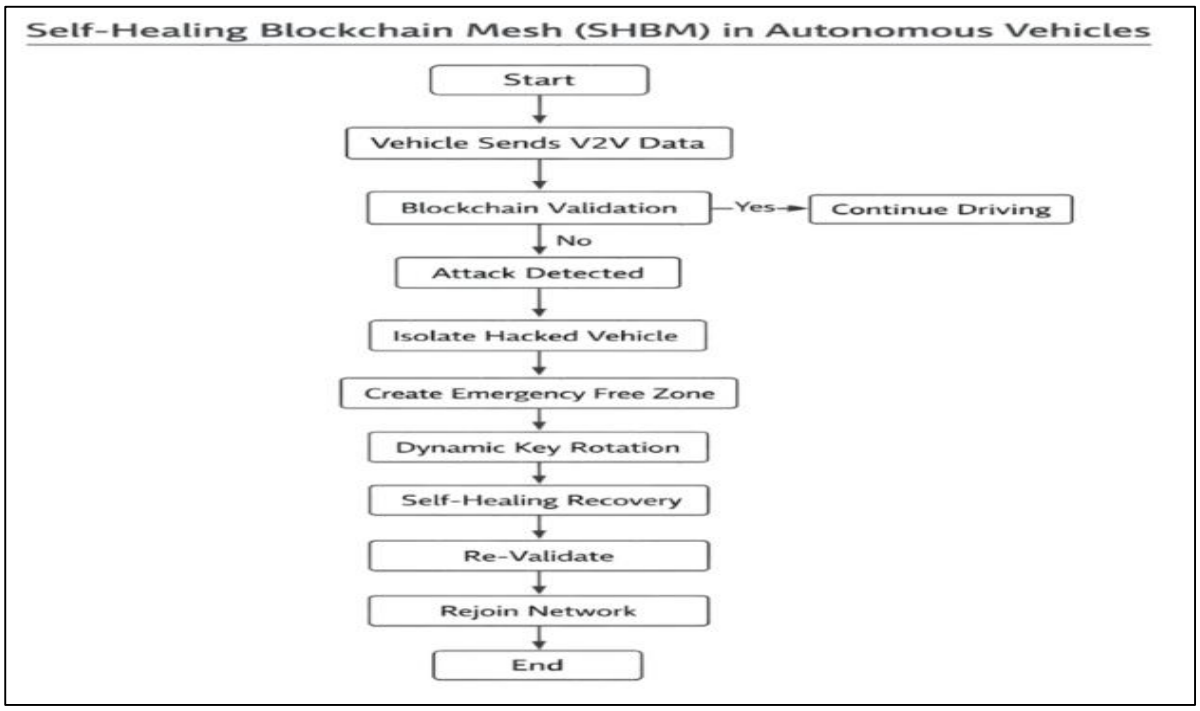

Figure 2. Flow Diagram of Proposed Work

3.2 Dataset

The data set that will be used in this study includes real-world car hacking data and simulated car communication data. The data set will be suitable for the purpose of detecting anomalies, securing blockchain transactions and smart rerouting algorithms. The dataset

consists of N_a attack samples and N_n normal samples. The attack samples constituting spoofing, replay and injection attacks where the normal samples constitute normal vehicle communications. Feature normalization and temporal alignment were applied to handle the domain change between real-world and simulated data and anomaly detection models were trained on a combined dataset to improve generalization between heterogeneous data sources.

3.2.1 Car-Hacking Dataset (OCS Lab)

In the dataset, vehicle network activity is reported in the form of a time-series function:

$$A_{vi}(t) = \{ p_1(t), p_2(t), p_3(t),\ldots,p_m(t)\} \quad (1)$$

In eq (1) where pm represents network packets. When anomaly A* is determined

$$\sum^{M} P_m > T \quad (2)$$

In eq (2) where τ is the threshold, the vehicle is flagged as compromised

3.2.2 Blockchain Event Logs

Each equation (3) block bi in the blockchain contains transactions T:

$$B = \{\beta_1, \beta_2,\ldots,\beta_n\}\ T_{\beta i} = \{t_1, t_2, \ldots t_m\} \quad (3)$$

For a valid transaction:

$$H_n = \text{Hash}(\text{Data}_n \parallel H_{n-1}) \quad (4)$$

In eq (4) where Hn= current block hash, Dn= transaction data of current block, H n-1= hash of previous block, Hash() = secure cryptographic hash function,‖ = concatenation operator.

3.3 Mathematical Algorithms

3.3.1 Smart Car Rerouting Algorithm

The safest route R is computed as:

$$R = \arg\min \sum_{i=1}^{N} C(v_i) \quad (5)$$

In SUMO, the congestion cost C(vi) is determined as a weighted sum of vehicle density, average reduction in speed, and queue length at node v_i and is observed to represent the real-time level of congestion. In eq (5) where $C(v_i)$ represents the congestion cost, ensuring:

$$\forall v_i , v_j \in R, d(v_i , v_j) \geq d_{min} \quad (6)$$

In eq (6) where d_{min} is the minimum safe distance.

3.3.2 Smart Car Decision-Making Algorithm

The decision function D(t) at time t is:

$$D(t) = \begin{cases} \text{Change Lane, if } S \leq S^{th} \text{ and } C < C^{th} \\ \text{Continue, if } S > S^{th} \text{ and } C < C^{th} \\ \text{Stop, if } C \geq C^{th} \end{cases} \quad (7)$$

In eq (7) where S is speed, S^{th} is the threshold speed, and C^{th} is the congestion threshold.

3.3.3 Anomaly Detection using Isolation Forest and LSTM

The Isolation Forest model scores each data point:

$$S(x_i) = \sum_{i=1}^{T} h_i (x_i) / c(n) \quad (8)$$

In eq (8) where $h_t(x_i)$ is the path length in the isolation tree, and c(n) is the average path length. Anomalies satisfy

$$S(x_i) < \lambda \quad (9)$$

Selection and tuning of threshold values were done manually by validation data and based on tuning by repeated simulations in order to achieve a compromise between detection accuracy and false alarm rates. In eq (9) where λ is the anomaly threshold.

3.3.4 Hacked Vehicle Detection

The model of a combined anomaly and cryptographic consistency is used to determine the hacked state of a vehicle. Based on Section 3.2.1, the vehicle communication at time t is defined as follows:

$$A_{vi}(t) = (p_1 , p_2 , p_3,....,p_m)$$

With the Isolation Forest and LSTM models (Eq. 8- 9), an anomaly score $S(x_i)$ is computed. A vehicle is considered anomalous in case:

$$S(x_i) < \lambda$$

Besides, the threshold condition is used to check the presence of a packet abnormality:

$$\sum_{m=1}^{M} P_m > \tau$$

A binary hacking state is necessary to have a formally defined hacked vehicle

$$H_i = \begin{cases} 1, \text{ if } S(x_i) < \lambda \ \wedge \ \sum P_m > \tau \wedge K_{recv} \neq K_{exp} \\ 0, \text{ otherwise} \end{cases} \quad (10)$$

If $H_i=1$, the car is considered as hacked and withdrawn instantly out of the V2V connection.

3.3.5 Blockchain Security Mechanism

Using Elliptic Curve Digital Signature Algorithm (ECDSA):

$$P = dG \quad (11)$$

To guarantee low latency and security, the blockchain uses a lightweight Proof-of-Authority consensus mechanism with fixed block generation time, with a fixed set of predefined validators, and trusted and reliable nodes of the vehicular infrastructure as validators. In eq (11) where P is the public key, d is the private key, and G is the generator point. Transactions are signed as:

$S = (r, s) = (H(T) + d \cdot r)\ mod\ n$, ensuring cryptographic integrity (12)

3.3.6 Self-Healing Mechanism

The self-healing function updates the vehicle's state:

$$D_t = D_{t-1} + \delta D \quad (13)$$

In eq (13) where δD represents the recovered data. If δD < ϵ, additional recovery actions are triggered.

3.3.7 Cryptographic Hash Function

The algorithm that used is SHA-256 and the purpose ensures (3) data integrity of V2V messages stored in blockchain. Any data modification changes the hash value, indicating tampering

$$H=SHA256(Data)$$

3.3.8 Digital Signature Verification

The algorithm that used is Elliptic Curve Digital Signature Algorithm (ECDSA) and it authenticates vehicle messages, verifies that data is sent by a real vehicle, message signing using private key, signature verification using public key.

3.3.9 Dynamic Cryptographic Key Rotation

The algorithm that used is Time-based Key Update Function and it prevents replay and spoofing attacks. Detects hacked vehicles through key mismatch. Mathematical Logic:

$$K_{new} = f(K_{old}, T) \quad (14)$$

In eq(14) Where T = time interval.

3.3.10 Emergency-Free Zone Calculation

The algorithm that used is Distance-Based Radius Computation and it moves nearby vehicles to create a safe zone. Formula:

$$D = ((X_2 - X_1)^2 + (Y_2 - Y_1)^2)^{\wedge 2} \quad (15)$$

3.4 Software Development Life Cycle (SDLC) Model

For the Self- Healing Blockchain Mesh (SHBM) design, used the Agile Software Development Life Cycle (SDLC) Model. The Agile model promotes in flexibility, iterative

improvement, and rapid response to changing conditions needed by a security oriented system similar as SHBM.

3.4.1 Agile SDLC Model

The Agile SDLC model involves numerous iterations (sprints) to enable testing and enhancement at every phase. The following are the phases that undertook in SHBM development:

Requirement Analysis & Planning (Sprint 1)

Determined the need for real-time vehicle security using blockchain and V2V connectivity. Some of the specified aims are:

- Identify car hacking using Isolation Forest and LSTM, and securely isolate affected vehicles with blockchain.
- A Smart Rerouting Algorithm ensures that traffic flows properly.
- The datasets include Car-Hacking Dataset (OCS Lab) for detecting attacks, SUMO traffic simulation for vehicle navigation and rerouting. Blockchain logs for secure data tracking.
- The tools and technologies include Google Colab (SUMO, OpenCV, ML models), Flask/React.js for web-based visualizations and LevelDB for secure blockchain storage.

Design (Sprint 2)

The Architectural design with the following components are Attack Detection, Module (ML-based), Blockchain-Based Security Module, Smart Rerouting Module

Mathematical Model Design:

Defined attack detection logic: $\sum_{m=1}^{M} P_m > \tau$ (anomaly threshold)

Modeled vehicle rerouting: F = $\sum_{i=1}^{N} v_i / d_i$ (traffic flow)

Blockchain event logging using cryptographic hashing

Implementation (Sprint 3 & 4)

It created an SUMO-based car simulation in Google Colab. Isolation Forest and LSTM were used to identify attacks, blockchain was used for secure V2V communication and a Smart Rerouting Algorithm was developed to provide automatic lane change.

Testing & Evaluation (Sprint 5)

The Unit Testing includes [4] Validated attack detection accuracy with precision-recall metrics that confirmed vehicle rerouting without crashes in SUMO. The Integration Testing includes flawless integration among ML models, blockchain and SUMO. The verified tamper-proof security of blockchain. The Performance testing includes evaluated latency of attack detection & response time, and measured blockchain transaction time for security logs.

Deployment & Review (Sprint 6)

It implemented the SHBM prototype for testing in Google Colab & Flask/React.js. It completed final review for real-time security enhancements. It participated in a hackathon & paper presentation for external verification.

3.5 System Execution

The implementation of the Self-Healing Blockchain Mesh (SHBM) follows a structured process to ensure real-time security, anomaly discovery, rerouting safely and self-healing from compromised vehicles in independent traffic networks. The process of implementation includes the following major phases:

3.5.1 Data Preprocessing

The car hacking dataset (OCS Lab) is loaded and prepared for analysis. CAN bus signals (speed, RPM, steering angle, etc.) are extracted as features. Data is normalized and divided into training and testing sets.

3.5.2 Attack Detection

Original attack discovery is done by the Isolation Forest algorithm by detecting statistical anomalies in vehicular data. The LSTM model processes time-series data to identify

sequential anomalies with better discovery delicate. When an attack is linked, the vehicle declares as being hacked so that specific data is not contributed over V2V connection.

3.5.3 Vehicle Rerouting

The hacked vehicle is safely rerouted in the [2] SUMO simulation to avoid collisions with other vehicles. The Smart Car Contract Algorithm identifies the best and safe route to take the hacked vehicle. Other vehicles using Vehicle-to-Vehicle (V2V) communication will shift their routes and speed to allow the rerouted vehicle to pass through without causing any collision in the traffic. The occupied vehicle gradually moves to a safe lane rather than unexpected sudden changes.

3.5.4 Blockchain Logging (Blockchain)

The attack happened is securely stored on the blockchain and may be retrieved later. The original, unchanged data of the hacked vehicle is obtained from the blockchain, ensuring that no malicious modification exists. This prevents renewal attacks and provides a fake storage of vehicle data.

3.5.5 Self-Healing Process

The Self- Healing algorithm obtains the most recent secure state of the hacked vehicle from the blockchain. The control system of the vehicle is reset, removing the effect of the cyberattack. The vehicle is gradually moved back into regular service, continuing its original route without disturbing other vehicles. This recovery is achieved within one nanosecond resulting in minimal disruption.

3.5.6 Visualization & Analysis

The whole process is imaged through OpenCV to produce a final video. The output video displays the three phases of prosecution before attack,

- Normal vehicle movement (green vehicles),
- During the Attack - Blinking hacked vehicle(red) rerouting process,
- After Recovery - Vehicle securely restored (green again).

The video generated is employed for performance assessment, attack discovery effectiveness and verification of the repairing procedure.

3.6 Data Preprocessing & Working

3.6.1 Explanation & Working Method

The real-world CAN- machine dispatches and [12] simulates vehicular communication data in the SHBM design from its dataset. It assists in changing anomalies due to cyberattacks, protecting vehicle communication and allowing a secure rerouting.

3.6.2 Understanding the Dataset

The data set contains vehicle control signals like speed, RPM, braking status, acceleration and steering angle. Cyberattacks control these parameters, causing unusual vehicle behaviour such as sudden acceleration, brake failures, or illegal lane changes.

3.6.3 Preprocessing & Normalization

Raw CAN-bus data includes irregularities, missing values and outliers which have to be filtered. The system normalizes the data to rescale numerical features within a range of 0 to 1 so that no parameter controls the model's learning process.

3.6.4 Machine Learning Data Splitting

The dataset is resolved into 80 training data and 20 testing data to effectively train the anomaly discovery model. The training dataset includes normal vehicle actions and attack patterns to instruct the model to distinguish between safe and addressed countries.

3.6.5 Attack Detection with Isolation Forest & LSTM

The attack discovery process in the Self- Healing Blockchain Mesh (SHBM) employs a hybrid model consisting of Isolation Forest(IF) and Long Short-Term Memory (LSTM) to identify anomalies in vehicle behaviour. This ensures that hacked vehicle is detected in real time and protected before limiting business flow.

3.6.6 Overview of Attack Detection

Autonomous vehicles communicate via Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) networks makes them vulnerable to cyberattacks. Attackers can manipulate crucial parameters like speed (e.g., abrupt acceleration or brakes), braking System (e.g., loss of retarding control), lane positioning (e.g., illegal lane change), machine RPM & torque (e.g., exceeding machine capacity). This method uses Isolation Forest (IF) for anomaly detection and LSTM for sequential attack pattern analysis to identify similar vicious manipulations.

3.6.7 Isolation Forest for Anomaly Detection

Normal distribution is assumed by typical anomaly discovery models, while cyberattacks are compared to normal driving patterns. Isolation forest is the rare cases with smaller decision splits to detect anomalies. The isolation forest algorithm builds several arbitrary decision trees. The number of splits demanded to insulate a certain data point decides the anomaly score. The anomaly score is calculated as:

$$S_{(1)} = 2 - C_{(n)}E(h_{(x)}) \quad (16)$$

In eq (16) where:

E($h_{(x)}$) = Expected path length to isolate the vehicle state x

$C_{(n)}$ = Average path length of a binary search tree with n observations

$S_{(1)}$ close to 1 indicates a high anomaly likelihood

3.6.8 LSTM for Time-Series Attack Detection

Cyberattacks are frequently sequential and time-related (for example, steady acceleration drift resulting in loss of control). LSTM is a kind of Recurrent Neural Network (RNN) detects long-term connections in vehicle data. The model learns typical behavior and recognizes anomalous conduct as a possible attack. LSTM architecture for attack detection contains an input layer: Time-series vehicle data (e.g., speed, acceleration, RPM); LSTM Layers detect hidden sequential patterns in data. Dense Layer generates the chance of attack

incidence. Activation Function: Use Softmax or Sigmoid to distinguish between normal and hacked behavior. Mathematical Model of LSTM

Every LSTM cell processes data at time step according to the following equations:

Forget Gate: Determines

$$F_t = \sigma (W_f . [h_{t-1} , X_t] + b_f \quad (17)$$

Input Gate: Decides new data to store

$$i_t = \sigma(W_i .[h_{t-1},x_t]+b_i) \quad (18)$$

Cell State Update:

$$C_t = f_i . C_{t-1}+i_t \cdot C\sim t \quad (19)$$

Output Gate:

$$O_t = \sigma(W_o \cdot [h_{t-1},x_i]+b_o) \quad (20)$$

Final Hidden State:

$$H_t = o_t \tanh(C_t) \quad (21)$$

Output:

If output ≥ 0.5, the vehicle is considered safe.

If output < 0.5, a cyberattack is detected.

3.6.9 Hybrid Model: Combining IF and LSTM for Robust Detection

Since IF detects statistical anomalies and LSTM detects sequential behavior changes, combining them ensures higher accuracy. Isolation Forest detects sudden anomalies (e.g., a sudden increase in acceleration). LSTM detects gradual pattern deviations (e.g., subtle changes in speed over time). The final decision is made by a weighted combination of both scores.

To obtain the best results in terms of detection error and recovery performance at different levels of attack, phase 4 was chosen to be optimized by grid search to obtain the best parameters α and β. Where α+β = 1\α + 1\β = 1α+β=1 and weights are optimized based on training accuracy.

3.6.10 Real-Time Attack Detection in SUMO

If an attack is detected, the car flashes red in the SUMO simulation to show a cyberattack. The SHBM system separates the car and initiates a rerouting process. The attack incident is recorded in the blockchain for forensic examination. The vehicle self-heals, rebuilding secure driving parameters.

4. Vehicle Rerouting in SUMO (Simulation of Urban Mobility) & Real-Time Implementation

4.1 SHBM for Vehicle Rerouting

The following protocols are used in proposed Self-Healing Blockchain Mesh (SHBM) system to establish vehicle rerouting on V2V Communication with Blockchain-Backed Recovery. Vehicles can communicate their attack status in real time via the V2V communication protocol, which enables neighboring vehicles to change their routes and speeds. In order to detect attacks and make decisions about rerouting, the Smart Car Contract Algorithm (SCCA) offers safe and authenticated messaging. Based on traffic, road conditions and possible safe zones, the Car Rerouting Algorithm (CRA) determines a safe path for compromised automobiles. Blockchain-Based Recovery Protocol preserves the vehicle's condition prior to an attack, allowing for dependable data restoration and self-healing. This system projects the real-world SHBM behavior by dynamically overriding the car's movements in SUMO.

4.2 SHBM Reroute in Real Time (Beyond SUMO Simulation)

In the actual deployment of SHBM, rerouting would take place through the following process:

- **Attack Detection & Isolation:** A vulnerable vehicle is identified using Isolation Forest and LSTM. The hacked vehicle stops sharing compromised V2V data. A

distinct ID is generated by the Smart Car Contract Algorithm (SCCA) and stored on the Blockchain.

- **Safe Rerouting Decision via Car Rerouting Algorithm (CRA):** The safest alternative route is calculated by SHBM using conditions of the roads and density of traffic V2V communication is used to safely communicate a new rerouting method.
- **Safe Vehicle Rerouting Process:** The autonomous vehicle will admit instructions to move, If the addressed AV has a safer area to dislocate. Other vehicles in the area will continue to adjust their speeds and lane changes smoothly for the purpose to avoid the AV. SHBM assures that all other cars will accommodate so that they are not an impact on the other vehicle.
- **Self-Healing & Blockchain-Based Data Recovery:** Using the blockchain to access initial vehicular parameters. The compromised vehicle is reintroduced into the system and continues standard functioning. The blockchain system confirms the restored secure V2V.
- **SUMO Implementation for Rerouting (Simulation-Based):** It will manually reroute by replicate vehicle behavior because SUMO does not dynamically reroute vehicles because of hacking.

  Step 1: Determine vehicle has been hacked.

  Example car impacted by an attack:
  hacked_vehicle = "veh_3".
  To show that a car is hacking, change its color to red.
  Vehicle.setColor((255, 0, 0, 255), hacked_vehicle

  Step 2: Decrease Velocity Prior to Rerouting

  The function
  reduce_speed(vehicle_id, target_speed): traci.vehicle = current_speed.
  obtain While *current_speed > target_speed, speed(vehicle_id): current_speed -= 0.5*
  Slow down the track.vehicle gradually.
  set *Speed(current_speed, vehicle_id) traci.simulationStep().*
  This prevents collisions by ensuring the compromised car continues unexpectedly

  Step 3: Switch lanes to a more secure location. Slowly, the car shifts to a safer lane

Step 4: Enter a designated safe area

If

vehicle_id = def move_to_safe_zone: "safe_zone_road" = "safe_edge"

SUMO Traci's predetermined road segment.

Vehicle.change target(safe_edge, vehicle_id).

Take the compromised car to a specified safe area.

Go to the safe area *(hacked_vehicle).*

The automobile exits the current traffic flow to replicate isolation

Step 5: After Recovery, Reintegration

The function

reintegrate_vehicle(original_route, vehicle_id): Return to the first path.

Return the car to its original path.

"normal_route_road"=original_route.reintegrate_vehicle(original_route,hacked_vehicle)

After recovery, the car becomes green and resumes its previous path

5. Blockchain Integration & Self-Healing Mechanism

The Self- Healing Blockchain Mesh (SHBM) result uses a regular self-healing mechanism to give data integrity and safe vehicle recovery. After an attack, the procedure enables vehicles to recapture their original characteristics, enabling them to easily transfer business.

5.1 Self-Healing Process in SHBM

The self-healing process is made up of five fundamental steps:

- **Attack Detection & Vehicle Isolation:** The technology monitors vehicle performance. When a change using the Random Forest or LSTM is found, the modified bus is indicated. The technology immediately separates the attacked vehicle and prevents the transmission of attacks by removing the V2V connection.
- **Data Backup & Secure Storage:** Before the recovery process, all the original vehicle parameters such as route, position, speed and detector data are securely preserved. The

data is stored in a cloud database for future use and confirmations. The data makes it possible to trace any illegal modifications made to the vehicle's settings.

- **Rerouting & Traffic Coordination:** A smart rerouting algorithm ensures that the compromised vehicle is rerouted in a way that the safe redirection is done so that no accidents could occur. Overall traffic has reduced collisions. The routing is changed continually depending on the vehicles and traffic situations. SUMO simulates this rerouting process in real-world applications using real-time cloud-based navigation.
- **Parameter Restoration & Security Enforcement:** The system retrieves its original parameters from the database after the vehicle has arrived at a secure area. The self-healing system restores the previous speed, detector readings and safe route history. Security enforcement ensures that any affected control signals are excluded to prevent future exploitation. The Random Forest and LSTM model will be combinely used to ensure proper attack identification and restoration. The AV is securely rerouted and its variations (lane changing, speed oscillations) are made. SHBM uses SUMO to detect the attack to avoid a collision.
- **Self-Healing & Reintegration:** Previous safe classifications are used for collecting vehicle data from a database or cloud. Without impacts, the vehicle is slowly returned to its beginning lane. The system utilizes V2V communication to securely transmit attack data.

6. Results

This section compares the existing and proposed work. Figure 3 shows the proposed work reduced the attack detection and the recovery time compared to the existing time. Figure 4 shows overall safety improvements compared to the exiting methods.

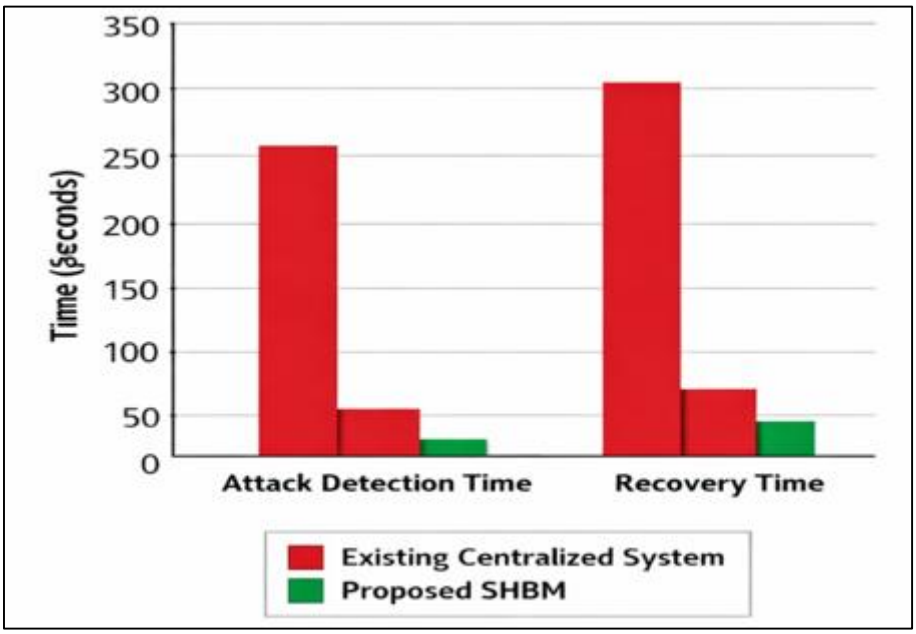

Figure 3. SHBM Reduces Attack Detection and Recovery Time

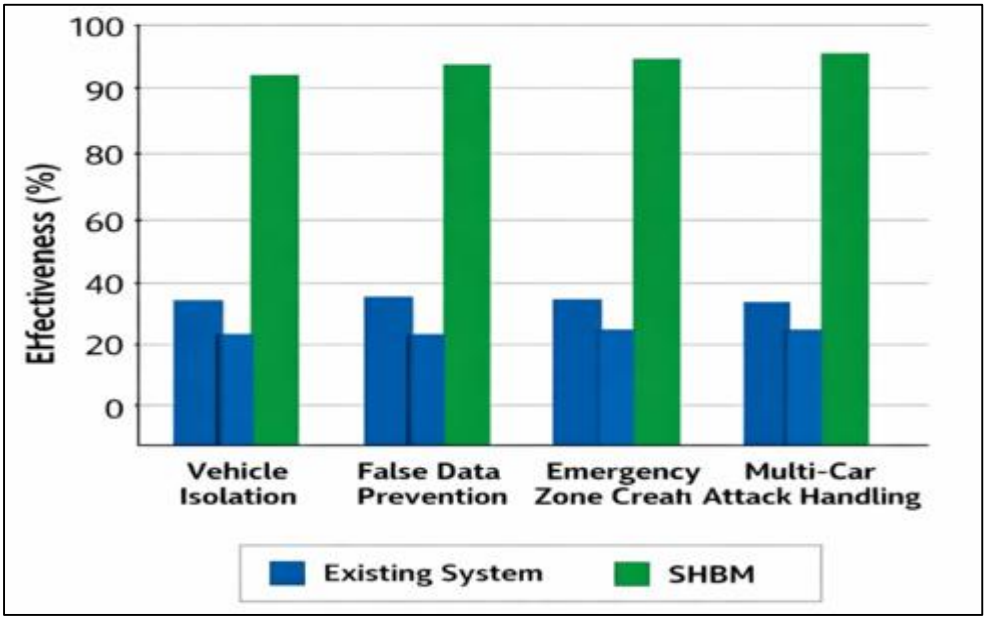

Figure 4. SHBM Improves Overall Safety Effectiveness

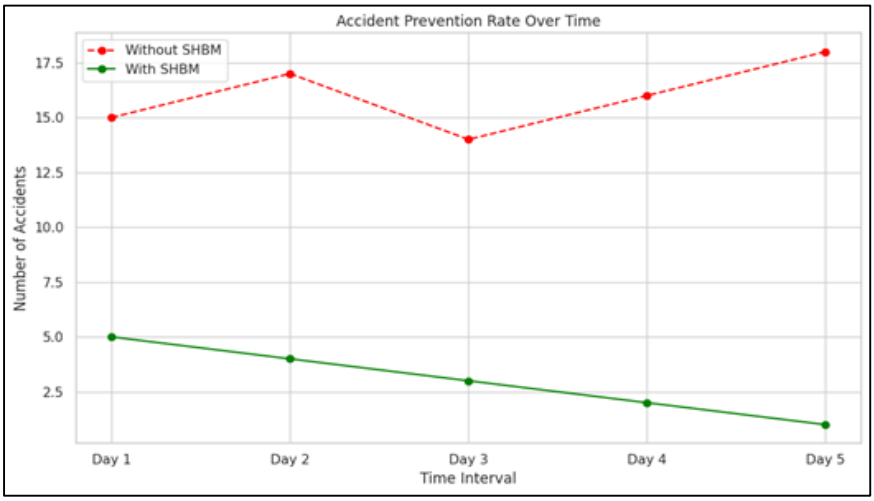

Figure 5. SHBM Lowers Accident Rates Over Time

Figure 5 shows the lower accidents compared to the existing system. The visual results prove that SHBM is always better than the existing systems that decreases the detection latency, increases safety response and minimizes the accident probability.

The below result provides overall working of the system. Figure 6 shows the overall vehicle runs in normal speed with constant flow makes the vehicle operate safely and without any attacks.

Figure 6. Normal Vehicle and Constant Speed

Figure 7 shows the various vehicles interact in a normal condition with stead velocity and speed which displayed in the below screen. The vehicles are functioned in a V2V framework and shows as secure.

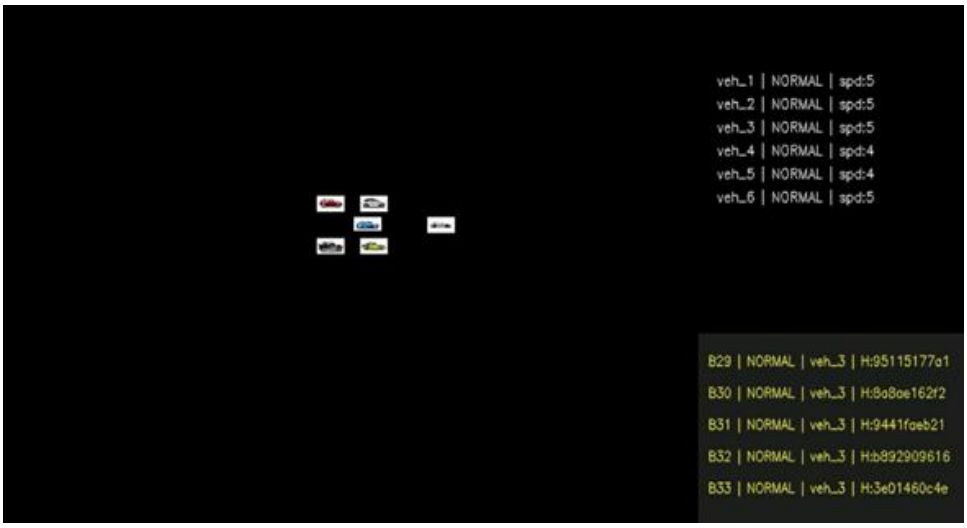

Figure 7. Displaying Safe and Joint V2V Functionality

Figure 8 shows one of the vehicle has detected to be attached and other vehicle operated in a normal mode makes the system to detect the attack effectively.

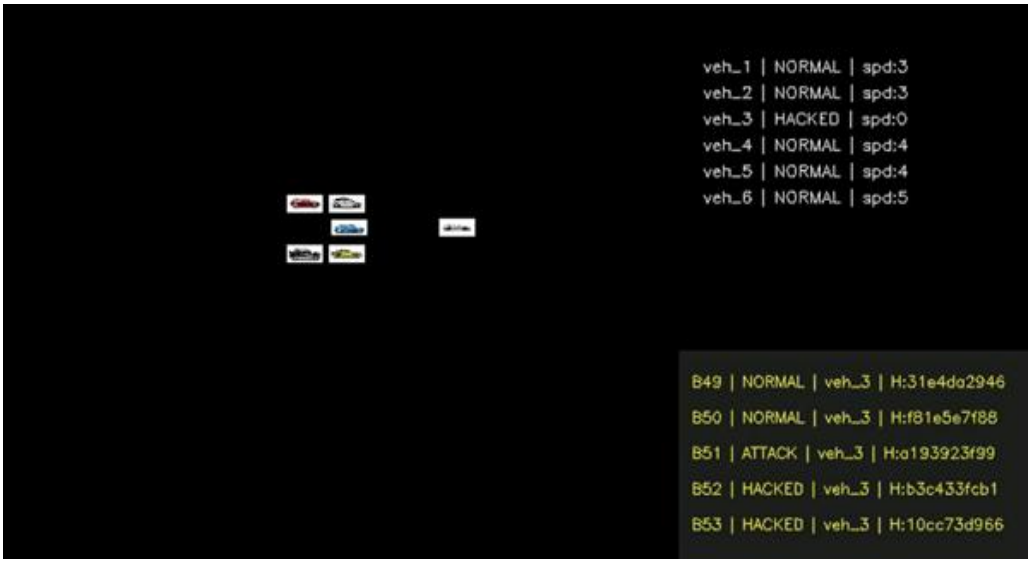

Figure 8. Attacked Vehicle Detected

Figure 9 illustrates the attacked vehicle should be isolated and healing processes are executed. The other car which are not affected are driving continuously. Figure 10 shows the affected vehicle is detected and isolated to detect the problem and makes the vehicle to operate normally for the safe drive.

Figure 9. Attacked Vehicle Isolated and Healing Process started

Figure 10. Veh_3 is Detected and Isolated Continues

Figure 11 shows the healing process of affected vehicle and displayed as recovered which makes the other vehicle can identify that the affected vehicle is cured to run safely.

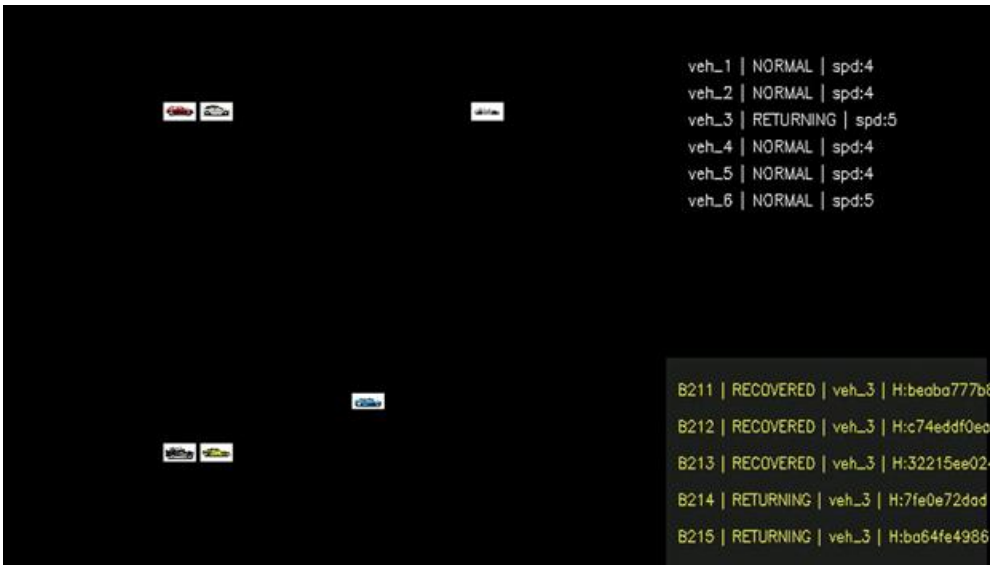

Figure 11. Healing of Veh_3 is Started and Switched to Recovered

Figure 12 illustrates the recovered vehicle is switched to the returning status with a higher speed to get back to the lane.

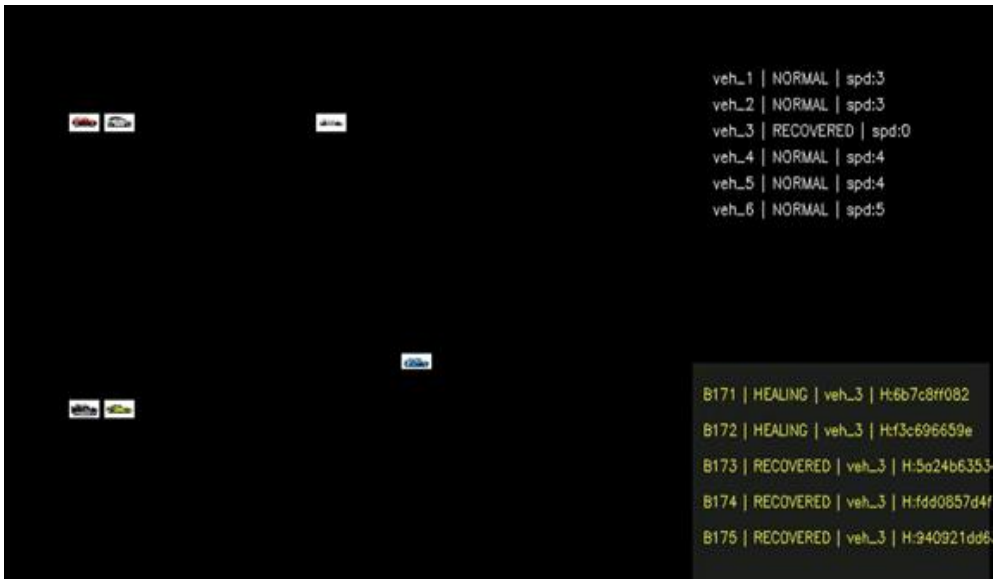

Figure 12. Recovered Vehicle Veh_3 Switches to Returning Status with a Higher Speed

Figure 13 shows the overall blockchain log that captures the vehicle real-time like vehicle speed, lane position to verify the data that integrate during the recovery process.

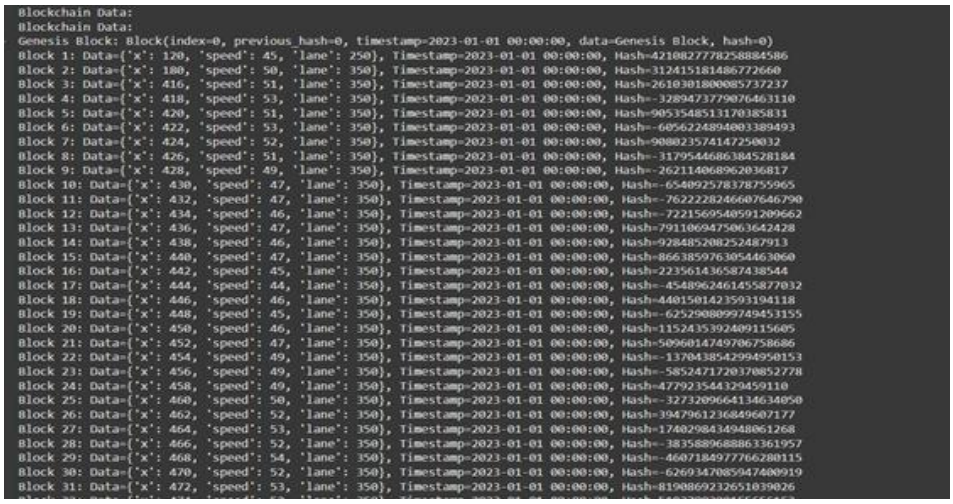

Figure 13. Blockchain Log Captures Vehicle Speed, Lane and Position for Verification

7. Conclusion

The proposed work is an innovative method of authorized, autonomous vehicle security. It will detect, extracts and recovers the repaired vehicles using decentralized blockchain-based self-healing mechanism for secure communication to prevent accidents and provide safe traffic flow. The proposed system detects the anomalies using hybrid model that combines LSTM network with random forest method in future. The nearby vehicles are also instructed using encrypted V2V communication to develop a secure data and reduce the risk of collision. The data securely stored on a blockchain with data recovery and validation using the sound repairing procedure. This provides the traceability, transparency and data evaluation. The complete setup is shown in a model developed with SUMO and OpenCV. It includes regular driving operations, attack detection, secure vehicle route and system recovery. The decentralized and robust structure of SHBM improves the adaptability and efficiency of future smart transportation systems.

References

[1]. Ghosh, Sanchita, and Tanushree Roy. "Assessment of Cyberattack Detection-Isolation Algorithm for CAV Platoons Using SUMO." In 2025 American Control Conference (ACC), IEEE, (2025): 1635-1640.

[2]. Willie, Alan. (2025). The Role of Blockchain in Enhancing Security for Autonomous Vehicles.

[3]. Kusari, Arpan, Pei Li, Hanzhi Yang, Nikhil Punshi, Mich Rasulis, Scott Bogard, and David J. LeBlanc. "Enhancing SUMO simulator for simulation based testing and validation of autonomous vehicles." In 2022 ieee intelligent vehicles symposium (IV), IEEE, (2022): 829-835.

[4]. Iordache, Stefan, Catalina Camelia Patilea, and Ciprian Paduraru. "Enhancing autonomous vehicle safety with blockchain technology: Securing vehicle communication and AI systems." Future Internet 16, no. 12 (2024): 471.

[5]. Anbalagan, Sudha, Wajdi Alhakami, Mugundh Jambukeswaran Bhooma, Vijai Suria Marimuthu, Kapal Dev, and Gunasekaran Raja. "Next-gen security: enhanced DDoS attack detection for autonomous vehicles in 6G networks." In 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), IEEE, (2024): 1-5.

[6]. Ming, Yu, Yanqiang Li, Zihui Zhang, and Weiqi Yan. "A survey of path planning algorithms for autonomous vehicles." SAE international journal of commercial vehicles 14, no. 02-14-01-0007 (2021): 97-109.

[7]. Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." Eai Endorsed Transactions on Security and Safety 3, no. 9 (2016): 21.

[8]. Luo, Weixin, Wen Liu, and Shenghua Gao. "A revisit of sparse coding based anomaly detection in stacked RNN framework." In Proceedings of the IEEE international conference on computer vision, (2017): 341-349.

[9]. "Vehicle-to-Vehicle (V2V) Communication," Avnet Abacus, 2025. communication/Avnet

[10]. Keerthana, S., Anitha Lakshmi, Naveen Kumar, and Naveen Kumar Kumar. "Connected Vehicles and The Future of Internet of Vehicles (IoV)." Journal of Automotive Engineering & Technology ISSN: 3107-7390 (Online) 10, no. 2 (2025).

[11]. Zhang, Xinyu, Junxian Li, Jingyi Zhou, Shiyan Zhang, Jingyuan Wang, Yi Yuan, Jiale Liu, and Jun Li. "Vehicle-to-everything communication in intelligent connected vehicles: a survey and taxonomy." Automotive Innovation 8, no. 1 (2025): 13-45.

[12]. Ye, Hao, Geoffrey Ye Li, and Biing-Hwang Fred Juang. "Deep reinforcement learning based resource allocation for V2V communications." IEEE Transactions on Vehicular Technology 68, no. 4 (2019): 3163-3173.

[13]. Sun, Wanlu, Erik G. Ström, Fredrik Brännström, Yutao Sui, and Kin Cheong Sou. "D2D-based V2V communications with latency and reliability constraints." In 2014 IEEE Globecom Workshops (GC Wkshps), IEEE, (2014): 1414-1419.

[14]. YMeng, Wanyu, Xinghe Chu, Zhaoming Lu, Luhan Wang, Xiangming Wen, and Meiling Li. "V2V communication assisted cooperative localization for connected vehicles." In 2021 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, (2021): 1-6.

[15]. Garcia, Mario H. Castañeda, Alejandro Molina-Galan, Mate Boban, Javier Gozalvez, Baldomero Coll-Perales, Taylan Şahin, and Apostolos Kousaridas. "A tutorial on 5G NR V2X communications." IEEE Communications Surveys & Tutorials 23, no. 3 (2021): 1972-2026.

[16]. Condliffe, J. "A single autonomous Car has a huge impact on alleviating traffic." (2017).

[17]. Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41, no. 3 (2009): 1-58.

[18]. Daniel, Alfred. "Vehicle to vehicle communication using Zigbee protocol." In Proceedings of the 29th annual ACM symposium on applied computing, pp. 715-716. 2014.

[19]. Hartenstein, Hannes, and L. P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." IEEE Communications magazine 46, no. 6 (2008): 164-171.

[20]. Zhang, Xinran, Mugen Peng, Shi Yan, and Yaohua Sun. "Deep-reinforcement-learning-based mode selection and resource allocation for cellular V2X communications." IEEE Internet of Things Journal 7, no. 7 (2019): 6380-6391.

[21]. Ray, Jayanta Kumar, Ardhendu Shekhar Biswas, Sanjib Sil, Rabindranath Bera, Subhankar Shome, Pallabi Biswas, and Monojit Mitra. "Realization of 5G V2V

communication system at 28 GHz for smart vehicle." Innovations in Systems and Software Engineering 20, no. 4 (2024): 669-687.

[22]. Li, Zan, Tianjiao An, Bo Dong, and Xiaohui Yuan. "Event-triggered V2V communication-based cooperative adaptive tracking control for nonlinear vehicle platoon systems with unknown lag time." Nonlinear Dynamics 113, no. 1 (2025): 519-532.

[23]. Mande, Spandana, and Nandhakumar Ramachandran. "A comprehensive survey on challenges and issues in v2x and v2v communication in 6g future generation communication models." Ingenierie des Systemes d'Information 29, no. 3 (2024): 951.

[24]. Su, Lan, Yong Niu, Zhu Han, Bo Ai, Ruisi He, Yibing Wang, Ning Wang, and Xiang Su. "Content distribution based on joint V2I and V2V scheduling in mmWave vehicular networks." IEEE Transactions on Vehicular Technology 71, no. 3 (2022): 3201-3213.