Resilient Security Frameworks for 6g Vehicular Iot: Integrating Blockchain, Ai-Driven Ids and Ethical Governance

Vinay Lomte[1], Yogendra Chhetri[2], Pankaj Kumar Sanda[3,4], Subhadip Goswami[5*], Mohammad Ashique Azad[6,7]

[1]Department of Mechanical Engineering, Dr Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar, Maharashtra

Email: vlomte.chemtech@bamu.ac.in

[2]Department of Centre for Continuing Education, Indian Institute of Science, Bengaluru, Karnataka

Email: chhetri.com@gmail.com

[3]Department of Electronics and Communication Engineering, National Institute of Technology, Mizoram-796012, Aizawal, Mizoram

[4]Department of Electronics & Communication Engineering, Brainware University, Kolkata, West Bengal

Email: eternal_deny_crist@yahoo.com

[*5]Department of Electrical Engineering, Sandip Institute of Technology & Research Centre (Autonomous), Nashik, Maharashtra

Email: subhadip.goswami@sitrc.org

[6]Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh

Email: azadashique@gmail.com

[7]PhD Research Scholar, NIT Jamshedpur

Abstract

The fast development of 6G-enabled vehicular Internet of Things (IoT) brings new opportunities of autonomous mobility, cooperative perception, and ultra-reliable communication, but also subjects vehicles to multi-layered, multi-faceted cyber threats. This paper is a cohesive investigation of security, privacy, and trust issues of next-generation vehicular networks and how blockchain, artificial intelligence (AI), and distributed edge architectures can work together to improve resilience. It initially presents the categorization of vehicular threats in terms of authentication, data integrity, availability, privacy, and physical tier, using real-life examples, including the Jeep Cherokee hack and GPS spoofing, to explain how severe the attacks can be practical. It next discusses blockchain-based trust models, which play roles in the decentralized management of identities, the sharing of data without any tampering, and the use of smart contracts to enable automation. Moreover, it examines the AI-driven intrusion detection systems that are based on machine learning, deep learning, federated learning, and reinforcement learning to identify the changing attacks in real-time. The combination of blockchain and AI is discussed as the synergistic model that can be used to secure trust, maintain integrity, and enhance adaptive threat identification. To make sure of responsible deployment, ethical and regulatory factors, such as privacy protection, liability, fairness, transparency, and global standardization, are addressed. This article presents a comprehensive background to the creation of a secure, trustful, and future-resistant vehicular ecosystem during the 6G era with its insights on architecture, case studies, and a pseudo-coded IDS framework.

Keywords: 6G Vehicular IoT, Blockchain Security, AI-driven Intrusion Detection, Vehicular Trust Management, Edge-Distributed Intelligence

1. Introduction

Vehicular networks are extremely dynamic, dispersed, and mission-critical ecosystems, particularly when considering the 6G-enabled Internet of Vehicles (IoV). These networks combine pedestrians, cars, roadside infrastructure, and cloud/edge servers into a framework for collaborative communication. Vehicular networks require ultra-reliable and ultra-low latency communication to guarantee road safety, traffic efficiency, and autonomous coordination, in contrast to traditional IoT systems that can withstand slight disruptions. As a result, security issues in automobile networks endanger not just privacy and data integrity but also human life.

Any deliberate or inadvertent activity that jeopardizes the confidentiality, integrity, authenticity, availability, or reliability of communication and computation in automotive IoT systems is considered a vehicular security hazard [1]. The physical, network, and application levels are all affected by these multifaceted risks, which change as 6G connectivity, blockchain, and artificial intelligence (AI) are included into automotive systems.

This section offers a thorough examination of security risks in vehicle networks, covering their categorization, methods of exploitation, practical applications, and brief case studies focused on specific applications.

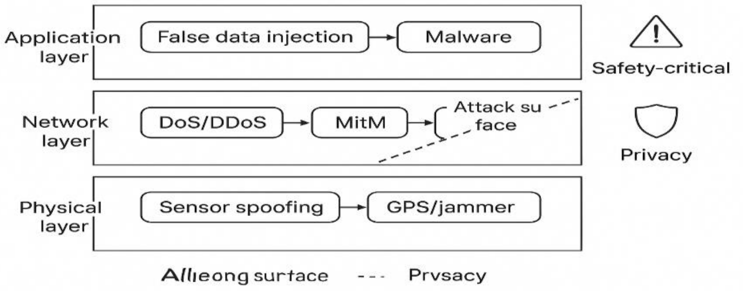

Figure 1: Layered Threat Model

1.1 Classification of Security Threats in Vehicular Networks

The various security threats that affect vehicular networks can be roughly divided into the following classes:

(a) Authentication and Identity-Based Threats

The foundation of safe vehicle communication is authentication. Malicious nodes can pose as trustworthy infrastructure or automobiles in the absence of strong authentication. Spoofing Attacks: To deceive others, attackers pretend to be a genuine car or roadside assistance unit (RSU). A rogue node might, for example, pose as an ambulance and ask for priority traffic flow [2]. To manipulate network consensus or overload vehicle communication with erroneous alarms, a single adversary fabricates several phony identities. This jeopardizes the credibility of joint awareness messaging.

(b) Data Integrity and False Information Threats

Vehicular networks depend upon continuous message exchanges which include Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs). In these attacks, adversaries introduce fake traffic or accident notifications, as well as deceptive navigation and route optimization algorithms [3]. When attackers change transmitted data, including GPS locations or speed readings, it can result in dangerous driving choices. In intersection management, inaccurate trajectory data can lead to collisions and conflicting driving patterns.

(c) Availability and Denial-of-Service Threats

For real-time vehicle coordination, communication channels must be available. Catastrophic failures may result from attacks that deplete system resources. Attackers overwhelm bandwidth and processing resources by bombarding RSUs or edge servers with fictitious requests [4]. Coordinated assaults from several malevolent vehicles increase interference and may result in widespread communication failures. A denial-of-service attack can hinder ambulances' ability to communicate with traffic signals during emergency vehicle priority, causing crucial response times to be delayed.

(d) Confidentiality and Privacy Threats

Sensitive information, such as driver identity, passenger information, and vehicle trajectories, is constantly exposed by vehicular communication. V2X messages intercepted without authorization jeopardize privacy [5]. Persistent monitoring of vehicular communication can reveal driver patterns and compromise anonymity. Adversaries exploit infotainment systems to collect personal data such as browsing history or biometric identifiers. In ride-hailing services, eavesdropping on location updates can endanger passengers by revealing travel patterns.

(e) Man-in-the-Middle (MitM) and Relay Attacks

Adversaries intercept and alter communications between nodes of confidence in MitM attacks. Attackers place themselves between two vehicles or between a vehicle and RSU, modifying or delaying data. Relay Attacks – Messages are captured and retransmitted by adversaries to create confusion in timing and location-based authentication systems [6]. In V2I toll payment systems, relay attacks can delay authentication, causing congestion or financial fraud.

(f) Physical and Hardware-Based Threats

Vehicular IoT also faces hardware-level vulnerabilities:

Sensor Spoofing – Manipulation of LiDAR, radar, or GPS signals causes vehicles to misinterpret their environment.

Side-Channel Attacks – Exploiting electromagnetic leaks or power consumption patterns of onboard units (OBUs).

Hardware Tampering – Unauthorized modifications to vehicular ECUs (Electronic Control Units).

GPS spoofing has been demonstrated to mislead autonomous vehicles into navigating incorrect routes [7].

1.2 Real-World Incidents Demonstrating Vehicular Threats

Jeep Cherokee Hack (2015): By securely taking advantage of a flaw in the infotainment system of the Jeep Cherokee, security researchers successfully managed to take over the functions of steering and braking [8].

Tesla Model S Attack (2016) – Researchers hacked the Tesla Model S via the CAN bus and remotely controlled braking functions.

GPS Spoofing on Drones – Demonstrations of GPS spoofing on unmanned aerial vehicles (UAVs) highlight the risk of similar attacks on autonomous vehicles [9].

These incidents underscore that vehicular security is not hypothetical; it has tangible safety implications.

1.3 Layered Threat Analysis in Vehicular IoT

Security threats manifest across multiple layers of vehicular IoT architecture:

Physical Layer – Sensor spoofing, jamming, and hardware tampering.

Network Layer – DoS/DDoS, MitM, routing attacks.

Application Layer – False message injection, software malware.

Cross-Layer Threats – Coordinated attacks that exploit multiple layers simultaneously, such as tampering with sensor input while launching a DoS on communication.

Understanding these layers is critical for developing multi-layered defense architectures in 6G vehicular IoT.

1.4 Emerging Threats in 6G Vehicular Networks

The transition to 6G-enabled vehicular networks introduces novel threats:

- AI-Powered Adversaries – Attackers using generative adversarial networks (GANs) to craft synthetic vehicular messages that evade detection [10].
- Quantum-Enabled Attacks – Future quantum computers may break traditional cryptographic schemes, threatening V2X communication integrity.
- Edge and Federated Learning Attacks: In automotive AI, federated learning frameworks are compromised by data poisoning or model inversion attacks.

A federated learning-based intrusion detection system's capacity to identify hostile nodes within a platoon could be compromised by an adversary.

1.5 Implications of Security Threats

Beyond just causing technological hiccups, security breaches in the automotive IoT have the following effects:

- Traffic fatalities, collisions, and impaired pedestrian safety are examples of safety risks.
- Economic Losses: Attacks on autonomous logistics fleets cause supply chain interruptions.
- Erosion of Trust: The public's mistrust about the introduction of autonomous driving.
- Regulatory Challenges: Governments are having trouble assigning blame for cyber-physical mishaps.

1.6 Short-Term Applications in Mitigating Threats

- Secure Authentication Protocols: These are simple cryptographic techniques that prevent spoofing.
- AI-Based Anomaly Detection: Machine learning intrusion detection systems to combat dynamic threats.
- Blockchain-Backed Trust Models: Unchangeable ledgers used to validate communications sent by vehicles.
- Privacy-Preserving Mechanisms: To protect user data, use pseudonym-based IDs and differential privacy.

The threat landscape for vehicular networks in the 6G era is complicated and constantly changing. Threats range from data injection and identity spoofing to DoS and AI-powered attackers, with practical ramifications for trust, safety, and the economy. Ultra-low latency, distributed AI, and blockchain interact to produce new risks as well as resilience-boosting options. Understanding these threats in detail forms the foundation for designing next-generation defense mechanisms, which are explored in the subsequent sections.

2. Blockchain-Enabled Vehicular Trust

For trustworthy and safe communication, the Internet of Vehicles (IoV) is heavily dependent on trust. Unlike conventional mobile networks, vehicular systems operate in dynamic environments where nodes (vehicles, roadside units, and edge servers) frequently join and leave the network. When used in extremely portable vehicle environments, traditional centralized trust models like Public Key Infrastructure (PKI) have challenges with scalability and latency [11]. Blockchain technology has become known as a viable accelerator of decentralized trust in vehicle IoT for addressing these issues.

Blockchain is referred to as an immutable ledger that is distributed with an independently verified record of transactions in each block that is kept up to the present by an agreement process [12]. By removing the dependency on a single trusted authority, blockchain provides tamper-proof, transparent, and auditable communication suitable for 6G-enabled vehicular networks that demand ultra-low latency and high reliability.

This section explores blockchain-enabled vehicular trust, including its fundamental principles, applications in vehicular communication, consensus mechanisms, integration challenges, and research-oriented use cases.

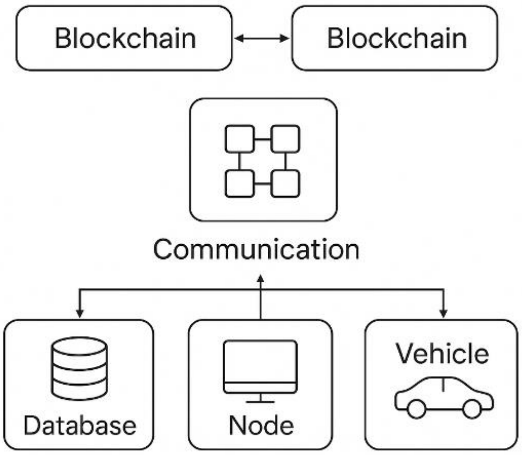

Figure 2: Blockchain-enabled Vehicular Trust Architecture

2.1 Principles of Blockchain in Vehicular Networks

(a) Immutability and Integrity

Data can not be modified once it has been added to an existing blockchain without turning the whole network invalid. This ensures that vehicular communication records—such as location updates, safety alerts, and certificate validations—remain tamper-proof [13].

(b) Decentralization and Trustless Operation

Blockchain eliminates reliance on a central server. Trust is distributed across participating nodes, making it resilient to single-point-of-failure attacks [14]. In vehicular networks, where mobility creates intermittent connectivity, decentralization ensures robust security even when infrastructure nodes are temporarily unavailable.

(c) Transparency and Auditability

Transactions recorded on blockchain can be traced back to their source. This provides accountability in vehicular interactions, for example, proving whether a vehicle genuinely reported a road hazard.

(d) Smart Contracts

Blockchain supports automated execution of rules through smart contracts. These can enforce vehicular trust policies such as priority-based intersection management, platooning rules, or toll payments without human intervention [15].

2.2 Blockchain Applications in Vehicular IoT

Blockchain supports multiple trust-oriented applications in vehicular IoT, particularly in safety-critical and commercial scenarios:

(a) Secure Identity and Authentication

Blockchain can provide decentralized vehicle identity management. Instead of relying on a centralized PKI, vehicles are registered on blockchain with unique cryptographic credentials. This prevents spoofing and Sybil attacks.

Emergency vehicles (ambulances, fire trucks) can authenticate their priority claims on-chain, preventing malicious impersonation [16].

(b) Data Integrity and Provenance

Blockchain ensures that vehicular data—such as Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs)—is verifiable and traceable. When an accident occurs, blockchain can prove whether warning messages were genuinely broadcast by nearby vehicles, enabling forensic accountability.

(c) Decentralized Trust for V2V and V2I

Vehicles and roadside units (RSUs) can validate messages against blockchain entries, eliminating the need for third-party trust authorities. In platooning, only vehicles with verified blockchain identities can join the convoy, ensuring trust among participants [17].

(d) Autonomous Transactions and Services

Smart contracts can automate vehicular services such as toll collection, charging, and insurance claims. In electric vehicle (EV) charging, blockchain-based micropayments enable secure, transparent transactions between vehicles and charging stations.

2.3 Consensus Mechanisms for Vehicular Blockchain

How consumers of blockchain technology agree on the trustworthiness of transactions shall be determined by the consensus algorithm. However, because of the significant energy and latency costs, traditional approaches like Proof of Work (PoW) are not compatible with vehicle IoT [18]. Research proposes lightweight alternatives:

- Proof of Authority (PoA): RSUs or trusted infrastructure nodes act as validators, ensuring low latency validation suitable for 6G URLLC.
- Practical Byzantine Fault Tolerance (PBFT): Efficient consensus for small networks, resilient against malicious participants.

- Delegated Proof of Stake (DPoS): Vehicles elect delegates to validate transactions, balancing decentralization with efficiency.
- Hybrid Consensus: Combining blockchain with AI to dynamically select consensus mechanisms based on network conditions [19].

Each consensus mechanism involves a trade-off between latency, scalability, and security. For 6G vehicular IoT, sub-second consensus is essential to support time-critical applications like collision avoidance and intersection scheduling.

2.4 Benefits of Blockchain for Vehicular Trust

- Tamper-Proof Data Sharing: Ensures integrity of vehicular messages.
- Decentralized Trust: Removes reliance on centralized authorities.
- Resilience Against Attacks: Mitigates spoofing, Sybil, and message tampering.
- Automated Policy Enforcement: Smart contracts regulate vehicular interactions.
- Forensic Evidence: Blockchain records can be used in accident investigations or legal disputes.

2.5 Challenges of Blockchain Integration in Vehicular IoT

Despite its advantages, blockchain adoption in vehicular networks faces significant challenges:

(a) Latency Overhead

Even lightweight consensus mechanisms introduce delays, potentially conflicting with the sub-millisecond latency requirement of 6G vehicular coordination [20].

(b) Scalability

With millions of vehicles exchanging data, blockchain storage requirements may become excessive. Lightweight solutions such as sharding and off-chain storage are under exploration.

(c) Energy Consumption

Vehicles, particularly electric ones, cannot afford heavy computational loads. Blockchain must be designed for energy efficiency to avoid depleting vehicular batteries.

(d) Interoperability

Different automotive manufacturers and service providers may adopt different blockchain frameworks, creating compatibility issues.

(e) Security Vulnerabilities

Blockchain itself is not immune to attacks, such as 51% attacks, smart contract bugs, or denial-of-service on validator nodes.

2.6 Research-Oriented Case Studies

Case Study 1: Blockchain for Intersection Management

Researchers have proposed blockchain-enabled intersection management systems where vehicles submit their trajectories to a smart contract. The blockchain ensures that trajectories are validated, preventing conflicts and collisions [21].

Case Study 2: Platooning with Blockchain

Blockchain can manage secure platooning by recording vehicle credentials on-chain. Only authenticated vehicles can join or leave the platoon, preventing malicious infiltration [22].

Case Study 3: Blockchain-Assisted Accident Forensics

In the event of a collision, blockchain provides immutable records of vehicular communication prior to the incident. This ensures transparency in determining liability and prevents falsification of evidence [23].

Blockchain offers a paradigm shift in vehicular trust management, moving from centralized, authority-driven systems to decentralized, transparent, and resilient frameworks. Through secure identity management, data integrity, and smart contract automation, blockchain mitigates many of the threats outlined in Section 4.1.

However, its integration with 6G vehicular IoT requires addressing latency, scalability, and energy challenges. Future research points toward hybrid blockchain-AI architectures, lightweight consensus protocols, and interoperable frameworks to ensure blockchain's practicality in ultra-low latency vehicular systems.

Blockchain, when combined with AI (explored in Section 4.4), forms a cornerstone of secure, privacy-preserving, and trustworthy vehicular communication in the 6G era.

3. AI-Driven Intrusion Detection Systems (IDS)

Vehicular networks are vulnerable to a variety of dynamic threats, as described in Section 4.1, from denial-of-service (DoS) and AI-powered adversarial attacks to spoofing and fake data insertion. The dynamic, high-mobility, and ultra-low latency needs of 6G-enabled vehicular IoT are making traditional security measures like static firewalls and signature-based intrusion detection systems (IDS) increasingly inadequate [24].

An Intrusion Detection System (IDS) can be defined as a monitoring mechanism that identifies malicious activities or policy violations within a network or computing environment [25]. In vehicular IoT, IDS must operate in real time, under strict latency constraints, and with the ability to adapt to continuously changing vehicular traffic conditions.

The emergence of artificial intelligence (AI) and machine learning (ML) has transformed IDS from rule-based, reactive systems into adaptive, intelligent, and proactive defense tools. AI-driven IDS leverage data analytics, pattern recognition, and predictive modeling to detect both known and unknown attacks. This section explores the types of AI-driven IDS, their architectures, applications in vehicular IoT, challenges, and case studies.

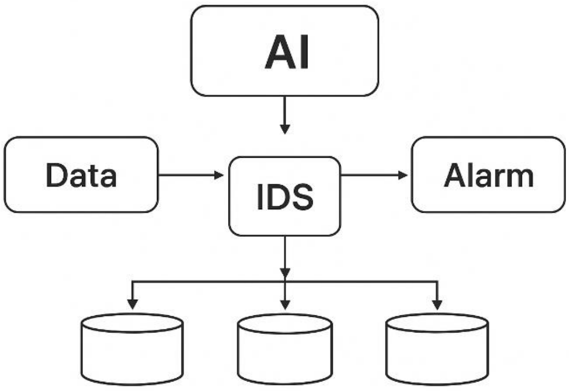

Figure 3: AI-diven IDS (edge-distributed)

3.1 Types of Intrusion Detection Systems

IDS in vehicular IoT can be classified based on detection methodology, deployment architecture, and AI integration.

(a) Signature-Based IDS

These systems detect intrusions by matching observed traffic against a database of known attack signatures. While effective against well-documented threats, they fail against novel or evolving attacks [26].

(b) Anomaly-Based IDS

Anomaly-based IDS models normal network behavior and detects deviations that may indicate malicious activity. AI plays a key role here, as ML algorithms can dynamically update behavioral baselines [27].

(c) Hybrid IDS

Higher detection accuracy and greater adaptability are offered by hybrid intrusion detection systems, which integrate signature-based and anomaly-based techniques [28].

(d) Distributed IDS

Distributed IDS in vehicular IoT use federated learning and edge computing to facilitate cooperative anomaly detection among several cars and roadside units (RSUs). This decentralization improves resilience and scalability.

3.2 AI Techniques in Vehicular IDS

(a) Machine Learning Algorithms

Support Vector Machines (SVMs) are useful for classifying traffic as either malicious or benign.

Random Forests (RF): Effectively manage high-dimensional vehicle traffic data.

Lightweight for real-time intrusion detection systems at the vehicle edge are Naïve Bayes classifiers.

(b) Deep Learning Techniques

Convolutional Neural Networks (CNNs): These networks may identify bogus message insertion by extracting spatial patterns from vehicle traffic flows.

LSTMs and Recurrent Neural Networks (RNNs): Due to their ability to capture temporal correlations in sequential vehicular communication, these technologies are ideal for detecting DoS or Sybil assaults [29].

Autoencoders: Model normal vehicular traffic and detect anomalies by reconstruction error.

(c) Federated and Edge AI

Federated Learning (FL): In order to protect privacy, vehicles work together to train IDS models without exchanging raw data.

Edge AI: Onboard units (OBUs) or RSUs perform inference locally, reducing reliance on distant cloud servers and improving latency [30].

(d) Reinforcement Learning IDS

Reinforcement Learning (RL) enables IDS to dynamically adapt detection policies based on feedback from the environment. For example, an RL-based IDS may adjust thresholds for anomaly detection in response to varying traffic loads [31].

3.3 Applications of AI-Driven IDS in Vehicular IoT

(a) Detection of DoS/DDoS Attacks

AI-driven IDS can identify traffic flooding patterns by analyzing sudden spikes in packet transmission, thereby preventing communication breakdowns.

(b) Spoofing and Sybil Attack Detection

ML classifiers can analyze message consistency (location, speed, trajectory) to distinguish between legitimate and malicious identities.

(c) False Data Injection Attacks

Deep learning models can detect semantic inconsistencies in vehicular messages, such as conflicting speed and location updates.

(d) Insider Threats

AI IDS can identify abnormal driving or communication behaviors even from authenticated vehicles that have been compromised.

(e) Cross-Layer Threats

By combining sensor data with network traffic analysis, AI-based IDS can detect coordinated attacks involving both hardware spoofing and network manipulation.

3.4 Research-Oriented Case Studies

Case Study 1: LSTM-Based IDS for Vehicular Networks

Researchers proposed an LSTM-based IDS to capture sequential dependencies in vehicular communication. The system achieved high detection accuracy against DoS and false data injection attacks in simulated IoV environments [32].

Case Study 2: Federated Learning IDS for Privacy-Preserving Security

Vehicles could jointly train detection models using a federated IDS without sharing raw traffic data. This approach improved scalability and maintained privacy while detecting Sybil and spoofing attacks [33].

Case Study 3: Edge AI for Platooning Security

An edge-deployed IDS was integrated into roadside units for real-time monitoring of platoons. CNNs trained on traffic patterns detected malicious braking commands that could destabilize platoons [34].

3.5 Advantages of AI-Driven IDS

Adaptive Defense: AI IDS adapt to evolving attack strategies.

High Detection Accuracy: Deep learning models capture complex patterns in vehicular traffic.

Scalability: Federated learning and distributed AI scale across large vehicular networks.

Real-Time Responsiveness: Edge AI ensures IDS operate within millisecond-level latency.

Cross-Domain Detection: Capable of integrating data from multiple sources (sensors, communication logs).

3.6 Challenges of AI-Driven IDS in Vehicular IoT

(a) Real-Time Constraints

AI IDS must detect attacks within milliseconds to support collision avoidance or intersection management. Heavy ML models may introduce computational delays [35].

(b) Adversarial Machine Learning

Attackers may craft adversarial inputs to fool AI models, reducing detection accuracy. For instance, carefully perturbed traffic messages may evade anomaly detection.

(c) Resource Limitations

Onboard vehicular devices have limited storage, processing, and energy, restricting the deployment of large deep learning models.

(d) Data Scarcity and Imbalance

Vehicular attack datasets are scarce and often imbalanced, with few attack samples compared to normal traffic. This hampers AI model training.

(e) Privacy Concerns

While federated IDS preserves privacy, communication of model updates can still leak sensitive information about vehicular patterns.

3.7 Future Research Directions

Adversarially Robust IDS: Developing models resilient to adversarial ML attacks.

Lightweight Deep Learning: Deploying energy-efficient AI architectures on OBUs.

Synthetic Dataset Generation: Using generative models to create realistic vehicular attack datasets for IDS training [36].

Blockchain-Integrated IDS: Leveraging blockchain to securely share IDS alerts across vehicles and RSUs.

Explainable AI (XAI): Making IDS decisions interpretable for regulators and manufacturers.

AI-driven IDS represent a critical defense layer in 6G-enabled vehicular IoT. By leveraging machine learning, deep learning, federated learning, and reinforcement learning, IDS can detect both known and emerging threats with high accuracy. Despite challenges in latency, adversarial robustness, and resource limitations, AI-driven IDS remain a cornerstone of next-generation vehicular security.

As vehicular IoT scales to millions of vehicles, future IDS will need to integrate AI, blockchain, and distributed edge architectures to deliver resilient, real-time, and trustworthy protection. This integration is explored in the following section (4.4), where blockchain and AI converge for resilient vehicular security.

4. Integrating Blockchain with AI for Resilient Security

The 6G-enabled Internet of Vehicles (IoV) is envisioned as an ultra-reliable, ultra-low latency, and intelligent ecosystem where autonomous vehicles interact with each other and surrounding infrastructure. However, the convergence of large-scale connectivity, real-time decision-making, and safety-critical communication also introduces multi-layered security risks. Neither blockchain nor artificial intelligence (AI) alone can fully address these threats. Blockchain provides immutable trust and transparency, while AI enables adaptive anomaly detection and prediction. When combined, they form a resilient, decentralized, and intelligent security framework for vehicular networks [37].

This section examines the synergies, applications, architectures, and challenges of blockchain–AI integration in vehicular IoT.

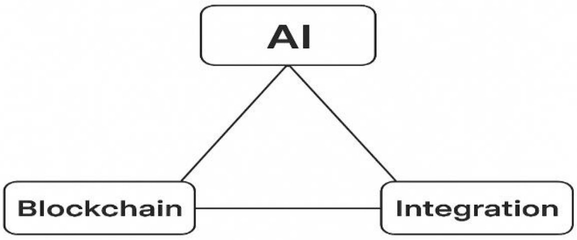

Figure 4: Blockchain-AI Integration Triad

4.1 Synergies Between Blockchain and AI in Vehicular Security

(a) Data Integrity and Trust

Blockchain ensures data authenticity by recording vehicular messages in an immutable ledger.

AI validates the semantic correctness of messages, identifying false data injection or adversarial manipulations. If a malicious vehicle broadcasts a false accident alert, blockchain proves the origin, while AI cross-validates it against other vehicles' sensory inputs.

(b) Collaborative Intrusion Detection

Blockchain secures the exchange of IDS alerts among vehicles and roadside units.

AI ensures real-time threat detection, even in dynamic traffic environments.

(c) Automated Decision-Making

Smart contracts enforce security rules (e.g., granting platoon access only to authenticated vehicles).

AI agents predict malicious behaviors and adjust smart contract parameters adaptively [38].

(d) Privacy Preservation

Blockchain anonymizes vehicular identities through pseudonyms.

AI enhances privacy by applying differential privacy and federated learning, ensuring that raw data is not exposed.

4.2 Architectural Models of Blockchain–AI Integration

(a) Decentralized AI on Blockchain

AI models are trained collaboratively across vehicles (federated learning). Model updates are recorded on blockchain to ensure tamper-proof version control.

(b) Blockchain-Assisted IDS

IDS alerts generated by AI are uploaded to blockchain, allowing all network participants to verify the authenticity of detection results.

(c) Smart Contract-Driven AI Policies

Smart contracts encode AI-based policies, such as automatically adjusting intrusion detection thresholds in response to network congestion or attack intensity.

(d) Edge-Blockchain-AI Triad

At the vehicular edge (OBUs, RSUs), AI provides fast detection, blockchain provides distributed trust, and edge servers coordinate global updates. This triad balances latency, scalability, and reliability.

4.3 Applications of Blockchain–AI Integration in Vehicular IoT

(a) Secure Platooning

Blockchain ensures that only authenticated vehicles can join a platoon, while AI monitors vehicular behaviors to detect anomalies such as malicious braking or lane deviation [39].

(b) Intersection Management

Smart contracts enforce priority and scheduling rules at intersections, while AI predicts traffic patterns to optimize throughput and detect abnormal behavior.

(c) Cooperative Perception

Vehicles share sensor data (LiDAR, radar, cameras) to build a collective situational map. Blockchain ensures provenance, while AI filters out corrupted or poisoned data.

(d) Accident Forensics

Blockchain provides immutable logs of vehicular communication, while AI analyzes patterns to reconstruct accident causes and detect malicious interference.

(e) Secure Over-the-Air (OTA) Updates

Blockchain guarantees the authenticity of OTA software updates, while AI detects anomalies in update distribution (e.g., compromised servers injecting malware).

4.4 Advantages of Blockchain–AI Integration

Resilience: Dual-layer protection against both external and insider threats.

Transparency: Blockchain records enable post-incident audits and accountability.

Adaptability: AI continuously learns from new attack strategies.

Decentralization: Removes reliance on single points of failure.

Efficiency: Smart contracts automate trust enforcement and anomaly responses.

4.5 Challenges in Blockchain–AI Integration

(a) Latency Overhead

Both AI processing and blockchain consensus introduce delays. Achieving sub-millisecond latency remains a critical challenge in time-sensitive vehicular applications [40].

(b) Resource Constraints

AI models and blockchain validation require computational resources, which are limited in onboard vehicular devices. Lightweight architectures are necessary.

(c) Data Quality and Poisoning Attacks

AI IDS depends on high-quality data. Attackers may poison federated learning updates, while blockchain immutably stores poisoned information if not detected.

(d) Scalability

Blockchain transaction volume may explode in large vehicular networks. Sharding and hierarchical blockchain architectures are proposed, but integration with AI at scale is still immature.

(e) Security of Blockchain–AI Itself

Both blockchain and AI introduce their own vulnerabilities. Smart contracts may contain exploitable bugs, and AI remains vulnerable to adversarial examples.

4.6 Research-Oriented Case Studies

Case Study 1: Blockchain-Federated IDS

A blockchain-based federated learning framework was proposed where vehicles collaboratively trained IDS models. Blockchain guaranteed authenticity of model updates, preventing data poisoning [41].

Case Study 2: Smart Contract-Assisted Platooning

Smart contracts managed platoon membership and vehicle behaviors. AI continuously monitored braking patterns, detecting anomalies and triggering smart contract penalties for malicious vehicles [42].

Case Study 3: Blockchain-AI Edge Security

An edge-based vehicular security system combined blockchain consensus with AI IDS to detect DDoS attacks. The hybrid system reduced false positives and improved trust in collaborative detection [43].

The integration of blockchain and AI represents a holistic security paradigm for 6G vehicular IoT. Blockchain establishes decentralized trust, while AI provides adaptive, intelligent intrusion detection. Together, they enable applications such as secure platooning, intersection management, cooperative perception, and forensic accountability.

However, integration also introduces challenges in latency, scalability, and adversarial robustness. Future research must focus on lightweight consensus protocols, adversarially robust AI models, and edge-optimized blockchain–AI architectures. Ultimately, the blockchain–AI synergy is a cornerstone for achieving resilient, transparent, and trustworthy vehicular communication systems in the 6G era.

5. Ethical and Regulatory Considerations

While Sections 4.1–4.4 focused on technical mechanisms such as blockchain, AI, and intrusion detection, security in vehicular IoT cannot be fully addressed through technology alone. The integration of autonomous vehicles, 6G communication, and AI introduces ethical dilemmas and regulatory challenges that determine public trust and acceptance. A highly secure system is meaningless if it lacks legal enforceability, ethical transparency, or societal legitimacy.

This section examines the ethical and regulatory dimensions of vehicular IoT security, including data privacy, accountability, liability, fairness, explainability, and standardization. It also highlights ongoing policy frameworks and suggests future research and governance directions.

5.1 Ethical Dimensions of Vehicular Security

(a) Privacy and Data Protection

Autonomous vehicles generate vast amounts of data: location histories, driving patterns, passenger identities, and even biometric information from onboard sensors. This creates privacy risks if data is collected or shared without informed consent [44].

Risk: Continuous V2X communication enables location tracking, which can reveal personal routines and habits.

Requirement: Privacy-by-design frameworks must be integrated into vehicular IoT, ensuring minimal data collection, anonymization, and encryption.

Ride-hailing services must ensure that drivers' and passengers' identities are not exposed to third parties via vehicular data streams.

(b) Accountability and Liability

One of the most critical ethical issues is determining who is responsible when things go wrong. If an AI-driven car involved in a collision relied on 6G communication for decision-making, accountability could fall on:

The vehicle manufacturer,

The AI software developer,

The network operator, or

The vehicle owner.

This raises the problem of shared liability in cyber-physical systems [45]. Without clear accountability frameworks, public trust in autonomous driving may erode.

(c) Fairness and Non-Discrimination

AI-driven IDS and decision-making models must avoid algorithmic bias. If models are trained on incomplete or biased datasets, they may disproportionately misclassify certain vehicles or environments as risky [46]. If traffic data from urban areas dominates training, IDS may underperform in rural contexts, potentially mislabeling legitimate behaviors as malicious.

Thus, fairness must be embedded into AI-based vehicular security systems to ensure equitable treatment across diverse users and geographies.

(d) Transparency and Explainability

AI models in vehicular IDS and decision-making are often black boxes, making it difficult to understand why a vehicle flagged an anomaly or executed a maneuver. Lack of transparency undermines trust.

Solution: Explainable AI (XAI) approaches are required to make IDS outputs interpretable for regulators, insurers, and drivers [47].

Impact: Transparent explanations also support legal investigations in the event of disputes.

(e) Ethical Dilemmas in Autonomous Driving

Autonomous vehicles may face moral dilemmas, such as the "trolley problem"—deciding between two harmful outcomes. Security systems must ensure that adversarial manipulation does not exploit these dilemmas. Moreover, the ethical principles guiding vehicular AI must be aligned with societal values, such as prioritizing human life over property.

5.2 Regulatory Considerations

(a) Standardization of Vehicular Security Protocols

To ensure interoperability, vehicular networks require globally accepted standards. Current frameworks include:

IEEE 1609.2: Security services for vehicular environments.

ETSI ITS-G5: European standard for Intelligent Transportation Systems.

3GPP Release 16/17: Standards for 5G-V2X communication, which will extend to 6G [48].

However, none fully address blockchain–AI integration or federated IDS frameworks, highlighting the need for updated standards.

(b) Data Protection Laws

Regional laws regulate vehicular data privacy:

General Data Protection Regulation (GDPR) in Europe requires consent for data collection and provides users with rights to erase their data.

California Consumer Privacy Act (CCPA) provides similar protections in the United States.

For vehicular IoT, compliance means ensuring anonymization of V2X communication while still preserving safety-critical information [49].

(c) Certification and Compliance

Vehicles must undergo security certification before deployment. Regulatory agencies may mandate:

Compliance with vehicular IDS performance benchmarks.

Certification of blockchain-based trust models.

Verification of AI transparency and fairness.

(d) Legal Liability Frameworks

Governments must define liability in case of:

Cyberattacks causing accidents,

Malicious broadcasting of false alerts, or

System failures due to AI or blockchain malfunctions.

Insurance models may need to evolve toward shared liability pools involving manufacturers, operators, and owners.

(e) Cross-Border Regulatory Challenges

Vehicles often travel across borders. Differing regulatory standards between countries create fragmentation. An autonomous car secure under European standards may not meet U.S. or Asian compliance requirements. Harmonization of vehicular security regulations is essential for global adoption [50].

5.3 Future Governance and Policy Directions

Blockchain Governance Models: Establish rules for validator selection, smart contract auditing, and dispute resolution in vehicular blockchains.

AI Auditing Frameworks: Mandate regular fairness, robustness, and transparency checks for vehicular IDS.

Ethics-by-Design: Embed ethical principles (privacy, accountability, fairness) directly into vehicular software architectures.

Global Regulatory Collaboration: Develop unified 6G vehicular IoT standards under international organizations such as ITU or ISO.

Dynamic Regulatory Sandboxes: Enable real-world testing of vehicular IoT security under controlled regulatory environments before large-scale deployment.

In order to create safe and reliable automotive IoT ecosystems, ethical and regulatory factors are just as important as technical ones. Alongside blockchain and AI integration, concerns like privacy, responsibility, justice, and transparency need to be addressed.

Gaining public trust and regulatory approval for 6G-enabled vehicle systems requires clear legal frameworks, updated global standards, and ethics-by-design strategies. Ultimately, public acceptance and the legitimacy of government are just as important to the success of autonomous transportation as technical robustness.

A pseudo code framework is described below to illustrate the deployment of AI-driven models for intrusion detection in edge-distributed vehicle networks. The technique mimics the process of training intrusion detection data locally at several edge nodes before aggregating the results for use in global decision-making.

Our Contributions of this article are as follows,

- Gives a comprehensive taxonomy of 6G security threats to vehicles backed up with a real-world case study.
- Creates a detailed study of the blockchain based trust, authentication and data integrity systems.
- Suggests AI-based IDS models with deep learning, federated learning and reinforcement learning to detect dynamic threats.
- Presents a combined blockchain and intelligent platform that allows decentralized and robust vehicular security.
- Offers ethical, regulatory and governance guidelines necessary in safe implementation of autonomous vehicles systems.

6. Results and Discussion

Pseudo Code: AI-driven IDS (Edge-distributed Simulation)

```
BEGIN
1. Generate synthetic intrusion detection dataset:
  - Create 3000 samples with 15 features
  - Labels: Benign or Malicious (binary classes)
  - Training/Test split (70% / 30%)
2. Distribute training data across 3 edge nodes:
  - Split training set into 3 equal partitions
  - Each edge node holds its local data and labels

3. Train IDS model on each edge node:
  FOR each edge node i in {1, 2, 3}:
     - Initialize Random Forest classifier with 50 trees
     - Train classifier on local data (edge_data[i])
     - Store trained model
     - Predict on local data
     - Compute local accuracy
     - Save accuracy for reporting
  END FOR
4. Aggregate models (ensemble voting at edge/cloud):
  - Initialize probability matrix with zeros
  - FOR each trained model:
        - Predict probabilities on global test set
        - Add probabilities to matrix
    END FOR
  - Average probabilities across models
  - Final prediction = class with highest probability
5. Evaluate performance of aggregated IDS:
  - Compute confusion matrix between predicted and true labels
  - Plot confusion matrix (Benign vs. Malicious)
  - Compute ROC curve (True Positive Rate vs False Positive Rate)
  - Calculate Area Under Curve (AUC)
  - Plot ROC curve with AUC
  - Plot bar chart of accuracy for each edge node model
END
```

The pseudo code begins with the generation of a synthetic intrusion detection dataset, which is then partitioned across three edge nodes. Each node independently trains a Random Forest classifier, after which predictions are aggregated at the edge/cloud using ensemble voting. The final evaluation includes confusion matrix analysis, ROC curve plotting, and per-node accuracy reporting.

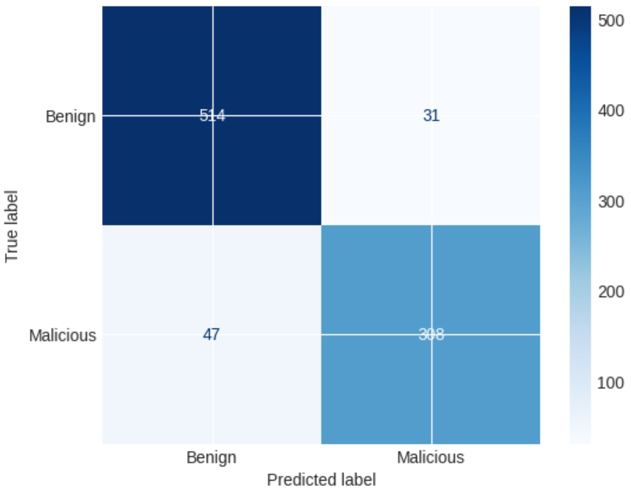

Figure 5: Confusion Matrix – Aggregated IDS

The clarity of the aggregated IDS's ability to differentiate between hostile and benign traffic is demonstrated by the confusion matrix. Correct classifications are represented by the diagonal cells, while off-diagonal cells show misclassifications. A high number of true positives and true negatives indicates reliable detection performance, whereas false positives suggest benign traffic wrongly flagged as attacks, and false negatives reflect missed detections. Eliminating false negatives is crucial in security since undetected attacks are very dangerous. Researchers can evaluate the strengths and limitations of the classifier using this graph, which provides clear insights into the operational dependability, accuracy, and balance of the AI-driven IDS in vehicular networks.

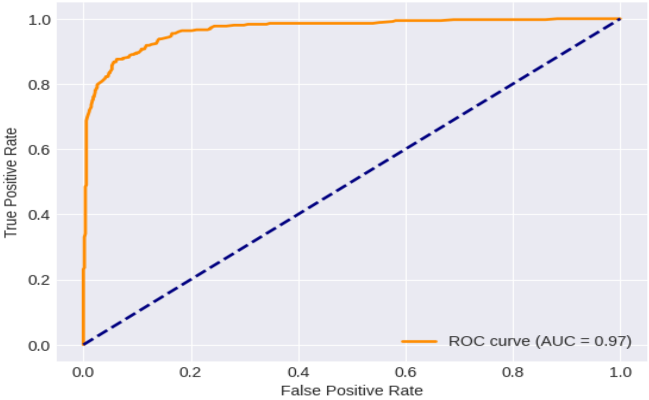

Figure 6: ROC Curve – Aggregated IDS

The Receiver Operating Characteristic (ROC) curve shows the trade-off between true positive rate (TPR) and false positive rate (FPR) for the aggregated IDS. Stronger discriminative power is shown by a curve toward the upper-left corner. This performance is measured by the Area Under Curve (AUC), where values close to 1.0 signify extremely successful intrusion detection. This graphic aids in evaluating the resilience of the model at different thresholds, particularly when it comes to separating malicious activity from genuine traffic. The ROC curve offers a useful standard for evaluating IDS models and their performance in real-world deployment circumstances because vehicular systems require both high sensitivity and minimal false alarms.

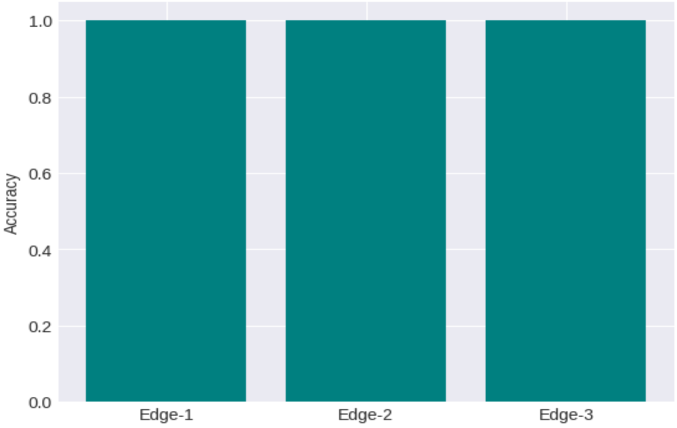

Figure 7: Accuracy per Edge Node IDS

The detection accuracy attained by each edge node after being separately trained on its local dataset is displayed in this bar chart. All nodes attain excellent accuracy, validating the model's dependability, albeit the minor discrepancies across nodes represent variations in the local data distribution. Since no single node dominates detection capability, displaying edge-level performance guarantees transparency in distributed IDS deployment. Such outcomes demonstrate that even lightweight models at the edge can attain respectable accuracy in real-world scenarios. In 6G vehicular networks, where scalability, low-latency detection, and cooperative defense methods are essential to system robustness, this supports the argument for distributed IDS systems.

7. Conclusion

This article confirms that the holistic approach is necessary to ensure the realization of 6G-enabled vehicular IoT that produces technical resilience and ethical and regulatory readiness. Vehicular networks are used in mission-critical environments, a failure of which may cause loss of life, economic instability, and reputation. As the analysis shows, the threats at all levels are not limited to spoofing and false data injection; DoS attacks, privacy breaches, and hardware attacks are also required, and multi-layered defenses will be necessary. Blockchain becomes a root facilitator of decentralized trust, offering unchangeable identity management, records that are immutable and smart contracts that are automated. At the same time, AI-enhanced intrusion detection systems can be used to provide adaptable, intelligent and real-time detection of threats, which is beyond the capabilities of the conventional signature-based systems. The combination of blockchain and AI will establish a strong security paradigm where the trust, integrity, and anomaly detection are effectively connected on the edge and vehicular layer and on the cloud layer. Nonetheless, issues of latency, adversarial machine learning, scalability and resource constraints are major challenges that need to be overcome by use of lightweight consensus, robust AI, and optimized edge architectures. The ethical issues, including fairness, transparency, privacy, and liability, are also important in order to make sure that the society is acceptable and adheres to the regulations. With the increase in the vehicle level of IoT worldwide, coordinated standards and ethics-by-design models will be significant. Conclusively, decentralized security, trustful AI, and good governance are the keys to the future of intelligent transportation to create safe, transparent, and resilient mobility ecosystems.

References

[1] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. Journal of Network and Computer Applications, 37, 380–392. (https://doi.org/10.1016/j.jnca.2013.02.036)

[2] Hartenstein, H., & Laberteaux, K. (2008). A tutorial survey on vehicular ad hoc networks. IEEE Communications Magazine, 46(6), 164–171. (https://doi.org/10.1109/MCOM.2008.4539481)

[3] Rawat, D. B., & Popescu, D. C. (2015). Enhancing VANET performance by joint adaptation of transmission power and contention window size. IEEE Transactions on Parallel and Distributed Systems, 26(12), 3349–3360. (https://doi.org/10.1109/TPDS.2014.2381666)

[4] Wang, Q., & Jiang, J. (2018). Comparative examination on architecture and protocol of VANET. International Journal of Distributed Sensor Networks, 14(2), 1–12. (https://doi.org/10.1177/1550147718758395)

[5] Lu, R., Lin, X., Zhu, H., Ho, P. H., & Shen, X. (2012). ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. IEEE INFOCOM 2012, 1229–1237. (https://doi.org/10.1109/INFCOM.2012.6195491)

[6] Raya, M., & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39–68. (https://doi.org/10.3233/JCS-2007-15103)

[7] Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Proceedings of the Institute of Navigation GNSS, 55(5), 2314–2323.

[8] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015 Conference.

[9] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. Proceedings of the IEEE, 104(6), 1258–1270. (https://doi.org/10.1109/JPROC.2016.2526658)

[10] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems (NeurIPS), 27, 2672–2680.

[11] Yang, Z., Yu, R., Zhang, Y., Yang, Y., & Zhang, Y. (2019). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495–1505. (https://doi.org/10.1109/JIOT.2018.2872076)

[12] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from (https://bitcoin.org/bitcoin.pdf)

[13] Zeng, J., & Cai, Z. (2020). Blockchain security in vehicular networks: A survey. Digital Communications and Networks, 6(2), 139–147. (https://doi.org/10.1016/j.dcan.2019.06.001)

[14] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data, 557–564. (https://doi.org/10.1109/BigDataCongress.2017.85)

[15] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. (https://doi.org/10.1109/ACCESS.2016.2566339)

[16] Li, C., Wang, H., Xu, X., & Wang, Y. (2018). A blockchain-based authentication and security mechanism for vehicular ad hoc networks. IEEE International Conference on Communications (ICC), 1–6. (https://doi.org/10.1109/ICC.2018.8422343)

[17] Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., & Zhang, Y. (2019). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 6(3), 4660–4670. (https://doi.org/10.1109/JIOT.2018.2875542)

[18] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the 13th EuroSys Conference, 1–15. (https://doi.org/10.1145/3190508.3190538)

[19] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432–1465. (https://doi.org/10.1109/COMST.2020.2969702)

[20] Wu, J., Gai, K., & Zhu, L. (2021). Blockchain-based secure communications for vehicular networks. Future Generation Computer Systems, 119, 1–12. (https://doi.org/10.1016/j.future.2021.01.011)

[21] Liu, B., & Li, W. (2021). Blockchain-enabled secure intersection management in vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4038–4051. (https://doi.org/10.1109/TITS.2020.2996721)

[22] Sharma, P. K., Park, J. H., & Yang, C. (2019). Blockchain-based distributed framework for secure and trusted cooperative driving. IEEE Transactions on Intelligent Transportation Systems, 20(8), 3332–3342. (https://doi.org/10.1109/TITS.2018.2884715)

[23] Xu, C., Liu, J., Zhang, Z., & Zhang, F. (2020). Blockchain-assisted vehicle forensics in intelligent transportation systems. IEEE Transactions on Vehicular Technology, 69(6), 5711–5723. (https://doi.org/10.1109/TVT.2020.2989399)

[24] Pahlavan, K., & Krishnamurthy, P. (2021). Principles of wireless networks: A unified approach. John Wiley & Sons.

[25] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication 800-94.

[26] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16–24. (https://doi.org/10.1016/j.jnca.2012.09.004)

[27] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. (https://doi.org/10.1109/COMST.2015.2494502)

[28] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. (https://doi.org/10.1016/j.jnca.2015.11.016)

[29] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. (https://doi.org/10.1109/ACCESS.2017.2762418)

[30] Lim, W. Y. B., Xiong, Z., Niyato, D., Yang, Q., & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 2031–2063. (https://doi.org/10.1109/COMST.2020.2986024)

[31] Gao, X., Liu, Z., & Liu, Z. (2019). Reinforcement learning for network security: A survey. IEEE Access, 7, 188573–188602. (https://doi.org/10.1109/ACCESS.2019.2959776)

[32] Kim, J., Kang, J., Kim, D., & Kim, H. (2020). Long short-term memory-based intrusion detection system for vehicular networks. Sensors, 20(23), 7087. (https://doi.org/10.3390/s20237087)

[33] Pokhrel, S. R., & Choi, J. (2020). Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. IEEE Transactions on Communications, 68(8), 4734–4746. (https://doi.org/10.1109/TCOMM.2020.2990735)

[34] Li, Z., Tang, J., & Wang, Y. (2020). Intelligent edge defense for secure vehicular platooning. IEEE Internet of Things Journal, 7(5), 4000–4010. (https://doi.org/10.1109/JIOT.2020.2964351)

[35] Sun, J., Wang, Y., & Dai, J. (2020). Lightweight intrusion detection for vehicular networks. Ad Hoc Networks, 106, 102240. (https://doi.org/10.1016/j.adhoc.2020.102240)

[36] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167. (https://doi.org/10.1016/j.cose.2019.06.005)

[37] Kumar, N., Zeadally, S., & Rodrigues, J. J. P. C. (2020). Vehicular delay-tolerant networks for smart grid data management using blockchain and AI. IEEE Transactions on Industrial Informatics, 16(7), 4661–4670. (https://doi.org/10.1109/TII.2019.2949493)

[38] Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., ... & Kim, D. I. (2021). Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things Journal, 8(1), 18–43. (https://doi.org/10.1109/JIOT.2020.3000447)

[39] Li, H., Pei, Q., Luan, T. H., Gao, L., & Zheng, X. (2019). Blockchain meets AI: Opportunities and challenges. IEEE Network, 33(6), 58–64. (https://doi.org/10.1109/MNET.001.1900107)

[40] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchain in Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1676–1717. (https://doi.org/10.1109/COMST.2018.2886932)

[41] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics, 16(6), 4177–4186. (https://doi.org/10.1109/TII.2019.2941971)

[42] Sun, Y., Zhang, R., Xie, S., Yu, F. R., & Leung, V. C. M. (2020). Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node

deployment. IEEE Internet of Things Journal, 7(8), 7489–7503. (https://doi.org/10.1109/JIOT.2020.2974829)

[43] Xu, R., Li, C., & Liu, J. (2019). Smart contract-based edge computing resource allocation for vehicular networks. IEEE Transactions on Industrial Informatics, 15(7), 4214–4226. (https://doi.org/10.1109/TII.2019.2897900)

[44] Tselentis, D., Yannis, G., & Vlahogianni, E. I. (2020). Innovative vehicle applications and their impact on road safety. Transportation Research Procedia, 48, 1872–1883. (https://doi.org/10.1016/j.trpro.2020.08.225)

[45] Stilgoe, J. (2018). Machine learning, social learning and the governance of self-driving cars. Social Studies of Science, 48(1), 25–56. (https://doi.org/10.1177/0306312717741687)

[46] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM Computing Surveys, 54(6), 1–35. (https://doi.org/10.1145/3457607)

[47] Gunning, D., & Aha, D. (2019). DARPA’s explainable artificial intelligence (XAI) program. AI Magazine, 40(2), 44–58. (https://doi.org/10.1609/aimag.v40i2.2850)

[48] Araniti, G., Campolo, C., Condoluci, M., Iera, A., & Molinaro, A. (2013). LTE for vehicular networking: A survey. IEEE Communications Magazine, 51(5), 148–157. (https://doi.org/10.1109/MCOM.2013.6515060)

[49] Kosta, E., Marinos, A., & Christou, E. (2020). Privacy by design in connected vehicles: Legal perspectives and challenges. Computer Law & Security Review, 36, 105381. (https://doi.org/10.1016/j.clsr.2019.105381)

[50] Papadimitratos, P., La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S. (2009). Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE Communications Magazine, 47(11), 84–95. (https://doi.org/10.1109/MCOM.2009.5307471)