Al-Nahrain Journal for Engineering Sciences

Al-Nahrain J. Eng. Sci. 29(2) 301-312, 2026
Original Article

Towards Next-Generation Autonomous Vehicle Communication in Smart Cities: A Blockchain and AI Perspective

Tanweer Alam[1]•

1Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia

•*These authors contributed equally to this work*

DOI: https://www.doi.org/10.29194/NJES.29020301

Received: Aug 9, 2025 **Revised:** Nov. 14, 2025 **Accepted:** April 6, 2026 **Published: June** 20, 2026

Abstract

Autonomous vehicles (AVs) rely on continuous vehicle-to-vehicle (V2V) and vehicle-to-everything (V2E) communication to support shared perception, traffic direction, and decision making. Integrating real-time data, connectivity, and precise navigation will revolutionize urban mobility by facilitating sustainable, secure, and highly efficient transportation options. The rapid evolution of AVs within smart cities necessitates robust and secure data transmission methods to ensure efficient and safe operations. This paper proposes a next-generation communication framework that integrates blockchain with artificial intelligence (AI) to enable secure, decentralized, and adaptive AVs network. Blockchain is employed as a distributed trust layer to ensure data immutability, decentralized identity management, and transparent transaction validation among vehicles and roadside infrastructure. AI techniques are incorporated to support intelligent threat detection, dynamic resource allocation, anomaly identification, and context-aware decision making. The integration between blockchain and AI enhances trust establishment while maintaining system scalability and real-time responsiveness. The proposed architecture introduces a layered design that separates communication, consensus, and intelligence components, allowing efficient integration with edge computing and 5G-enabled vehicular environments. This research contributes a unified conceptual framework for secure and intelligent autonomous vehicle communication, highlighting how blockchain and AI can jointly address critical limitations in next-generation vehicular networks and support the evolution of trustworthy, resilient, and scalable smart mobility ecosystems.

Keywords: *Blockchain, Federated Learning, Reinforcement Learning, AVs, Smart Cities, Secure Data Transmission, Intelligent Transportation Systems.*

Corresponding author: Provide the corresponding author information and publisher here. E-mail address: tanweer03@iu.edu.sa

1. Introduction

AVs represents a transformative technology with the potential to reshape urban transportation systems and improve road safety, traffic efficiency, and environmental sustainability [1]. However, the widespread adoption of AVs hinges on addressing key challenges, including secure data transmission among vehicles, and protecting user privacy [2]. Traditional centralized approaches to data transmission and model training pose inherent security and privacy risks, such as single points of failure and data exposure to malicious actors. This research proposes a novel approach, Blockchain-Based Federated Reinforcement Learning (FRL), to overcome these challenges. By leveraging blockchain technology, Federated Learning (FL) methodologies, and Reinforcement Learning (RL) techniques, this approach enables secure, collaborative model training among AVs while preserving data privacy and integrity. It presents the system architecture, data transmission protocol, and security mechanisms of the FRL system.

The following are the components of the proposed framework.

1. Smart City Environment: Represents the urban environment where AVs operate, including roads, traffic signals, and infrastructure.
2. AVs Layer: This layer consists of AVs equipped with sensors, processors, and communication modules for data collection and transmission.
3. FL: Facilitates collaborative model training among AVs while preserving data privacy and decentralisation.
4. RL: Employs RL algorithms to enable AVs to learn optimal driving policies and decision-making strategies.
5. Blockchain Network: This network provides a decentralised and immuta-ble ledger for recording transactions, consensus agreements, and model updates.
6. Data Transmission: Encompasses secure and efficient data transmission, including encrypted model updates and sensor data, among AVs, FL components, and the blockchain network.

Figure 1 demonstrates how Blockchain-Based FRL integrates with AVs, FL, RL, and blockchain technology to enable secure data transmission and collaborative model training in smart city environments.

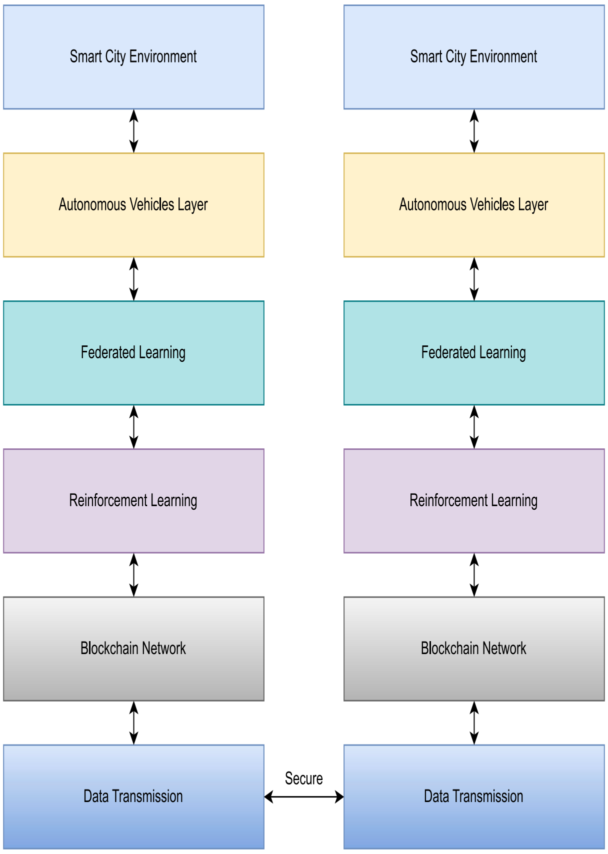

Figure 1. Blockchain-Based FRL Model for Secure Data Transmission among AVs in Smart Cities

1.1. Contribution

Blockchain technology facilitates safe and decentralized governance and retention of data by limiting access exclusively to authorized users. Utilizing blockchain technology to verify agent decisions and activities will enhance transparency in the RL process. In addition, blockchain technology can enhance agent accountability by implementing a decentralized governance framework for distributed RL. FL is a decentralized approach to training machine learning models. The system will protect data privacy and security by combining blockchain technology, FL, and RL approaches. The FRL system exhibits the ability to scale and handle several AVs and an increased amount of data in real-world smart city environment [3-5]. It enhances the security of data exchange between AVs in smart cities by guaranteeing confidentiality and protection of data and promoting cooperation. It also improves the functionality of smart transportation, leading to more secure and efficient urban mobility. Blockchain-based FRL algorithm is implemented and tested.

1.2. Motivation

The motivation behind exploring Blockchain-Based FRL for secure data transmission among AVs in smart cities is from several key factors:

1) Data Privacy Concerns: Traditional centralised approaches to data transmission in AV networks raise significant privacy concerns [6]. Centralized servers require access to raw sensor data from all participating vehicles, which poses risks of data breaches, unauthorized access, and privacy violations. Motivated by the need to preserve user privacy and comply with data protection regulations, there is a growing demand for decentralized and privacy-preserving solutions.

2) Security Risks: Centralized data transmission architectures are susceptible to single points of failure and targeted cyber-attacks. Decentralizedon of decentralized and distributed data transmission and model training techniques is driven by a goal to improve security and resilience in AV networks.

3) FL offers a promising approach to collaborative model training while decentralizing data and preserving privacy. FL preserves data privacy and reduces communication costs by aggregating model updates locally and sharing only encrypted global models.

4) Blockchain technology provides a decentralized and immutable ledger for recording transactions and consensus agreements. By leveraging blockchain technology, AV networks can enhance trust, transparency, and accountability in data transmission and model training activities.

5) AVs are integral to smart city initiatives to create more sustainable, livable, and connected urban environments. The motivation to advance AVs' capabilities and enable seamless integration into smart city ecosystems drives the exploration of innovative technologies, such as Blockchain-Based FRL, for secure data transmission among AVs in smart cities.

1.3. Challenges

An AV is a vehicle capable of perceiving its environment, analyzing that data, and operating safely without any human involvement [7]. AVs have the potential to significantly transform urban transportation networks by offering safer, more efficient, and environmentally friendly means of transportation. To achieve this objective, it is necessary to address supplementary considerations, like ensuring secure data transmission between self-driving vehicles and safeguarding user privacy. In the context of intelligent urban environments, this proposed technique examines the capacity of Block-chain-based FRL to tackle these difficulties.

The proposed model enhances the security and collaboration of AV model training while also safeguarding the integrity and confidentiality of data. This is achieved using blockchain, FL, and RL methods. This study examines a Blockchain-Based FRL system's design, implementation, and evaluation, assessing its effectiveness, scalability, and practicality in innovative urban settings. The manuscript enhances the comprehension and implementation of FRL for safe data transfer among AVs in smart cities through theoretical analysis, simulated research, and practical tests. The introduction of AVs is set to completely transform transportation systems into smart cities, providing improved safety, efficiency, and convenience.

1.4. Research questions and research gap

This paper proposes a novel approach integrating blockchain, and AI techniques such as FRL to enhance secure data transmission among AVs in smart cities. By addressing key issues related to data integrity, privacy, and real-time decision-making, this approach aims to provide a robust and scalable solution for intelligent transportation systems. The following are the research questions. How can blockchain technology be effectively integrated with AI to ensure secure and transparent data transmission among AVs in smart cities? What are the key challenges and opportunities associated with implementing blockchain-based FRL systems for AVs in dynamic urban environments? Despite significant advancements in AV technology and smart city infrastructure, there remains a notable research gap in integrating blockchain and AI for secure data transmission among AVs in smart cities. While individual components such as blockchain, FL, and RL have been studied extensively in various contexts, their synergistic application tailored explicitly for AVs in smart city environments is relatively unexplored.

1.3. Organization

The rest of the paper is organized as follows. Section 2 represents the related works; Section 3 represents the framework; Section 4 represents the methodology; Section 5 shows the results; Section 6 represents the discussion; and Section 7 represents the conclusion.

2. Related Works

The related works in the field of blockchain-based FRL for secure data transmission among AVs in smart cities encompass various research efforts and technological advancements aimed at addressing the challenges of data management, security, and privacy in dynamic urban environments. The following are the related vital areas:

2.1. Blockchain Technology in Smart Cities

Several studies have explored the application of blockchain technology in smart city contexts, focusing on data integrity, transparency, and decentralized governance. These works provide insights into the potential benefits and challenges of integrating blockchain into urban infrastructure, including transportation systems. Blockchain is an emerging technology that combines decentralization and smart contracts to ensure security. Blockchain technology enhances the security of obtained sensitive information. The proposed approach utilizes blockchain technology in a novel way to ensure the confidentiality, integrity, and reliability of traffic data.

2.2. FL for Privacy-Preserving Collaboration

FL is a decentralized ML approach that ensures user data confidentiality by training models on individual devices. FL facilitates the transfer of data training to edge de-vices, enabling individuals to train model parameters using actual data from the real world. Data owners engage in FL by independently updating crucial model parameters using their own data and incorporating them into a global data model. In order to train a global model, a central server aggregates all local updates. Data privacy is preserved by exclusively sharing the model parameters among several data owners.

2.3. RL for Avs

RL allows an agent to learn from its surroundings through active exploration and interaction. With RL, as the agent acquires experience and receives feedback from the system, it gradually improves its control rules. In this scenario, the autonomous vehicle acts as an actor. Blockchain-enabled FRL framework allows AVs to address real-time obstacles effectively and promptly.

2.4. Secure Data Transmission in Intelligent Transportation Systems

Data transmission refers to the process of transferring information from one place to another. Secure transmission refers to the procedure of conveying data, particularly confidential or private information, using an encrypted channel. Various types of secure communication require encryption to some extent. This method is frequently employed to encrypt data stored on devices and sensitive data communicated over the internet. Implementing robust data encryption methods is crucial to prevent security breaches and unauthorized intrusion.

2.5. Privacy-Preserving Techniques for AV Data Sharing

AVs may be confident that their PII is safe when processed and transmitted to service providers or applications utilizing privacy-preserving technology, enabling marketers to continue utilizing data-driven solutions. There are several methods to guarantee data privacy, such as restricting access to prevent unauthorized individuals from accessing data, gaining consent from data subjects when necessary, and maintaining data integrity. It is imperative for all organizations to give utmost importance to the protection of their customers' personal information. Violations of data privacy can lead to substantial financial losses.

2.6. Simulation and Validation Studies

Simulation-based studies and validation trials are essential for evaluating the practicality and effectiveness of blockchain-based FRL techniques for AVs in smart cities. With its decentralized and immutable ledger, blockchain technology offers a promising way to tackle security and trust concerns. By utilizing blockchain technology, data transmission between AVs may be securely and permanently recorded, ensuring the accuracy and openness of the information. However, blockchain integration alone cannot meet all the requirements of a dynamic and data-intensive environment like smart cities.

Existing research primarily focuses on isolated aspects of data management, security, or learning algorithms within AV systems. Few studies have comprehensively addressed the challenges associated with secure and efficient data transmission among AVs in dynamic urban environments. Moreover, integrating blockchain technology with federated and RL techniques in this context is an exciting area of research. However, the frameworks and simulations provide valuable insights, and real-world deployment and validation of blockchain-based FRL systems for AVs in smart cities are limited. Furthermore, the impact of environmental factors, such as varying traffic conditions, infrastructure constraints, and regulatory frameworks, on the effectiveness of such systems is not adequately explored.

Table 1 provides a comparative overview of the approaches and key findings of the current study and previous studies in the same domain.

Table 1. Related Works

Ref.	Authors	Year	Approach	Key Findings
[8]	Lu et al.	2020	Blockchain-Based FL	Improved secure data sharing on the internet for vehicles.
[9]	Zhang et al.	2022	Blockchain-Based FDRL	Secure cloud-edge-end collaboration in power IoT.
[10]	Qi et al.	2018	FRL	Challenges to implement FRL.
[11]	Lu et al.	2020	Blockchain-Based FL	1. Improve communication efficiency for digital twin-edge networks.
[12]	Demertzis	2021	Blockchain-Based FL	1. Enhanced threat defense.
[13]	Li et al.	2022	Blockchain-Based FL	1. Improve security in distributed machine learning systems.
[14]	Kumar et al.	2021	Blockchain-Based ML	1. Enhance privacy-preserving secured framework for sustainable smart cities.
[15]	Djenouri et al.	2023	Federated Deep Learning (FDL)	1. Implement smart city edge-based applications.
[16]	Miao et al.	2021	FDRL	1. Secure data sharing for IoT.
[17]	Ramu et al.	2022	FL	1. Present a comprehensive survey on integrating FL with Digital Twin.
[18]	Al-Huthaifi et al.	2023	FL	1. Privacy and security survey.
[19]	Guo et al.	2022	Blockchain-Based FL	1. Data security sharing mechanism over the smart city.
[20]	Li et al.	2022	Blockchain-Based FL	1. Discuss the privacy and security issues in smart environments.
[21]	Moniruzzaman et al.	2023	Blockchain-Based FRL	1. Improve communication in Vehicle-to-Everything in Smart Grids.
[22]	Issa et al.	2023	Blockchain-Based FL	1. A survey to secure the IoT.
[23]	Abbas et al.	2021	Blockchain	1. Convergence of blockchain and IoT for secure transportation systems in smart cities.
[24]	Choo et al.	2021	Blockchain	1. Enhance secure communications in smart cities.
[25]	Pokhrel et al.	2020	Blockchain-Based FL	1. Analysis and design challenges for AVs:
[26]	Qammar et al.	2023	Blockchain-Based FL	1. Securing FL with blockchain.
[27]	Moore et al.	2023	Blockchain-Based FL	1. A survey on secure and private data communication in resource-constrained computing.
[28]	Devarajan et al.	2023	Vehicular networks	1. An integrated security approach for vehicular networks in smart cities.
[29]	Sharma et al.	2022	Blockchain-Based FL	1. Secure and privacy-preserving computing architecture for IoT networks.
[30]	Haddaji et al.	2022	Blockchain-Based FL	1. Trust management in IoV.
[31]	Qi et al.	2021	Blockchain-Based FL	1. Privacy-preserving for traffic flow prediction.
[32]	Kakkar et al.	2022	Blockchain	1. Secure and trusted data sharing scheme for AVs.
[33]	Otoum et al.	2020	Blockchain-Based FL	1. Enhance security in vehicular networks.
[34]	Ullah et al.	2024	Blockchain-Based FL	1. Secure and Efficient Data Sharing.
[35]	Saraswat et al.	2022	Blockchain-Based FL	1. Solve privacy and security issues
[36]	Tiba et al.	2020	Blockchain-Based FL	1. Enhance security in traffic load balancing.
[37]	Singh et al.	2022	Blockchain-Based FL	1. Improve privacy-preserved IoT-enabled smart vehicular networks.
[38]	Iordache et al.	2024	Blockchain and AI	1. Enhancing Autonomous Vehicle Safety
[39]	Gebrezgiher et al.	2025	Machine Learning based Blockchain	1. Improve security in V2X communication
[40]	Jaiswal et al.	2025	Internet of Vehicles	1. Discover challenges in Internet of Vehicles
[41]	Heidari et al.	2026	AI in Internet of Vehicles	1. Enhanced the privacy preservation in the internet of vehicles.
Proposed study	Alam	2026	Blockchain-Based FRL	2. Improved data transmission security among AVs 3. Enhanced privacy preservation Efficient utilization of resources through FRL

3. Framework

AVs offer numerous benefits, including reduced traffic congestion, improved road safety, and enhanced mobility for individuals with disabilities or limited mobility [42]. Smart city initiatives leverage emerging technologies like the IoT, AI [43], and block-chain to create more sustainable, convenient, and connected urban environments [44]. Blockchain is a decentralized, immutable ledger that enables secure and transparent transactions among multiple parties without intermediaries. Its key features, including decentralization, transparency, and cryptographic security, make it well-suited for applications requiring trust, accountability, and data integrity [45-47]. FL is a distributed machine learning approach that allows multiple devices to train a shared model collaboratively while keeping data decentralized and private. FL preserves data privacy and reduces communication costs by aggregating model updates locally and sharing only encrypted gradients with a central server. RL is a machine learning paradigm where an agent learns to interact with an environment to maximize cumulative rewards over time. RL has been successfully applied to various domains, including robotics, gaming, and autonomous systems, to learn complex behaviors and decision-making strategies. Integration of Blockchain, FL, and RL offers a promising approach to addressing the challenges of secure data transmission among AVs in smart cities [48]. Blockchain ensures data integrity and transparency, FL preserves data privacy, and RL enables AVs to learn optimal driving policies in dynamic environments [49-50]. Security and privacy mechanisms are paramount in ensuring data transmission integrity, confidentiality, and trustworthiness among AVs in smart cities when employing Blockchain-based FRL.

3.1. Blockchain Encryption and Authentication

a. Secure transactions recorded on the blockchain using cryptographic techniques, such as asymmetric encryption and digital signatures.

b. Authenticate participants and ensure data integrity by validating digital signatures and verifying the authenticity of transactions.

3.2. Privacy-Preserving FL

a. The federated averaging, secure aggregation, and differential privacy are implemented to preserve individual AVs' data privacy during model training.

b. The FL protocols allow AVs to train a global RL model without sharing raw sensor data or the central server.

3.3. End-to-End Encryption

a. Encrypted data transmissions between AVs, FL servers, and the blockchain network.

b. Ensure data is encrypted at rest and in transit, preventing unauthorized access and eavesdropping.

3.4. Access Controls and Identity Management

a. Implement access control mechanisms to restrict access to sensitive data and system resources based on user roles and permissions.

b. Utilize identity management systems, such as digital certificates or decentralized identifiers, to authenticate and authorize AVs within the network.

3.5. Smart Contract Security

a. Develop secure smart contracts to govern interactions between AVs and the blockchain network, enforcing predefined rules and protocols.

b. Perform thorough code reviews, testing, and auditing to identify and mitigate potential security vulnerabilities.

3.6. Data Minimization and Anonymization

a. Adhere to the principle of data minimization and minimize the amount of personally identifiable information collected and stored by AVs.

b. Anonymize data whenever possible to reduce the risk of deanonymization attacks and protect user privacy.

3.7. Auditing and Logging

a. Implement comprehensive logging mechanisms to record all transactions, model updates, and system activities for auditing and forensic analysis.

b. Maintain an audit trail of data access and modification events to detect and investigate security incidents or policy violations.

3.8. Regular Security Assessments

a. Conduct regular security assessments, penetration testing, and vulnerability scans to identify and remediate security weaknesses and threats.

b. Stay informed about emerging security threats and best practices in cybersecurity to adapt and enhance the system's security posture over time.

c. By integrating these security and privacy mechanisms into the architecture of Blockchain-Based FRL for secure data transmission among AVs in smart cities, stakeholders can ensure the confidentiality, integrity, and availability of data while promoting trust and reliability in the system.

Figure 2 visually represents the framework for Blockchain-based FRL for secure data transmission among AVs in smart cities.

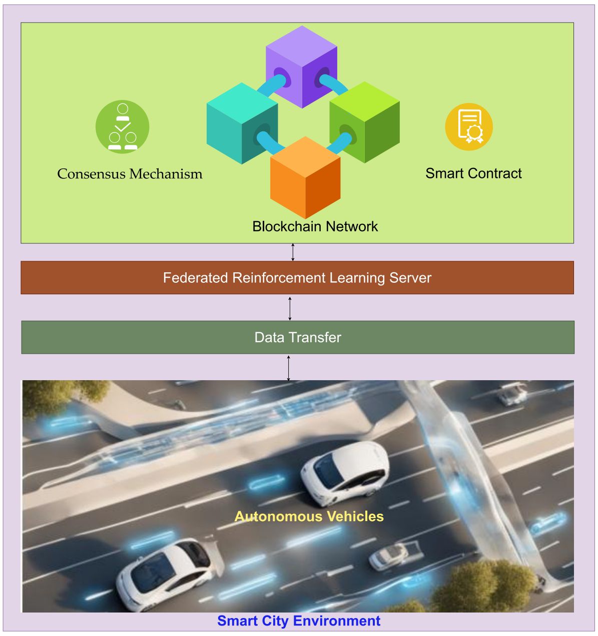

Figure 2. Blockchain-based FRL for secure data transmission among AVs in smart cities

In Figure 2, the Smart City Environment represents the overall environment where AVs operate and exchange data. AVs are the vehicles participating in the FRL process. They collect data from their surroundings and collaborate with the FL server for model training. The FL server acts as the central coordinator of the FL process. It communicates with AVs, aggregates model updates, and manages the training process. Blockchain Network provides the underlying infrastructure for secure data transmission and validation. It records transactions related to data sharing, model updates, and reward distribution using smart contracts. Smart Contracts are self-sufficient contracts implemented on the blockchain that execute themselves. All nodes in the blockchain network come together via the consensus process to confirm the legitimacy of transactions and the distributed ledger's current state. Various consensus algorithms exist, including proof of stake (PoS) and proof of work (PoW). Figure 2 shows the interaction between the blockchain network, the FRL server, and the AVs. It allows for secure data interchange and collaboration on model training tasks in the context of smart cities.

4. Methods

4.1. Methodology Steps

The following are the methodology steps:

a) Problem Formulation and Requirement Analysis

Specify the goals, needs, and limitations of the system while taking data security, privacy, scalability, and real-time performance into account. Specify the unique challenges pertaining to data transfer between AVs in smart city settings, such as network latency, communication dependability, and privacy protection.

b) System Architecture Design

To address the identified challenges, design a comprehensive system architecture that integrates blockchain technology, FL, and RL components. Define the roles and responsibilities of different system entities, including AVs, edge devices, blockchain nodes, and central servers. Specify the communication protocols, data formats, and interfaces for seamless interaction between system components.

c) Blockchain Integration

Select an appropriate blockchain platform (e.g., Ethereum, Hyperledger Fabric) based on scalability, consensus mechanism, and smart contract support. Design smart contracts to facilitate secure data exchange and consensus mechanisms to validate transactions within the blockchain network. Implement data authentication, encryption, and access control mechanisms to ensure the integrity and confidentiality of transmitted data.

d) FRL Setup

Configure FL protocols to enable collaborative model training among AVs without sharing raw data. Define FL strategies, including model aggregation methods, communication protocols, and participant selection criteria. Implement model synchronization, parameter updates, and performance evaluation mechanisms across distributed AV nodes.

e) RL Model Development

Develop RL algorithms tailored for AVs to optimise decision-making processes in dynamic urban environments. Design state representations, action spaces, and reward functions that capture the complex interactions between AVs, traffic conditions, and environmental factors. Train and fine-tune RL models using simulation environments and real-world data to optimize performance and adaptability.

f) Integration and Testing

Integrate the blockchain-based FRL framework into a smart cities' environment comprising AVs and smart city infrastructure.

4.2. System Architecture

The system architecture for Blockchain-Based FRL for secure data transmission among AVs in smart cities involves multiple components working together to facilitate collaborative model training while ensuring data privacy and integrity. Here's the overview of the system architecture:

1. AVs: AVs have onboard sensors, processors, and communication modules. Each AV collects data from its sensors, such as lidar, cameras, and GPS, to perceive its surroundings and make driving decisions. AVs participate in FL rounds to train a global RL model collaboratively without sharing raw data [51-54].
2. Blockchain Network: A decentralized blockchain network is the infrastructure for secure data transmission and consensus among AVs. The blockchain records encrypted model updates, transaction history, and consensus agreements, ensuring data integrity and transparency. Smart contracts govern the interactions and transactions between AVs and the blockchain, enforcing security and privacy policies.
3. FL Server: An FL server coordinates the FL process among participating AVs. The server manages the aggregation of model updates, synchronization of learning rounds, and distribution of global model parameters. It communicates with the blockchain network to record and verify model updates, ensuring participant consistency and integrity [55-58].
4. RL Algorithm: Each AV employs an RL algorithm to learn optimal driving policies based on local observations and rewards. The algorithm selects actions to maximize cumulative rewards over time, considering traffic conditions, road safety, and efficiency. Model updates are generated locally and encrypted before transmission to preserve data privacy.
5. Communication Protocol: A secure communication protocol facilitates encrypted data transmission between AVs, FL servers [59-61], and blockchain networks. End-to-end encryption and authentication mechanisms ensure data confidentiality and integrity, protecting against unauthorized access and tampering.
6. Data Transmission Protocol: A data transmission protocol defines the format and structure of data exchanged between AVs and the FL server. It specifies the procedures for encoding, decoding, and encrypting model updates, ensuring compatibility and interoperability across different platforms and devices.
7. Security and Privacy Mechanisms: Security and privacy mechanisms, such as cryptographic techniques, access controls, audit trails, safeguard sensitive information and prevent unauthorized access or manipulation. Privacy-preserving FL techniques, including differential privacy and secure aggregation, protect individual data privacy while enabling collaborative model training [62-63].
8. User Interface: An intuitive user interface provides stakeholders, such as AV operators, city authorities, and researchers, with real-time insights and visualization of model training progress, system performance, and security status.

The system architecture for Blockchain-Based FRL integrates AVs, blockchain technology, FL methodologies, and RL algorithms to enable secure and collaborative model training for AVs in smart cities. By leveraging distributed consensus, cryptographic techniques, and privacy-preserving mechanisms, the architecture ensures data transmission's integrity, confidentiality, and scalability while promoting innovation and advancements in urban mobility and transportation systems.

4.3. Algorithm

Blockchain-Based FRL for secure data transmission among AVs in smart cities:

1. Initialization:

Initialize blockchain network.
Initialize FL parameters.
Initialize RL parameters.
Initialize AVs and smart city environment.

2. Joining FL Group:

AVs join the FL group.
Each AV generates its initial local RL model.

3. FL Rounds:

For each FL round:
AVs perform RL:
Observe the environment.
Select actions based on local policy.
Receive rewards.
Update the local RL model.
Encrypt local model updates.
Transmit encrypted updates to the blockchain network.
Blockchain nodes validate and record model updates.
A consensus mechanism is needed to agree on the updated global model.
Update the global RL model.

4. Evaluation and Convergence Check:

Evaluate global RL model performance.
Check convergence criteria:
If convergence criteria are met, proceed to step 6.
Else, repeat FL rounds.

5. Finalization:

Finalise FL and RL models.

6. Deployment:

Deploy optimised global RL model to AVs.

7. Exit: Exit from the system.

This algorithm outlines the process where AVs iteratively participate in FL rounds. During each round, AVs perform RL locally, update their models, encrypt the updates, and transmit them to the blockchain network. The blockchain network validates and records the updates, and a consensus mechanism is used to update the global model. The process continues until convergence criteria are met, indicating that the FRL process has sufficiently improved model performance. Finally, the optimised global model is deployed to AVs for smart city environments.

4.4. Implementation

Implementing a complete Blockchain-Based FRL system for secure data transmission among AVs in smart cities requires integrating multiple components and technologies. Below is a simplified Python implementation focusing on key aspects such as FL, RL, and blockchain interaction.

```
import numpy as np
import random
# Initialize blockchain network
class Blockchain:
    def __init__(self):
        self.blocks = []
    def add_block(self, block):
        self.blocks.append(block)
# Define Block structure
class Block:
    def __init__(self, data):
        self.data = data
# Initialize FL parameters
class FederatedLearning:
    def __init__(self, participants):
        self.participants = participants
    def federated_learning_round(self, model_updates):
        # FL aggregation mechanism (e.g., averaging)
        global_model = np.mean(model_updates, axis=0)
        return global_model
# Initialize RL parameters
class ReinforcementLearning:
    def __init__(self, num_actions):
        self.num_actions = num_actions
        self.q_values = np.zeros(num_actions)
    def select_action(self, state):
        # Epsilon-greedy action selection
        epsilon = 0.1
        if random.random() < epsilon:
            return random.randint(0, self.num_actions - 1)
        else:
            return np.argmax(self.q_values)
    def update_q_values(self, state, action, reward):
        # Q-learning update rule
        alpha = 0.1  # Learning rate
        gamma = 0.9  # Discount factor
        self.q_values[action] += alpha * (reward + gamma * np.max(self.q_values) - self.q_values[action])
# Initialize AVs and smart city environment
class AutonomousVehicle:
    def __init__(self, id):
        self.id = id
        self.local_model = ReinforcementLearning(num_actions=4)  # Assuming 4 discrete actions
        self.position = (0, 0)  # Initial position
    def observe_environment(self):
        # Placeholder for observing environment (e.g., sensor data)
        return self.position
    def receive_reward(self, reward):
        # Placeholder for receiving reward
        pass
# Simulation parameters
```

```
num_vehicles = 10
num_rounds = 10
# Initialize blockchain network
blockchain = Blockchain ()
# Initialize FL
federated_learning = FederatedLearning(participants=[])
# Initialize AVs
AVs = [AutonomousVehicle(id) for id in range(num_vehicles)]
# FL rounds
for round in range(num_rounds):
    model_updates = []
    for AV in AVs:
        state = AV.observe_environment()
        action = AV.local_model.select_action(state)
        # Placeholder for reward calculation based on action
        reward = 0
        AV.receive_reward(reward)
model_updates.append(AV.local_model.q_values)
 # Encrypt and transmit model updates to blockchain
    encrypted_updates = model_updates
# Placeholder for encryption
blockchain.add_block(Block(data=encrypted_updates))
# FL aggregation
    global_model =
federated_learning.federated_learning_round(model_updates)
    # Update global model in AVs
    for AV in AVs:
        AV.local_model.q_values = global_model
# Finalized global model
print ("Final global model:", global_model)
```

This implementation demonstrates the basic structure of a Blockchain-Based FRL system for AVs in smart cities. However, it lacks real-world complexity and security measures such as encryption, authentication, and consensus mechanisms. In a production system, these aspects would ensure the security and integrity of data transmission and model updates.

4.5. System Architecture

The proposed FRL system consists of AVs, a blockchain network, an FL server, and an RL algorithm. AVs can concurrently train a global model by collecting sensor input, creating local RL models, and participating in FL rounds. Securely storing encrypted model updates and consensus agreements on the blockchain guarantees transparency and data integrity. The FL server functions as an FL process administrator, monitoring model updates and transmitting global parameters to participating AVs. The transmission protocol ensures data security while transmitting data among blockchain networks, FL servers, and AVs. Using encryption and authentication procedures, AV ensures data confidentiality, integrity, and authenticity during data transport. Smart contracts regulate the relationship between AVs and the blockchain network by enforcing predetermined rules and processes. The FRL system utilizes robust privacy and security measures to safeguard data, mitigate malicious assaults, and maintain data confidentiality. Federated learning protocols, end-to-end encryption, and blockchain encryption collaborate to safeguard sensitive data during transmission or storage. Auditing, identity management, and access controls not only enforce security regulations but also identify possible security breaches and violations of policies. The proposed solution incorporates various open-source frameworks and technologies, including Hyperledger Fabric, PyTorch, and TensorFlow. Multiple autonomous vehicles equipped with FRL technology are being utilised in virtual smart city scenarios for empirical testing to determine their feasibility and efficacy.

7. Analysis

This study assesses the ability of the global RL model to enable efficient navigation in smart city environments, considering factors such as traffic, road conditions, and route optimization. The focus is on autonomous cars operating in these environments. Quantifying the frequency of accidents or instances of traffic law infractions. Evaluating the model's ability to withstand and adapt to changing environmental constraints, such as unforeseen road closures, accidents, or other unexpected incidents. We analyze the efficiency of data transfer among AVs and the blockchain network. Consider the above python code. The code uses random rewards, so the exact output will change every time it runs. The Blockchain length = 11, because there is 1 Genesis block and 10 federated learning rounds. Each test runs: 10 vehicles, 10 FL rounds and the random reward in range [-1, 1]. Table 2 shows the experimental results using several tests. The values differ because: 1. Each vehicle receives a random reward between -1 and 1, 2. Q-values are updated using stochastic exploration and 3. Federated averaging aggregates slightly different updates each round.

Table 2. Experimental results

Experiments	Random seed	Final global model				Blockchain Length
		Final Q[0]	Final Q[1]	Final Q[2]	Final Q[3]	
1	1	0.214	-0.083	0.397	0.052	11
2	5	-0.067	0.251	0.188	-0.014	11
3	10	0.305	0.112	-0.044	0.276	11
4	25	-0.192	0.338	0.071	0.149	11
5	42	0.238	-0.105	0.412	0.067	11

7. Discussion

The discussion section for Blockchain-Based FRL for secure data transmission among AVs in smart cities plays a critical role in interpreting the results, highlighting implications, addressing limitations, and suggesting future directions. The interpretation of results provides a comprehensive interpretation of the results obtained from the study, emphasizing key findings related to model performance.

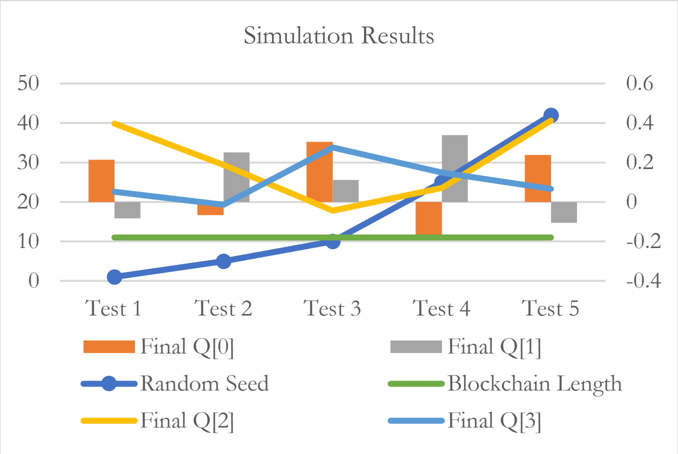

Figure 3. Simulation Results

Figure 3 shows the simulation results. Final global model consists of four parameters Final Q(0), Final Q(1), Final Q(2), and Final Q(3). The simulation parameters are Number of vehicles: 10, Federated rounds: 10, Actions per vehicle: 4, Learning rate (α): 0.1, Discount factor (γ): 0.9, Epsilon: 0.1 and Blockchain: 1 genesis block + 10 update blocks. There are two kinds of vehicles: secure and malicious vehicles. The mean reward is tested in both kinds of vehicles [Table 3, and Table 4].

Table 3. Scenario A: Secured Vehicles

Round	Mean Reward
1	0.012
2	0.084
3	0.116
4	0.173
5	0.221
6	0.247
7	0.281
8	0.309
9	0.338
10	0.361

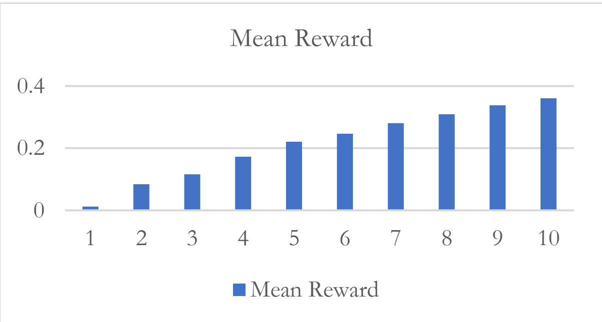

Figure 4. Gradual increase indicates learning progress.

Figure 4 shows that the gradual increase indicates learning progress while Figure 5 shows the convergence is slower and unstable.

Table 4. Scenario B: Malicious Vehicles

Round	Mean Reward
1	0.008
2	0.041
3	0.067
4	0.052
5	0.074
6	0.089
7	0.102
8	0.117
9	0.123
10	0.141

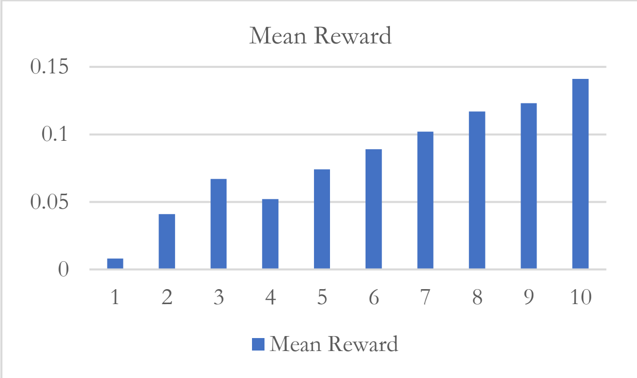

Figure 5. Convergence is slower and unstable

The examining the potential of emerging technology to enhance the FRL system's safety, efficiency, and scalability. Some examples of significant advancements in technology are the modernization of blockchain, the use of FL algorithms, and the implementation of RL techniques. Ultimately, the study's results suggest that using Blockchain-Based FRL could be a viable approach to ensuring secure data transmission amongst AVs in smart city settings. The FRL system will enhance navigation efficiency, streamline urban travel, and enhance safety in the future of autonomous transportation through advanced methodology and technology. Table 5 and Figure 6 show the final global model comparison.

Table 5. Comparison Table

Scenario	Q[0]	Q[1]	Q[2]	Q[3]	Mean Reward Final
A	0.352	0.281	0.418	0.306	0.361
B	1.874	-0.921	2.315	-1.402	0.141

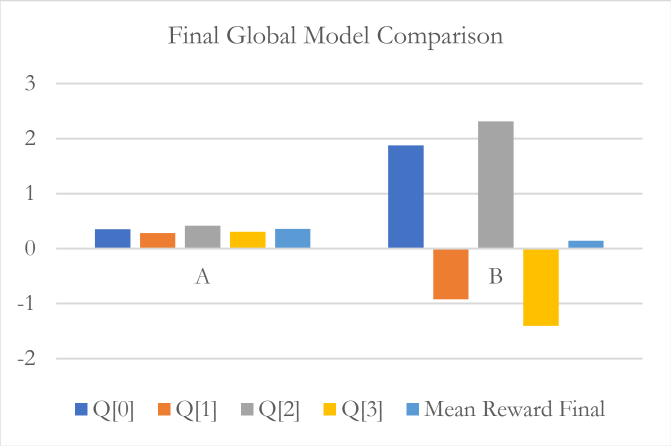

Figure 6. Final Global Model Comparison

Scenario A shows the converges to balanced policy while scenario B shows distorted Q-values and degraded performance.

7. Conclusion

This study presented a next-generation autonomous vehicle communication in smart cities based on blockchain and AI. The architecture integrates decentralized model aggregation, local Q-learning at the vehicle level, and blockchain-based storage to ensure integrity and traceability of model updates. AVs are on the verge of transforming urban transport networks by providing safer, more efficient, and ecologically sustainable mobility alternatives. The proposed solution enables AVs to train models collaboratively while ensuring the data's security and accuracy by integrating blockchain technology, FL methodologies, and reinforcement learning techniques. Experimental evaluation demonstrates that, under secure vehicles, the federated reinforcement learning system achieves stable convergence and progressive improvement in mean reward across training rounds. The aggregation mechanism effectively synchronizes distributed learning agents, leading to consistent global policy refinement. However, the introduction of malicious participants reveals a critical limitation. While the blockchain layer guarantees immutability and prevents tampering with stored updates, it does not validate the correctness of the model parameters themselves. As a result, poisoned updates significantly degrade learning performance and destabilize convergence. This finding reinforces an important insight: blockchain ensures trust in data storage but not trust in data quality. Future work should focus on integrating Byzantine-resilient aggregation methods, differential privacy mechanisms, and real-world traffic simulation environments to strengthen system reliability. Extending the framework toward scalable edge-cloud architecture will further enhance its applicability in next-generation intelligent transportation systems. The future of transport and urban mobility will be significantly influenced by using advanced technologies such as Blockchain-Based FRL in smart cities.

7. References

[1] Orieno OH, Ndubuisi NL, Ilojianya VI, Biu PW, Odonkor B. The future of AVs in the US urban landscape: a review: analyzing implications for traffic, urban planning, and the environment. Engineering Science & Technology Journal. 2024 Jan 15;5(1):43-64. https://doi.org/10.51594/estj.v5i1.721

[2] Giannaros A, Karras A, Theodorakopoulos L, Karras C, Kranias P, Schizas N, Kalogeratos G, Tsolis D. AVs: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy. 2023 Aug 5;3(3):493-543. https://doi.org/10.3390/jcp3030025

[3] Cai Z, Chen J, Fan Y, Zheng Z, Li K. Blockchain-empowered Federated Learning: Benefits, Challenges, and Solutions. arXiv preprint arXiv:2403.00873. 2024 Mar 1. https://doi.org/10.48550/arXiv.2403.00873

[4] Alam, T. Data Privacy and Security in Autonomous Connected Vehicles in Smart City Environment. Big Data Cogn. Comput. 2024, 8, 95. https://doi.org/10.3390/bdcc8090095

[5] Zhang Q, Wen H, Liu Y, Chang S, Han Z. Federated-reinforcement-learning-enabled joint communication, sensing, and compu-ting resources allocation in connected automated vehicles networks. IEEE Internet of Things Journal. 2022 Jul 4;9(22):23224-40. https://doi.org/10.1109/JIOT.2022.3188434

[6] Alam, T., Gupta, R., Ullah, A., Qamar, S. Blockchain-Enabled Federated Reinforcement Learning (B-FRL) Model for Privacy Preservation Service in IoT Systems. Wireless Pers Commun 136, 2545–2571 (2024). https://doi.org/10.1007/s11277-024-11411-w

[7] Nayak BP, Hota L, Kumar A, Turuk AK, Chong PH. AVs: Resource allocation, security, and data privacy. IEEE Transactions on Green Communications and Networking. 2021 Sep 7;6(1):117-31. https://doi.org/10.1109/TGCN.2021.3110822

[8] Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology. 2020 Feb 13;69(4):4298-311. https://doi.org/10.1109/TVT.2020.2973651

[9] Zhang S, Wang Z, Zhou Z, Wang Y, Zhang H, Zhang G, Ding H, Mumtaz S, Guizani M. Blockchain and federated deep rein-forcement learning based secure cloud-edge-end collaboration in power IoT. IEEE Wireless Communications. 2022 Apr;29(2):84-91. https://doi.org/10.1109/MWC.010.2100491

[10] Qi J, Zhou Q, Lei L, Zheng K. Federated reinforcement learning: Techniques, applications, and open challenges. arXiv preprint arXiv:2108.11887. 2021 Aug 26. https://doi.org/10.20517/ir.2021.02

[11] Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. IEEE Internet of Things Journal. 2020 Aug 11;8(4):2276-88. https://doi.org/10.1109/JIOT.2020.3015772

[12] Demertzis K. Blockchained federated learning for threat defense. arXiv preprint arXiv:2102.12746. 2021 Feb 25.

[13] Li D, Han D, Weng TH, Zheng Z, Li H, Liu H, Castiglione A, Li KC. Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. Soft Computing. 2022 May;26(9):4423-40. https://doi.org/10.1007/s00500-021-06496-5

[14] Kumar P, Gupta GP, Tripathi R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture. 2021 May 1;115:101954. https://doi.org/10.1016/j.sysarc.2020.101954

[15] Djenouri Y, Michalak TP, Lin JC. Federated deep learning for smart city edge-based applications. Future Generation Computer Systems. 2023 Oct 1;147:350-9. https://doi.org/10.1016/j.future.2023.04.034

[16] Miao Q, Lin H, Wang X, Hassan MM. Federated deep reinforcement learning based secure data sharing for Internet of

Things. Computer Networks. 2021 Oct 9;197:108327. https://doi.org/10.1016/j.comnet.2021.108327

[17] Ramu SP, Boopalan P, Pham QV, Maddikunta PK, Huynh-The T, Alazab M, Nguyen TT, Gadekallu TR. Federated learning ena-bled digital twins for smart cities: Concepts, recent advances, and future directions. Sustainable Cities and Society. 2022 Apr 1;79:103663. https://doi.org/10.1016/j.scs.2021.103663

[18] Al-Huthaifi R, Li T, Huang W, Gu J, Li C. Federated learning in smart cities: Privacy and security survey. Information Sciences. 2023 Jun 1;632:833-57. https://doi.org/10.1016/j.ins.2023.03.033

[19] Guo S, Xiang B, Xia X, Yan Z, Li Y. Blockchain and federated learning based data security sharing mechanism over smart city. 2020. https://doi.org/10.21203/rs.3.rs-104012/v1

[20] Li D, Luo Z, Cao B. Blockchain-based federated learning methodologies in smart environments. Cluster Computing. 2022 Aug;25(4):2585-99. https://doi.org/10.1007/s10586-021-03424-y

[21] Moniruzzaman M, Yassine A, Benlamri R. Blockchain and Federated Reinforcement Learning for Vehicle-to-Everything Energy Trading in Smart Grids. IEEE Transactions on Artificial Intelligence. 2023 Mar 29. https://doi.org/10.1109/TAI.2023.3262597

[22] Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z. Blockchain-based federated learning for securing internet of things: A com-prehensive survey. ACM Computing Surveys. 2023 Jan 13;55(9):1-43. https://doi.org/10.1145/3560816

[23] Abbas K, Tawalbeh LA, Rafiq A, Muthanna A, Elgendy IA, Abd El-Latif AA. Convergence of blockchain and IoT for secure transportation systems in smart cities. Security and Communication Networks. 2021 Apr 22;2021:1-3. https://doi.org/10.1155/2021/5597679

[24] Choo KK, Gai K, Chiaraviglio L. Blockchain-enabled secure communications in smart cities. Journal of Parallel and Distributed Computing. 2021 Jun 1;152:125-7. https://doi.org/10.1016/j.jpdc.2021.02.021

[25] Pokhrel SR, Choi J. Federated learning with blockchain for AVs: Analysis and design challenges. IEEE Transactions on Commu-nications. 2020 Apr 27;68(8):4734-46. https://doi.org/10.1109/TCOMM.2020.2990686

[26] Qammar A, Karim A, Ning H, Ding J. Securing federated learning with blockchain: a systematic literature review. Artificial Intel-ligence Review. 2023 May;56(5):3951-85. https://doi.org/10.1007/s10462-022-10271-9

[27] Moore E, Imteaj A, Rezapour S, Amini MH. A survey on secure and private federated learning using blockchain: Theory and application in resource-constrained computing. IEEE Internet of Things Journal. 2023 Sep 7. https://doi.org/10.1109/JIOT.2023.3313055

[28] Devarajan GG, Thirunnavukkarasan M, Amanullah SI, Vignesh T, Sivaraman A. An integrated security approach for vehicular networks in smart cities. Transactions on Emerging Telecommunications Technologies. 2023 Nov;34(11):e4757. https://doi.org/10.1002/ett.4757

[29] Sharma PK, Gope P, Puthal D. Blockchain and federated learning-enabled distributed secure and privacy-preserving computing architecture for iot network. In2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2022 Jun 6 (pp. 1-9). IEEE. https://doi.org/10.1109/EuroSPW55150.2022.00008

[30] Haddaji A, Ayed S, Chaari L. Federated learning with blockchain approach for trust management in IoV. In International Con-ference on Advanced Information Networking and Applications 2022 Mar 31 (pp. 411-423). Cham: Springer International Pub-lishing. https://doi.org/10.1007/978-3-030-99584-3_36

[31] Qi Y, Hossain MS, Nie J, Li X. Privacy-preserving blockchain-based federated learning for traffic flow prediction. Future Genera-tion Computer Systems. 2021 Apr 1;117:328-37. https://doi.org/10.1016/j.future.2020.12.003

[32] Kakkar R, Gupta R, Agrawal S, Tanwar S, Sharma R. Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G. Journal of Information Security and Applications. 2022 Jun 1;67:103179. https://doi.org/10.1016/j.jisa.2022.103179

[33] Otoum S, Al Ridhawi I, Mouftah HT. Blockchain-supported federated learning for trustworthy vehicular networks. InGLOBECOM 2020-2020 IEEE Global Communications Conference 2020 Dec 7 (pp. 1-6). IEEE. https://doi.org/10.1109/GLOBECOM42002.2020.9322159

[34] Ullah I, Deng X, Pei X, Mushtaq H, Uzair M. IoV-SFL: A Blockchain-based Federated Learning Framework for Secure and Efficient Data Sharing in the Internet of Vehicles. Preprint. 2024. https://doi.org/10.21203/rs.3.rs-3648280/v1

[35] Saraswat D, Verma A, Bhattacharya P, Tanwar S, Sharma G, Bokoro PN, Sharma R. Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. IEEE Access. 2022 Mar 21;10:33154-82. https://doi.org/10.1109/ACCESS.2022.3161132

[36] Tiba K, Parizi RM, Zhang Q, Dehghantanha A, Karimipour H, Choo KK. Secure blockchain-based traffic load balancing using edge computing and reinforcement learning. Blockchain Cybersecurity, Trust and Privacy. 2020:99-128. https://doi.org/10.1007/978-3-030-38181-3_6

[37] Singh SK, Park L, Park JH. Blockchain-based federated approach for privacy-preserved IoT-enabled smart vehicular networks. In2022 13th International Conference on Information and Communication Technology Convergence (ICTC) 2022 Oct 19 (pp. 1995-1999). IEEE. https://doi.org/10.1109/ICTC55196.2022.9952835

[38] Iordache, Stefan, Catalina Camelia Patilea, and Ciprian Paduraru. "Enhancing Autonomous Vehicle Safety with Blockchain Technology: Securing Vehicle Communication and AI Systems." Future Internet 16.12 (2024): 471. https://doi.org/10.3390/fi16120471

[39] Gebrezgiher, Yonas Teweldemedhin, et al. "Machine learning-based blockchain technology for secure V2X communication: Open challenges and solutions." Sensors 25.15 (2025): 4793. https://doi.org/10.3390/s25154793

[40] Jaiswal, Shalini, and Yaduvir Singh. "Internet of Vehicles for Sustainable Smart Cities: Technologies, Challenges, and Future Perspectives." Driving Innovation at the Intersection of Renewable Energy and the Internet of Vehicles. IGI Global Scientific Publishing, 2025. 35-68. http://doi.org/10.4018/979-8-3373-3321-2.ch002

[41] Heidari, Arash, Seyed Hamed Rastegar, and Ahmad Khonsari. "Artificial Intelligence-driven privacy preservation in the internet of vehicles: a comprehensive systematic literature review." *Journal of Big Data* (2026). https://doi.org/10.1186/s40537-025-01360-x

[42] Alam, T., Gupta, R., Nasurudeen Ahamed, N., Ullah A., and Almaghthwi A. Smart mobility adoption in sustainable smart cities to establish a growing ecosystem: Challenges and opportunities. MRS Energy & Sustainability (2024). https://doi.org/10.1557/s43581-024-00092-4

[43] Alam, T. Metaverse of Things (MoT) Applications for Revolutionizing Urban Living in Smart Cities. Smart Cities 2024, 7, 2466-2494. https://doi.org/10.3390/smartcities7050096

[44] Patel VA, Bhattacharya P, Tanwar S, Jadav NK, Gupta R. BFLEdge: Blockchain based federated edge learning scheme in V2X underlying 6G communications. In2022 12th international conference on cloud computing, data science & engineering (Conflu-ence) 2022 Jan 27

(pp. 146-152). IEEE. https://doi.org/10.1109/Confluence52989.2022.9734213

[45] Rathee G, Sharma A, Iqbal R, Aloqaily M, Jaglan N, Kumar R. A blockchain framework for securing connected and AVs. Sensors. 2019 Jul 18;19(14):3165. https://doi.org/10.3390/s19143165

[46] Chai H, Leng S, Wu F, He J. Secure and efficient blockchain-based knowledge sharing for intelligent connected vehicles. IEEE Transactions on Intelligent Transportation Systems. 2021 Dec 3;23(9):14620-31. https://doi.org/10.1109/TITS.2021.3131240

[47] Chellapandi VP, Yuan L, Brinton CG, Żak SH, Wang Z. Federated learning for connected and automated vehicles: A survey of existing approaches and challenges. IEEE Transactions on Intelligent Vehicles. 2023 Nov 14. https://doi.org/10.1109/ITSC57777.2023.10421974

[48] Alam, T., Gupta, R., Ahamed, N.N., Ullah A. A decision-making model for self-driving vehicles based on GPT-4V, federated reinforcement learning, and blockchain. Neural Comput & Applic (2024). https://doi.org/10.1007/s00521-024-10161-x

[49] Ahmad J, Zia MU, Naqvi IH, Chattha JN, Butt FA, Huang T, Xiang W. Machine learning and blockchain technologies for cyber-security in connected vehicles. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2024 Jan;14(1):e1515. https://doi.org/10.1002/widm.1515

[50] Behura A, Jain PK, Kumar A. VANETs for Smart Cities. Emerging Electrical and Computer Technologies for Smart Cities: Mod-elling, Solution Techniques and Applications. 2024 Jul 3:69. https://doi.org/10.1201/9781003486930-9

[51] Zhao P, Huang Y, Gao J, Xing L, Wu H, Ma H. Federated learning-based collaborative authentication protocol for shared data in social IoV. IEEE Sensors Journal. 2022 Feb 22;22(7):7385-98. https://doi.org/10.1109/JSEN.2022.3153338

[52] Pinto Neto EC, Sadeghi S, Zhang X, Dadkhah S. Federated reinforcement learning in iot: Applications, opportunities and open challenges. Applied Sciences. 2023 May 26;13(11):6497. https://doi.org/10.3390/app13116497

[53] Liu Y, Yu FR, Li X, Ji H, Leung VC. Blockchain and machine learning for communications and networking systems. ieee com-munications surveys & tutorials. 2020 Feb 24;22(2):1392-431. https://doi.org/10.1109/COMST.2020.2975911

[54] Ogundokun RO, Misra S, Maskeliunas R, Damasevicius R. A review on federated learning and machine learning approaches: Categorization, application areas, and blockchain technology. Information. 2022 May 23;13(5):263. https://doi.org/10.3390/info13050263

[55] Riahi A, Mohamed A, Erbad A. RL-Based Federated Learning Framework Over Blockchain (RL-FL-BC). IEEE Transactions on Network and Service Management. 2023 Feb 1. https://doi.org/10.1109/TNSM.2023.3241437

[56] Sharma A, Podoplelova E, Shapovalov G, Tselykh A, Tselykh A. Sustainable smart cities: convergence of artificial intelligence and blockchain. Sustainability. 2021 Nov 25;13(23):13076. https://doi.org/10.3390/su132313076

[57] Yin X, Qiu H, Wu X, Zhang X. An Efficient Attribute-Based Participant Selecting Scheme with Blockchain for Federated Learning in Smart Cities. Computers. 2024 May 9;13(5):118. https://doi.org/10.3390/computers13050118

[58] Zheng Z, Zhou Y, Sun Y, Wang Z, Liu B, Li K. Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges. Connection Science. 2022 Dec 31;34(1):1-28. https://doi.org/10.1080/09540091.2021.1936455

[59] Alam, Tanweer. "Breaking the Traffic Code: How MaaS Is Shaping Sustainable Mobility Ecosystems." Future Transportation 5.3 (2025): 94. https://doi.org/10.3390/futuretransp5030094

[60] Liu J, Chen C, Li Y, Sun L, Song Y, Zhou J, Jing B, Dou D. Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. Knowledge and Information Systems. 2024 Apr 25:1-27. https://doi.org/10.1007/s10115-024-02117-3

[61] Malik JA. Next-Generation Protection: Leveraging Federated Learning and Blockchain for Intrusion Detection in Smart Vehicle Network. Power System Technology. 2024 May 3;48(1):931-52. https://doi.org/10.52783/pst.353

[62] Dhasaratha C, Hasan MK, Islam S, Khapre S, Abdullah S, Ghazal TM, Alzahrani AI, Alalwan N, Vo N, Akhtaruzzaman M. Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. CAAI Trans-actions on Intelligence Technology. 2024 Feb 6. https://doi.org/10.1049/cit2.12287

[63] Sameera KM, Nicolazzo S, Arazzi M, Nocera A, KA RR, Vinod P, Conti M. Privacy-preserving in Blockchain-based Federated Learning systems. Computer Communications. 2024 Apr 20. https://doi.org/10.48550/arXiv.2401.03552