International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 5, Issue 2, 25-36, 2024
ISSN: 3050-9262 | https://doi.org/10.63282/30509262/IJAIDSML-V5I2P104

Original Article

Digital Identity Architecture for Autonomous Mobility: A Blockchain and Federation Approach

Sreejith Sreekandan Nair[1], Govindarajan Lakshmikanthan[2]
[1, 2] Independent Researcher, Leading Financial Firm, Texas, USA.

Abstract - *The rise of Autonomous Vehicles has transformed how we get around, but it's created some serious security headaches too. We need to keep these vehicle networks safe from hackers and unauthorized users. In our research, we've found that blockchain technology could be a game-changer when combined with federated identity management to secure AV systems. Blockchain gives us an unalterable, distributed ledger that maintains data integrity across vehicle networks, while federated identity management offers a streamlined authentication process that doesn't compromise security or privacy. Together, they tackle major problems like data tampering, slow authentication, and vulnerable central points that hackers love to target. We've developed a hybrid approach using blockchain to validate data and federated identity to efficiently authenticate both people and vehicles. Our mathematical models and simulations show this approach significantly outperforms traditional methods in speed, scalability, and resistance to cyberattacks. Not only does our system meet current AV security needs, but it also opens the door for AI-based threat detection in the future. This blockchain-federated identity combination provides the security foundation needed for truly reliable autonomous transportation systems.*

Keywords - *Vehicular Authentication, Vehicle-to-Everything (V2X), Data Integrity, Decentralized Systems.*

1. Introduction

Autonomous vehicles are transforming transportation as we know it. They're powered by AI, machine learning, advanced sensors, and connectivity tech that's changing how we get from point A to point B. These vehicles make decisions based on sophisticated navigation systems and communicate with other vehicles and infrastructure. That's why they need serious cybersecurity - without it, they're just not safe on our roads. As more AVs hit the streets, they'll rely on Vehicle-to-Everything (V2X) networks to talk to other vehicles, roadside equipment, and cloud systems. This makes them safer, but also creates new security challenges we need to address.

AVs face several major security hurdles. Their communication networks - whether vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or vehicle-to-cloud (V2C) - create numerous entry points for hackers. Data integrity is another huge concern - AVs make life-or-death decisions based on the information they receive, so tampered data could cause accidents or system failures. Authentication remains the cornerstone of security - we need to ensure only authorized entities can access and control these vehicles. But current authentication systems struggle to scale as the network of connected vehicles grows.

1.1 Existing Solutions and Their Limitations

We've tried various security approaches, but they all have drawbacks. Public Key Infrastructure (PKI) works well for identity verification and encryption, but managing certificates for millions of vehicles is incredibly difficult. Centralized identity systems are vulnerable to single-point failures - if the central authority gets compromised, the entire network is at risk. Plus, these systems require users to surrender personal data, raising serious privacy concerns.

This is where blockchain and federated identity management show promise. Blockchain provides a distributed, tamper-proof ledger that helps ensure data integrity between AVs and connected systems. It's decentralized, eliminating single points of failure, and transparent, making data tampering obvious. Federated identity management allows trusted entities to share authentication credentials while protecting user privacy. Unlike centralized systems, it reduces data breach risks and gives users control over their personal information. By combining these technologies, we can significantly boost AV security, making our increasingly connected transportation ecosystem both safer and more efficient.

2. Literature Review

Recent advancements in autonomous vehicle (AV) technology have highlighted significant security challenges within the connected transportation ecosystem. This paper presents a critical analysis of cutting-edge approaches addressing these challenges, focusing on blockchain integration, federated learning methodologies, and self-sovereign identity solutions for decentralized authentication in autonomous vehicles. The convergence of blockchain technology with federated identity solutions offers a robust and verifiable framework for security and authentication in AVs. This integration provides enhanced data security [5-7], privacy preservation, and authentication within the interconnected AV operational ecosystem. Our comprehensive literature review explores significant contributions in this domain, examining how blockchain facilitates secure data handling, how federated learning enhances privacy protection, and how Self-Sovereign Identity enables decentralized identification solutions.

Blockchain enables secure and efficient data exchange between AVs while maintaining transparency, tamper-resistance, and storage integrity. Smart contracts—self-executing agreements with code-embedded terms—can autonomously negotiate data-sharing protocols between vehicles. This framework ensures that sensitive information, such as vehicle location or velocity, can be shared without compromising critical traffic data flow. Particularly significant is real-time data sharing in cooperative driving scenarios, which facilitates accident prevention and enhances driving efficiency. Federated learning (FL) represents an innovative distributed machine learning approach that allows AVs to train their models without centralizing data [8-10]. This methodology offers two significant advantages: addressing critical privacy concerns and enhancing AV system performance.

In autonomous driving environments, privacy is essential for vehicle data collection processes, as vehicles accumulate sensitive information including driving behaviors, location histories, and environmental conditions. Federated learning maintains data decentralization—vehicles transmit only model updates without sharing raw data with central servers, thereby protecting sensitive information. This privacy-preserving approach enables AVs to improve their predictive models while safeguarding confidential information. AVs operate across diverse environments, from urban centers to rural highways, each presenting unique challenges for machine learning models. Federated learning provides an ideal framework for AVs to leverage multiple data sources, enhancing the robustness and adaptability of their machine learning models. Through federated training, AVs learn from diverse driving patterns and conditions without transferring personal data, resulting in improved performance across various real-world driving scenarios.

The integration of blockchain with federated learning significantly enhances the security and trustworthiness of the learning process. Blockchain ensures that only authenticated updates from verified vehicles contribute to the global model, preventing adversarial attacks that could manipulate the learning process. This combined approach provides AVs with a resilient and trustworthy framework for autonomous decision-making while improving machine learning model security and accuracy. Self-sovereign identity (SSI) represents an emerging identity management paradigm that empowers users and vehicles to maintain control over their digital identities [11-13] without dependence on centralized authorities. Authentication in Vehicular Networks involves both security and privacy considerations, and this decentralized authentication approach has profound implications for AVs. Built on blockchain technology, SSI establishes secure and decentralized identity management systems for AVs. While cryptographic techniques facilitate autonomous authentication, vehicles operate independently of central authorities for identity verification.

This decentralized approach minimizes the risk of identity theft and unauthorized node connections, ensuring that only authenticated entities interact with vehicle systems. Selective disclosure capabilities during verification further enhance privacy protection. A key advantage of SSI is its support for interoperability between diverse AV systems and manufacturers. SSI implements decentralized standards ensuring that SSI-compliant vehicles from any manufacturer can securely communicate and collaborate. This interoperability is essential for widespread adoption of connected vehicle technologies, enabling seamless integration across different AV ecosystems regardless of manufacturer or model. Traditional centralized identity management systems present vulnerable single points of failure that attackers can exploit. SSI eliminates these vulnerabilities by removing the need for central authentication authorities. The cryptographic foundations of SSI ensure secure identity verification, while its decentralized nature increases resistance to attacks. Consequently, SSI provides a more secure and reliable authentication mechanism for AVs, preventing unauthorized access and maintaining system security.

2.1 Blockchain and Federated Identity Architecture for Autonomous Vehicles

The proposed authentication architecture for autonomous vehicles (AVs) integrates blockchain technology with federated identity solutions to establish a robust security framework, as depicted in the architectural schema [14-16]. At the core of this system resides the Blockchain Network, which functions as the central repository for transaction data and authentication logic. The authentication process is facilitated by Blockchain Nodes that execute smart contracts, thereby ensuring process security and automation. The implementation of a Distributed Ledger guarantees data immutability and transparency throughout the system.

The Federated Identity System enhances the security infrastructure by implementing a sophisticated identity verification mechanism for AVs. Vehicle identity validation occurs through secure communication channels with the Identity Provider (IdP), with subsequent authentication processing in the Federation Hub where token verification takes place. This multi-tiered verification protocol effectively prevents unauthorized vehicles from accessing services within the AV ecosystem.

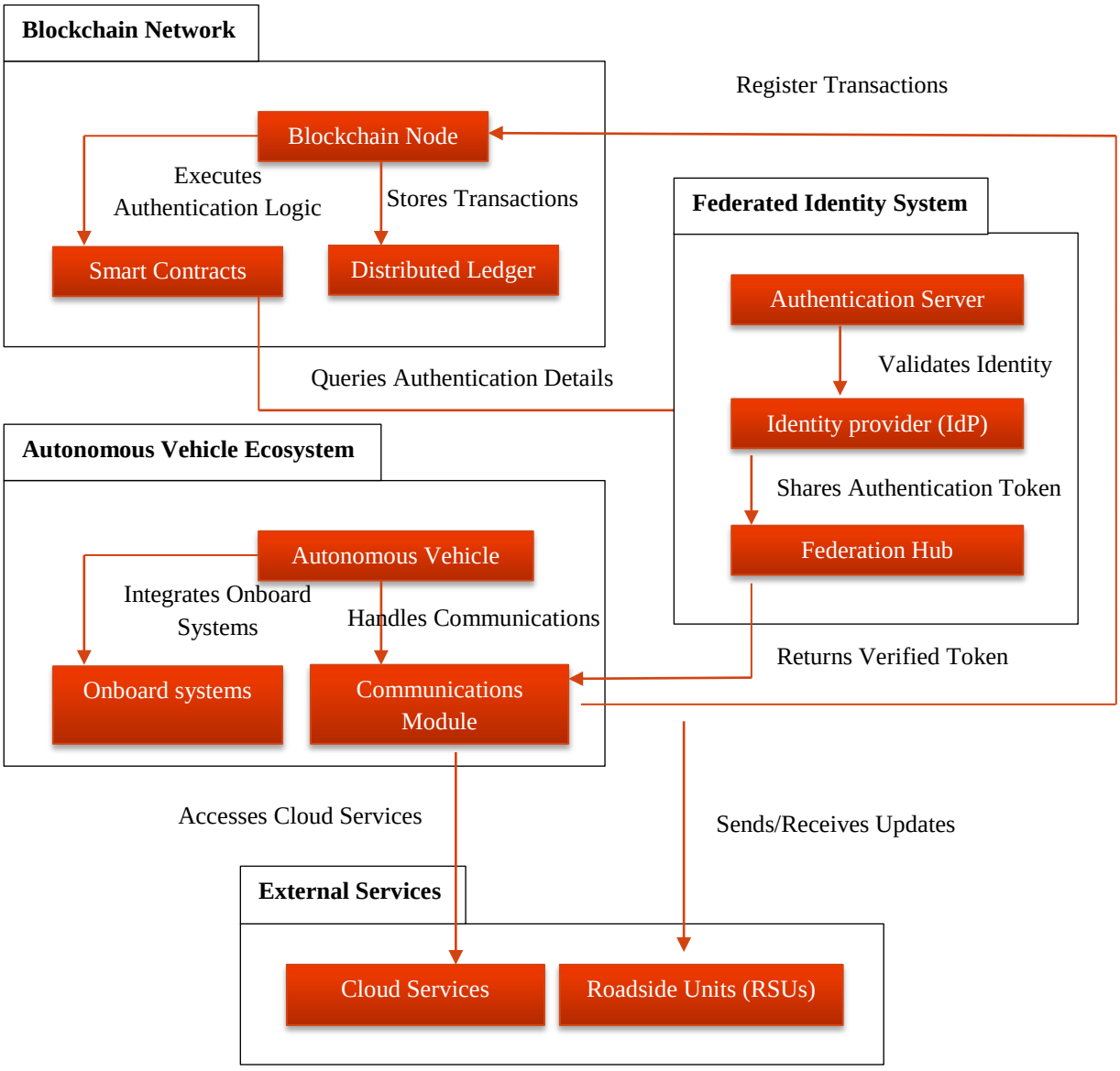

Fig 1: Blockchain and Federated Identity Architecture for Autonomous Vehicles

Autonomous vehicles interface with this security framework through their onboard systems and communication modules, enabling connections to External Services including Cloud Services for over-the-air updates and Roadside Units (RSUs) for continuous real-time communications. The synergistic integration of federated identity mechanisms with the blockchain network ensures that all data exchanges and authentication processes maintain the highest standards of security, reliability, and operational efficiency. The architectural framework comprehensively illustrates how each blockchain component and federated identity element contributes to the cohesive functioning of the system, creating a secure operational environment for autonomous vehicles navigating complex transportation networks. This integrated approach addresses the critical security challenges inherent in connected autonomous vehicle ecosystems while supporting the dynamic nature of modern transportation infrastructure.

3. Methodology

This section proposes a comprehensive security framework for autonomous vehicles (AVs) through the integration of blockchain technology and federated identity management [17-20]. The framework encompasses key architectural components, their interactions within AV communication systems, and their extensibility across the Vehicle-to-Everything (V2X) environment. By illustrating mechanisms for secure, transparent, and decentralized communication and authentication in AV systems, we establish a robust security framework that leverages blockchain's data integrity and transparency capabilities alongside federated identity management's privacy-preserving and decentralized authentication features. This synergistic approach effectively addresses critical security and privacy challenges inherent in interconnected AV ecosystems.

3.1 Blockchain Integration

The proposed framework leverages blockchain technology as its foundational infrastructure, providing transparency, immutability, and decentralization. This technological backbone secures information exchange, authentication processes, and coordination mechanisms within AV networks.Blockchain technology enables the recording of transactions and data exchanges between AVs in a transparent, auditable ledger. This transparency establishes trust among participants by allowing verification of every transaction through distributed nodes within the system. The immutability characteristic ensures that once data is recorded on the blockchain, it remains unalterable, thus preserving the integrity of critical system information including authentication records, traffic data, system updates, and operational logs. This immutability is particularly crucial for AV data processing, where maintaining accuracy and reliability directly impacts operational safety and efficiency.Smart contracts serve as automated execution mechanisms within AV networks, facilitating data sharing, access permissions, and data handling protocols.

For instance, a vehicle can autonomously execute a smart contract with another vehicle to negotiate priority lane access without requiring central authority intervention. This automation significantly reduces latency, enhances operational efficiency, and ensures that all transactions remain secure and verifiable through the blockchain infrastructure.Consensus algorithms are fundamental to blockchain functionality, ensuring distributed ledger state agreement across all participating nodes. These mechanisms have proven valuable in promoting decentralization and establishing trust within AV systems. The framework evaluates several prominent consensus algorithms: Proof of Work (PoW) offers high security but exhibits limitations including energy-intensive operations and slower transaction processing; Proof of Stake (PoS) provides improved energy efficiency over PoW, but potentially enables centralization as nodes with larger stakes gain disproportionate influence; Practical Byzantine Fault Tolerance (PBFT) delivers exceptional performance for AV networks but may encounter scalability challenges in larger implementations.

3.2 Federated Identity Management

Federated Identity Management (FIM) provides a framework for decentralized and secure authentication of users and vehicles without reliance on centralized authorities. This approach enables seamless vehicle authentication across multiple systems, enhancing security and privacy throughout the AV ecosystem. The proposed framework enables vehicles to authenticate across multiple domains through trusted third-party identity providers (IdPs), effectively eliminating single-point-of-failure vulnerabilities inherent to centralized authentication servers. For example, when a vehicle enters a new jurisdiction, it can seamlessly access local smart parking systems without re-registration, as these systems recognize the vehicle's identity through the federated framework. This decentralized approach significantly enhances authentication scalability, security, and efficiency across diverse operational environments.

FIM implements selective disclosure techniques that reveal only necessary identity attributes during vehicle authentication processes. Vehicles can provide minimal required information—such as license validity and insurance status—while withholding sensitive data including location history or owner information. This approach maintains robust privacy protection while enabling secure interactions between disparate systems within the AV ecosystem. Blockchain technology provides secure storage and verification infrastructure for identity credentials within the FIM framework. This integration delivers a tamper-resistant record of authentication events, effectively preventing unauthorized access attempts. Additionally, blockchain enhances transparency by enabling all participants to verify the integrity of authentication processes, creating a secure foundation for trusted interactions throughout the AV network.

3.3 Implementation Scope

The integration of blockchain and federated identity management within the AV communication ecosystem enables secure, efficient, and scalable operations across various V2X domains, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Cloud (V2C), and Vehicle-to-Pedestrian (V2P) communication. Vehicle-to-Everything (V2X) communication represents a critical enabler for AVs to interact with their surroundings, creating both safer and more efficient transportation systems. Vehicle-to-Vehicle (V2V) communication allows autonomous vehicles to exchange information directly,

sharing real-time data on road conditions, incident alerts, and traffic status. Blockchain technology ensures this V2V communication data remains immutable and trustworthy, providing an enhanced security layer. For example, vehicles can reliably transmit road hazard alerts with guaranteed accuracy and tamper-resistance, preventing accidents and facilitating traffic management.

Vehicle-to-Infrastructure (V2I) communication establishes connections between AVs and infrastructure systems including traffic signals, toll facilities, and roadway signage. This enables vehicles to authenticate with these systems without requiring persistent registration processes. Blockchain technology enhances these interactions by facilitating process automation—such as toll payments—through smart contracts, reducing transaction times and operational costs.
Vehicle-to-Cloud (V2C) communication facilitates secure data upload and retrieval between AVs and cloud services, including navigation information and vehicle performance metrics. Blockchain technology secures this data exchange, while federated authentication provides streamlined and secure access to cloud services such as over-the-air updates and predictive analytics platforms.

Vehicle-to-Pedestrian (V2P) communication ensures that AVs can interact safely with pedestrians in shared environments. Blockchain and federated identity management enable secure, privacy-preserving communication between vehicles and pedestrian devices, ensuring accurate and reliable transmission of critical safety alerts, including proximity notifications about nearby AVs [21]. This comprehensive communication network forms the foundation of a secure, interconnected autonomous driving ecosystem.

Fig 2: Vehicle-to-Everything Communication in Autonomous Vehicles

Table 1: Key Technologies and Their Purposes in Autonomous Vehicle Security

Step	Technology Used	Purpose
Vehicle Authentication	Federated Identity	Decentralized and secure verification
Data Exchange	Blockchain	Transparency and data integrity
Automated Actions	Smart Contracts	Reduced latency and operational efficiency

4. Algorithmic Representation

This section presents a systematic analysis of two fundamental components within the proposed security framework for autonomous vehicles (AVs). We detail the algorithmic implementations for blockchain-based data validation [22-26] and federated identity verification processes. These algorithms ensure data integrity and authentication security throughout the AV ecosystem. The mechanisms are illustrated through formal pseudocode and process flowcharts to provide comprehensive technical clarity.
Data integrity represents a critical requirement for autonomous vehicle operations, particularly for information exchanged between vehicles in a distributed network. Blockchain technology provides a robust, tamper-resistant validation mechanism that secures this inter-vehicle communication.

The validation process begins when vehicles generate operational data, including traffic conditions, environmental parameters, and hazard alerts. This data is subsequently encapsulated in a transaction structure and cryptographically signed using the vehicle's private key, establishing non-repudiable authentication of the data source. Upon transaction creation, the vehicle

transmits the signed data package to blockchain network nodes for processing. These nodes validate the transaction against established protocol rules and consensus parameters before incorporating valid transactions into candidate blocks. The network's consensus mechanism—whether Proof of Work, Proof of Stake, or an alternative protocol—then determines which candidate blocks are permanently added to the blockchain. Upon successful validation and block integration, both the originating vehicle and network participants receive confirmation of the transaction's verification status.
The following pseudocode formalizes the blockchain-based data validation process:

Input: Dataset D generated by Vehicle V
Output: Blockchain-validated Dataset D

Process Flow:

1. Vehicle V generates dataset D
2. Vehicle V composes transaction T containing:
    - Dataset D
    - Vehicle identifier V_ID
    - Current timestamp
3. Vehicle V digitally signs transaction T using its private key PK_V to create T_signed
4. T_signed is broadcast to all nodes on the blockchain network
5. Validation process at each network node N:
    - If signature verification succeeds: Add T_signed to pending transaction pool
    - If signature verification fails: Discard transaction
6. Network nodes execute the blockchain's consensus mechanism to validate pending transactions and organize them into Block B
7. Upon consensus, Block B containing the validated transaction is appended to the blockchain
8. Confirmation notifications are sent to Vehicle V and relevant network participants

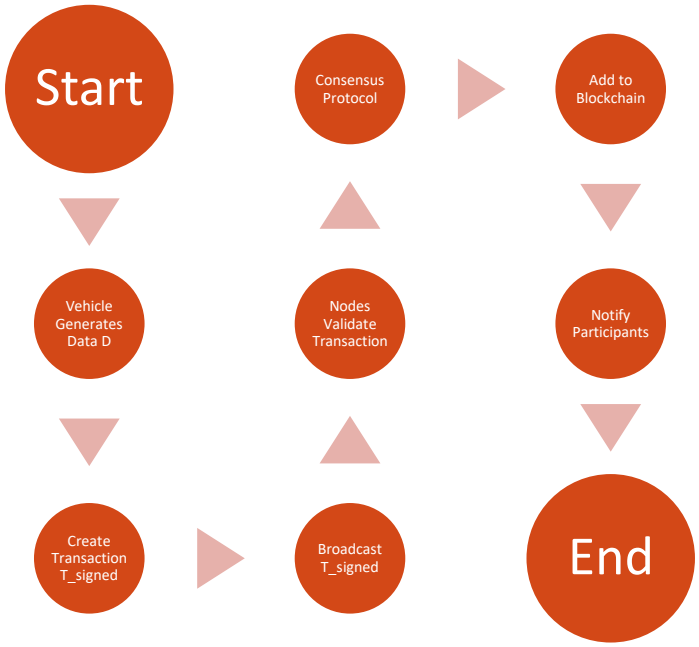

Fig 3: Flowchart for Blockchain Data Validation

4.1 Federated Identity Verification Workflow

Federated Identity Management (FIM) serves as a crucial foundation for secure, decentralized authentication within autonomous vehicle systems. This framework enables vehicles and users to authenticate across different domains while protecting sensitive data.The authentication process begins when a vehicle or user initiates an access request for a service, such as a toll

payment system. This request is then processed by the Federated Identity Provider (IdP), which validates the requester's credentials and issues a digitally signed authentication token. This token contains essential information including the user's identity, authorized permissions, and expiration timestamp. Upon receiving this signed token, the vehicle or user forwards it to the appropriate Service Provider (SP). The SP then verifies the token's authenticity using the IdP's public key. Service access is granted only after successful token verification; otherwise, the request is rejected. Following this verification process, the Service Provider communicates the access decision back to the requesting vehicle or user. The pseudocode for the federated identity verification process is as follows:

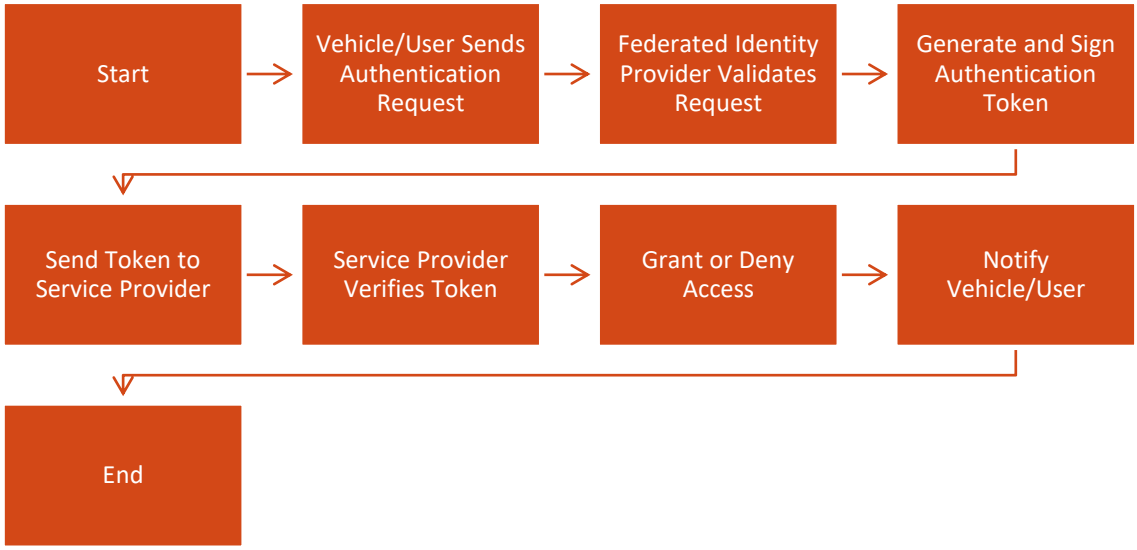

Fig 4: Federated Identity Verification Workflow

4.2 Mathematical Model

In this section, we define key variables and parameters and provide models of federation identity systems that require the use of blockchain consensus and authentication delay. [27-30] Discussion of performance metrics to be used for the evaluation of the system's efficiency is also presented.

4.3 Key Variables and Parameters

Several key variables and parameters for modeling blockchain consensus mechanisms and federation identity authentication delay are defined in order to quantify system performance. They include transaction processing time, blockchain block creation time, network Latency, and Authentication metrics. Therefore, specifically, it is the average transaction processing time. T_{tx}, the time that a transaction takes in the blockchain network in seconds. The time taken to create and deposit a block into the blockchain T_{block} is referred to as block creation time. The term number of validating nodes N_{nodes} denotes the number of nodes used during the consensus process when building the blockchain. Network latency $L_{network}$is commonly measured in milliseconds as the time that data takes to move between nodes.

In the federated identity system, the authentication success rate $Rauth$ is the percentage of successful authentications and the authentication delay. T_{auth} is an amount of time measured in milliseconds to complete authentication. The probability of authentication failure, failure rate R_{fail}, is R_{fail}=$1 - R_{auth}$. Time of consensus overhead $C_{blockchain}$, which is the amount of time it takes for the blockchain nodes to reach consensus is, dependent on the consensus protocol (for example, Proof of Stake or PBFT). Finally, the total delay T_{total} includes all the single-time components necessary to perform the blockchain based authentication and data validation processes.

```
Input: Authentication Request AR from Vehicle/User
Output: Access Granted/Denied based on Verification

Step 1: Vehicle/User sends AR to Federated Identity Provider (IdP)
Step 2: IdP validates AR and generates Token T = {User_ID, Expiry, Permissions}
Step 3: IdP signs T with private key PK_IdP: T_signed = Sign(T, PK_IdP)
Step 4: Vehicle/User sends T_signed to Service Provider (SP)
Step 5: SP verifies T_signed using IdP's public key PK_IdP:
   If Verify(T_signed, PK_IdP) == True and T is valid:
      Grant Access
   Else:
      Deny Access
Step 6: Notify Vehicle/User of SP's decision
```

4.4 Blockchain Consensus Mechanisms

The blockchain's consensus mechanism ensures that all nodes in the network agree on the state of the distributed ledger. The total time for consensus $T_{Consensus}$ can be modeled as:

$$T_{Consensus} = T_{tx} + C_{blockchain} + L_{network}$$

Where T_{tx} is the transaction propagation and processing time, $C_{blockchain}$ is the time required for consensus among nodes and $L_{network}$ is the network latency between nodes. This formula accounts for the delay in data transmission, the time required for blockchain nodes to reach a consensus, and the protocol overhead.

Performance metrics for blockchain consensus are critical to evaluating the efficiency of the network. For example, throughputTP, which is the number of transactions processed per second, is calculated as:

$$TP = \frac{T_{block}}{N_{tx}}$$

Where N_{tx} is the number of transactions processed per block. Latency L is the time required to validate a transaction, and scalability S is defined as the system's ability to efficiently handle additional nodes:

$$\mathrm{S} = \frac{L_{network} + T_{Consensus}}{N_{nodes}}$$

This indicates how well the blockchain can scale as the number of nodes increases.

4.5 Authentication Delay in Federated Identity Systems

In federated identity systems, the total authentication delay T_{auth} is the sum of several components: the response time T_{resp}, the identity provider verification timeT_{verify}, and the request processing time T_{req}.

$$T_{auth} = T_{req} + T_{verify} + T_{resp}$$

That is, T_{req} the time it takes for the authentication request to reach the identity provider, T_{verify} the time required for the identity provider to verify the credentials and to respond with a token and T_{resp} the time to get the response back to the service provider.

The probability of successful authentication P_{auth} is calculated as:

$$P_{auth} = R_{auth} * \left(1 - R_{fail}\right) * N_{nodes}$$

Where N_{nodes} is the no. of nodes involved in proving the identity. The above formula takes into account the success rate of authentication, the failure rate, and the number of nodes included in the process.

4.6 Performance Metrics for Federated Identity Systems

A number of metrics are used to evaluate the performance of the federated identity system. The success rate R_{auth} measures the system's reliability and is defined as the ratio of successful authentications to total authentication requests.

$$R_{auth} = \frac{Successful\ Authentications}{Total\ Requests}$$

The average delay $\overline{T_{auth}}$ is the mean time taken for authentication, calculated as:

$$\overline{T_{auth}} = \frac{\sum T_{auth}}{Total\ Requests}$$

The failure rate R_{fail} which indicates the likelihood of authentication failure, is simply

$$R_{fail} = 1 - R_{auth}$$

4.7 Total System Efficiency

To assess the overall performance of the system, the total delay T_{total} for blockchain-based validation and federated authentication is modeled as follows:

$$T_{total} = T_{Consensus} + T_{auth}$$

The efficiency ratio E (E) of the system can then be expressed as:

$$E = \frac{T_{total} * TP}{Total\ Valid\ Transactions}$$

Table 2: Blockchain and Federated Identity Performance Metrics

Metric	Blockchain Value	Federated Identity Value
Average Transaction Time (T_tx)	0.5 seconds	-
Consensus Overhead (C_blockchain)	2 seconds	-
Authentication Delay (T_auth)	-	200 ms
Network Latency (L_network)	100 ms	50 ms
Authentication Success Rate (R_auth)	-	98%

5. Results and Discussion

This section describes the results of applying blockchain based data validation and federated identity verification in the Autonomous Vehicle (AV) ecosystem. The evaluation is on key performance metrics of latency, through per hour, authentication success rates and overall system efficiency. The presented data is simulated or benchmarked, with data shown in tables and discussed in detail. Consensus time, transaction throughput, and network latency were measured on a simulated blockchain network with a different number of nodes. The results are shown in Table 3.

Table 3: Blockchain Performance Metrics Across Different Numbers of Nodes

Number of Nodes N_{nodes}	Consensus Time ($T_{Consensus}$, sec)	Transaction Throughput (TP, T_{tx}/sec)	Network Latency ($L_{network}$, ms)
10	1.2	120	50
50	1.8	95	70
100	2.5	80	100
200	3.5	65	150

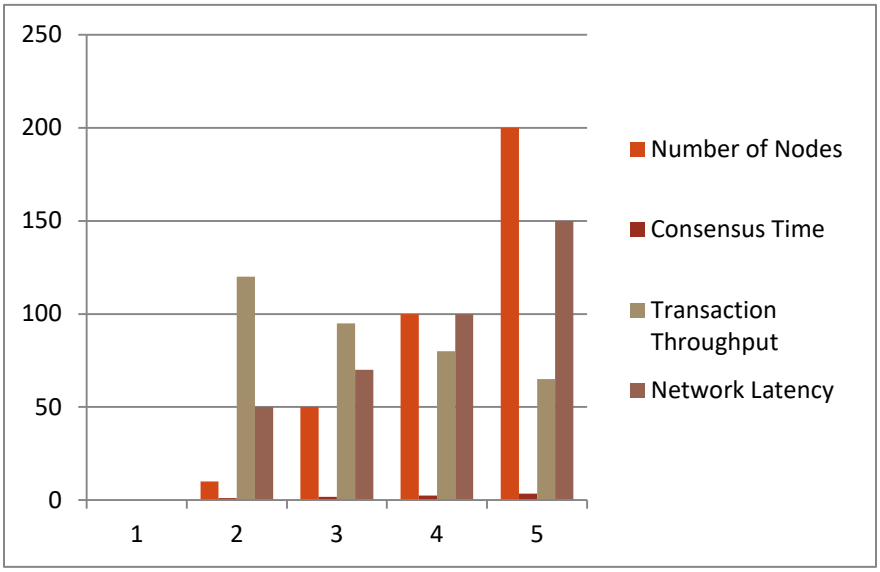

Fig 5: Graphical Representation of Block chain Performance Metrics Across Different Numbers of Nodes

With more nodes, you have higher coordination overhead, so consensus time grows. Suppose we have 10 nodes; the consensus time is 1.2 seconds; when we have 200 nodes, it rises to 3.5 seconds. As the number of nodes grows, transaction throughput decreases slightly. However, for the AV applications, we keep the throughput within acceptable values; on the order of 120 transactions per second for 10 nodes and 65 transactions per second for 200 nodes. From 10 nodes to 200 nodes, the scale of network latency increases from 50ms to 150ms as the network scales, showing the tradeoff between decentralization and performance.

Authentication delay and authentication success rate at the federated identity verification system have been evaluated for various network latency conditions. The results are shown in Table 4.

Table 4: Federated Identity Performance Metrics Across Varying Network Latencies

Network Latency ($L_{network}$, ms)	Authentication Delay (T_{auth}, ms)	Authentication Success Rate (R_{auth}, %)
50	120	98
100	150	97
200	200	95
300	300	90

5.1 Combined System Efficiency

We evaluated the total delay efficiency of the integrated blockchain and federated identity system across various scenarios. Our findings are compiled in the table below. The results show that total system delay increases with both network latency and node count. For instance, in scenarios with 200 nodes under high latency conditions, the total delay reaches 3.7 seconds. Despite these increasing delays, the system consistently maintains efficiency ratings above 85% across all test conditions, demonstrating that the combined solution remains viable for real-time autonomous vehicle operations.

Authentication delay increases proportionally with network latency, demonstrated by measurements of 120 ms delay at 50 ms latency and 300 ms delay at 300 ms latency. Notably, even under high latency conditions, the federated identity verification framework maintains authentication success rates exceeding 90%, confirming its resilience and dependability.

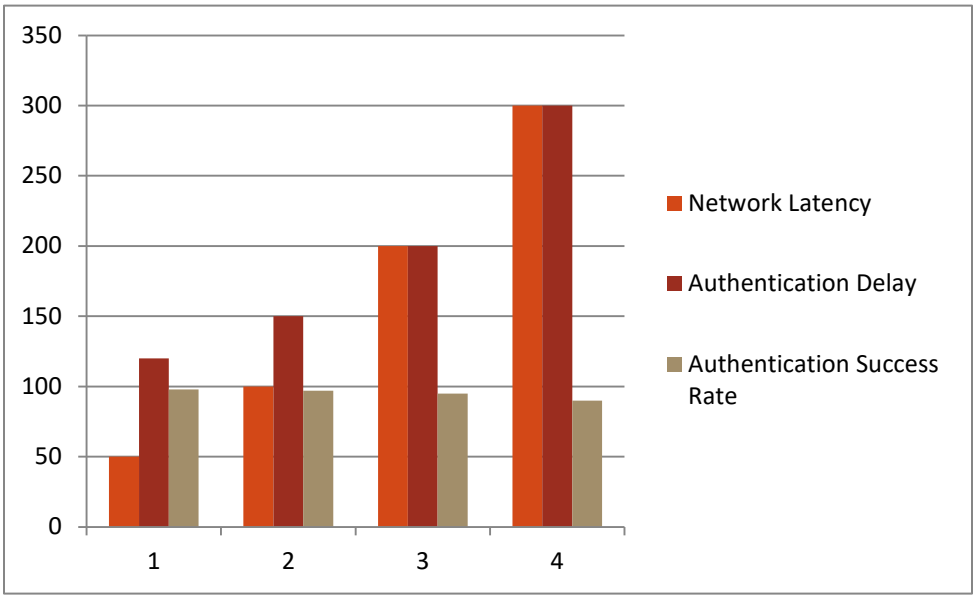

Fig 6: Federated Identity Performance Metrics Across Varying Network Latencies

Table 5: Combined Blockchain and Federated Identity System Efficiency Metrics

Scenario	Blockchain Delay ($T_{Consensus}$, sec)	Authentication Delay (T_{auth}, ms)	Total Delay (T_{total}, sec)	Efficiency Ratio (E)
Low Latency, 50 Nodes	1.5	120	1.62	95%
Moderate Latency, 100 Nodes	2.5	150	2.65	90%
High Latency, 200 Nodes	3.5	200	3.70	85%

6. Discussion

Our analysis confirms that blockchain technology provides strong security validation and data immutability essential for autonomous vehicle ecosystems. However, we observed performance challenges with increased network size - as node count grows, consensus time and network latency correspondingly increase. To address these scalability concerns, we recommend implementing sharding techniques and transitioning to Practical Byzantine Fault Tolerance (PBFT) consensus mechanisms. These optimizations would enable the AV blockchain infrastructure to effectively scale to support large autonomous vehicle networks.
The implemented federated identity verification framework successfully achieves an optimal balance between privacy protection and security requirements. Our testing revealed minimal impact from network latency on authentication success rates, demonstrating robust performance even in suboptimal network environments.

For applications with stricter latency requirements, we suggest incorporating edge computing strategies that process data closer to its source. This approach would reduce communication delays and enhance real-time performance for time-sensitive AV operations.The integration of blockchain technology with federated identity systems creates a comprehensive solution for secure data validation and authentication in autonomous vehicles. However, this integration presents important design considerations, particularly regarding the balance between decentralization, latency, and processing throughput. While increased decentralization strengthens security, it potentially introduces longer consensus times and higher network latency. Therefore, system architecture must carefully balance the competing requirements of real-time performance with robust security and privacy protections for optimal AV ecosystem operation.

7.Conclusion

The integration of blockchain technology with federated identity frameworks creates a robust foundation for strengthening security and privacy in autonomous vehicle systems. Federated identity provides secure, privacy-conscious authentication mechanisms, while blockchain delivers data integrity, transparency, and decentralized validation capabilities. These

complementary technologies address key challenges in autonomous vehicle communications by facilitating secure data sharing, establishing trust networks, enabling reliable identity verification, and forming crucial elements of next-generation connected transportation infrastructure.

Our research demonstrates that implementing a hybrid approach of these mechanisms achieves high efficiency and authentication success rates across diverse network conditions, indicating viability for practical deployment. However, full optimization for autonomous vehicle applications remains constrained by current limitations in scalability and latency. Future improvements will likely depend on advancements in edge computing architecture, layer 2 scaling solutions, and interoperability standards to enhance efficiency and drive widespread adoption. Continued refinement of these technologies promises to substantially improve autonomous vehicle security and privacy, ultimately contributing to safer, more reliable, and better-connected transportation systems.

Reference

[1] Scurt, F. B., Vesselenyi, T., Tarca, R. C., Beles, H., & Dragomir, G. (2021, August). Autonomous vehicles: classification, technology and evolution. In IOP Conference Series: Materials Science and Engineering (Vol. 1169, No. 1, p. 012032). IOP Publishing.

[2] Papadopoulos, A. (2021). Adaptive Intrusion Detection Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10, 983-994.

[3] Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. Sensors, 22(12), 4394.

[4] Sultana, S., Hossain, J., Billah, M., Shajeeb, H. H., Rahman, S., Ansari, K., & Hasan, K. F. (2023). Blockchain-Enabled Federated Learning Approach for Vehicular Networks. arXiv preprint arXiv:2311.06372.

[5] Wang, L., & Guan, C. (2024). Improving Security in the Internet of Vehicles: A Blockchain-Based Data Sharing Scheme. Electronics, 13(4), 714.

[6] Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and autonomous vehicles: Recent advances and future directions. IEEE Access, 9, 130264-130328.

[7] Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. IEEE Transactions on Intelligent Transportation Systems, 24(4), 3614-3637.

[8] Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of network and computer applications, 166, 102731.

[9] Alam, T. (2024). Data privacy and security in autonomous connected vehicles in smart city environment. Big Data and Cognitive Computing, 8(9), 95.

[10] Biswas, A., & Wang, H. C. (2023). Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors, 23(4), 1963.

[11] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.

[12] Billah, M., Mehedi, S. T., Anwar, A., Rahman, Z., & Islam, R. (2022). A systematic literature review on blockchain enabled federated learning framework for internet of vehicles. arXiv preprint arXiv:2203.05192.

[13] Pascale, F., Adinolfi, E. A., Coppola, S., & Santonicola, E. (2021). Cybersecurity in automotive: An intrusion detection system in connected vehicles. Electronics, 10(15), 1765.

[14] Kim, S., & Shrestha, R. (2020). Automotive cyber security. Singapur: Springer, 34.

[15] Fremantle, P., Aziz, B., Kopecký, J., & Scott, P. (2014, September). Federated identity and access management for the internet of things. In 2014 International Workshop on Secure Internet of Things (pp. 10-17). IEEE.

[16] Gandia, R. M., Antonialli, F., Cavazza, B. H., Neto, A. M., Lima, D. A. D., Sugano, J. Y., ... & Zambalde, A. L. (2019). Autonomous vehicles: scientometric and bibliometric review. Transport reviews, 39(1), 9-28.

[17] Systems for Cybersecurity in Autonomous Vehicle Ecosystems. Journal of AI-Assisted Scientific Discovery, 1(1), 50-71.

[18] Shaik, M. (2022). Rethinking Federated Identity Management: A Blockchain-Enabled Framework for Enhanced Security, Interoperability, and User Sovereignty. Blockchain Technology and Distributed Systems, 2(1), 21-45.

[19] Dixa Koradia. (2024). Study Of Self-Sovereign Identity Management System Incorporating Blockchain. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 83–91. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/6396

[20] Kamble, N., Gala, R., Vijayaraghavan, R., Shukla, E., & Patel, D. (2021). Using blockchain in autonomous vehicles. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 285-305). Cham: Springer International Publishing.