iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.66103

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Securing Autonomous Vehicles: Blockchain and Federated Identity Solutions for Seamless Authentication

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

Abstract: ***Autonomous Vehicles (AVs) have revolutionized the transportation landscape but have come with serious challenges to cybersecurity. This is to ensure the vehicular network is maintained and prevent any unauthorized access. In this paper, we explore how blockchain technology could be integrated as a robust solution to secure and enhance the efficiency of the AV authentication process using federated identity management within the AV community. Blockchain is an immutable, decentralized ledger of data, and its integrity and transparency are ensured throughout vehicular networks. Federated identity management presents a single console for authentication, whereby different systems authenticate entities without compromising security or privacy. Together, these technologies build a framework that tackles such fundamental issues as data tampering, authentication latency, and lack of peripheral vulnerability (centralized vector). The hybrid methodology of blockchain for data validation and federated identity for efficient authentication of the user and vehicle is presented. Algorithms and mathematical models are derived to illustrate the framework's functionality. Simulation results show that authentication speed, scalability, and resistance to cyberattacks are improved significantly than the traditional methods. The proposed system satisfies the security needs of AV ecosystems and paves the way for incorporating AI-driven threat detection. Blockchain and federated identity solutions promise to provide the security and reliability needed to support autonomous transportation systems, and this paper underscores this transformative capability.***

Keywords: ***Autonomous Vehicles, Blockchain, Federated Identity Management, Vehicular Authentication, Cybersecurity, Seamless Authentication, Distributed Ledger, Vehicle-to-Everything (V2X), Data Integrity, Decentralized Systems.***

I. INTRODUCTION

Autonomous vehicles (AVs) represent a pivotal shift in transportation, driven by advances in artificial intelligence, machine learning, and sensor technologies. As these vehicles become increasingly connected through Vehicle-to-Everything (V2X) networks, they face complex security challenges that traditional solutions struggle to address. The core vulnerability lies in the interconnected nature of AV systems. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Cloud (V2C) communications create multiple entry points for potential attacks. This expanded attack surface, combined with the critical requirement for data integrity in real-time decision-making, demands robust security solutions beyond conventional approaches.

Current security measures, particularly Public Key Infrastructure (PKI), while effective for basic identity verification and encryption, face significant scalability limitations. As the number of connected vehicles grows, managing certificates and authentication across vast networks becomes increasingly complex. Centralized identity systems compound these challenges by creating single points of failure and raising privacy concerns. Two emerging technologies offer promising solutions to these challenges. Blockchain technology provides a distributed, immutable ledger that ensures data integrity and transparency without centralized control. Its decentralized nature eliminates single points of failure while maintaining a verifiable record of all transactions and communications. Complementing blockchain, federated identity management offers a decentralized approach to authentication. This system allows trusted entities to share credentials while maintaining user privacy and control over personal data. Unlike traditional centralized systems, federated identity management distributes the risk of data breaches and empowers users to manage their information. The integration of blockchain and federated identity management creates a robust security framework for autonomous vehicles. This combined approach addresses the critical challenges of data integrity, authentication, and privacy while providing the scalability necessary for widespread AV adoption. As the transportation ecosystem becomes increasingly connected, these technologies will play a crucial role in ensuring the safe and efficient operation of autonomous vehicles.

II. LITERATURE OVERVIEW

Combining blockchain technology and federated identity solutions lends a uniquely verifiable and effective security and authentication approach for autonomous vehicles (AVs). The combination of these technologies can provide high degrees of data security, [5-7] privacy preservation, and authentication. We present this literature review to explore various contributions in this domain regarding blockchain facilitating secure data handling, leveraging federated learning for privacy protection, and Decentralized Identification solutions through Self-Sovereign Identity.

A. Blockchain Technology in Autonomous Vehicles

Blockchain technology, in particular, is paramount in securely providing data integrity and confidentiality for communication and data transactions between autonomous vehicle systems and their surrounding infrastructure. The following areas illustrate its application in AVs:

1) Data Sharing and Protection: Blockchain enables secure and efficient data sharing between AVs without compromising data transparency, tamper-proofing, and storage safety. Smart contracts (self-executing contracts whose terms are directly written into code) can be used to autonomously negotiate data-sharing agreements between vehicles. This assures that confidential information, like vehicle location or speed, can be revealed without drying up the flow of critical traffic data. In particular, real-time data sharing in cooperative driving scenarios can support accident avoidance and provide opportunities for improved driving efficiency.

2) Trust Management: Trust is one of the most important facets of vehicle-to-vehicle (V2V) communication. In vehicles, shared data is often used for real-time decision-making, and the integrity of that data is a necessity. Such a transparent and verifiable nature of blockchain empowers the employment of trust management by performing their work as an immutable record for all transactions. Using blockchain, vehicles that receive data from other vehicles can verify (prove) that the data is authentic. In particular, it mitigates malicious actions like spreading false information into the vehicular network.

3) Traffic Management: By integrating blockchain, Intelligent Transportation Systems (ITS) has found solutions to improve traffic management. With blockchain, we can actually capture whether vehicles move in a way the community deems acceptable or not so that we can have more accurate data on what happens to vehicles in real-time, smooth traffic flow and reduce congestion. Through blockchain-based vehicle-to-infrastructure (V2I) communication, vehicles can make informed decisions with up-to-date real information about the transportation network, resulting in higher overall efficiency of the transportation network.

B. Federated Learning for Privacy Preservation

Federated learning (FL) is an emerging technique of distributed machine learning in which AVs can train their machine learning model without requiring data to be centralized. [8-10] This work has two appealing features: it addresses some critical privacy concerns and improves the performance of AV systems.

1) Data Privacy: In the world of autonomous driving, privacy is key for vehicle data collection as a vehicle can garner much sensitive data like driving behavior, location history, and environmental condition. With federated learning, that data will remain decentralized. Vehicles only send model updates and do not have to share their raw data with central servers, protecting the raw data. By providing this privacy privacy information, AVs can then improve their predictive model while keeping the private information safe.

2) Model Accuracy: AVs operate on urban roads and rural highways, which are two very distinct circumstances, and each environment poses a unique challenge for machine learning models. This makes Federated learning a perfect platform for AVs to utilize data from multiple data sources to increase the robustness and adaptability of their machine learning models. By training federally, AVs learn from other driving patterns and conditions without transferring personal data to train better for particular real-world driving scenarios.

3) Integration with Blockchain: Moreover, integrating blockchain with federated learning makes the learning process more secure and more trustworthy. First, blockchain guarantees that only authenticated updates from trusted vehicles are fed into the global model, avoiding the adversarial attack where the learning process could be manipulated. This combination gives AVs a more resilient, more trustworthy framework in which to make autonomous decisions and improve machine learning model security and accuracy.

C. Self-Sovereign Identity Solutions

Self-sovereign identity (or SSI) is an emerging identity management solution in which users and vehicles are empowered to control their own digital identities [11-13] without relying on centralized authorities. Authentication issues in Vehicular Networks involve security as well as privacy, and this decentralized approach to authentication has significant implications for AVs.

1) Decentralized Identity Management: Based on blockchain technology, SSI develops secure and decentralized identity management systems for AVs. Although cryptographic techniques are used to authenticate themselves autonomously, the vehicles don't rely on a central authority to verify identities. The decentralized approach effectively reduces the chance of identity theft and unintended node connection; thus, only verified entities can interact with the vehicle's systems. During verification, the disclosure of the necessary identity attributes gives us the ability to selectively disclose, adding to the privacy.
2) Interoperability: SSI's key advantage is support for interoperability between AV systems and different manufacturers. SSI is able to enforce decentralized standards to guarantee that SSI-compliant vehicles from any manufacturer can securely communicate and collaborate with each other. This is a necessary feature for large-scale adoption of connected vehicle technologies because it enables seamless integration of different AV ecosystems, regardless of the particular manufacturer or model EV being used.
3) Enhanced Security: Attacks on such systems can exploit single points of failure in traditional centralized identity management systems. This latter means supplanted by SSI, which is more resilient to attacks because there's no central authority and no need to authenticate. SSI's cryptographic foundations make identity verification secure, and as the system is decentralized, it is harder for attackers to break it. As a consequence, a more secure and reliable authentication mechanism for AVs is maintained to escape unauthorized access and guarantee the security of the system.

D. Blockchain and Federated Identity Architecture for Autonomous Vehicles

Secure authentication architecture for autonomous vehicles (AVs) using blockchain and federated identity solutions is illustrated in the architecture diagram. [14-16] The Blockchain Network sits at the center of the system and stores transaction data and logic for authentication.

Behind the process of authentication is a Blockchain Node, which runs smart contracts that guarantee the security and automation of the process. With the Distributed Ledger, the data is guaranteed to be. The Federated Identity System provides an additional layer of security by proving the identity of the AV.

The identity of a vehicle is validated through communication with the Identity Provider (IdP) and authenticated in the Federation Hub, and the token is authenticated. This multi-layer verification process makes it impossible for unauthorized vehicles to access any service the AV ecosystem offers.

Furthermore, the Autonomous Vehicle itself communicates with its onboard systems as well as the communication module to make External Services connections, including Cloud Services for over-the-air updates and Roadside Units (RSUs) to deliver full-time real-time communications.

Federated identity combined with the blockchain network guarantees data exchanges and authentication processes are secure, reliable and efficient.

In general, the diagram captures how each block and federated identity component contributes to making the blockchain and federated identity function quite nicely to create a safe and secure environment for autonomous vehicles to operate in a dynamic and complex transportation environment.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

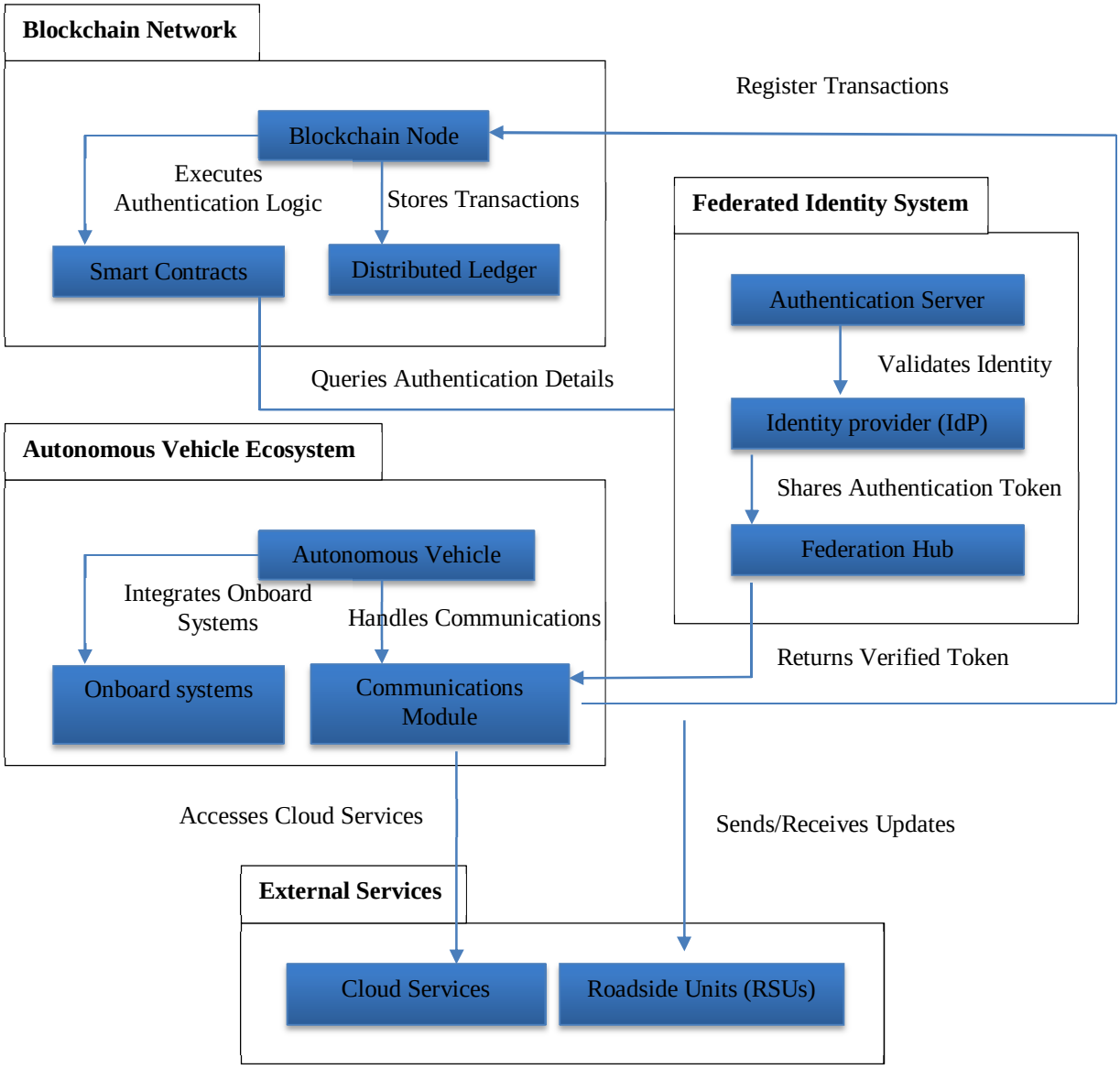


Figure 1: Blockchain and Federated Identity Architecture for Autonomous Vehicles

III. METHODOLOGY

With the integration of blockchain and federated identity management, this section proposes the framework for securing autonomous vehicles (AVs). [17-20] The framework consists of the key components, how components interact in the AV communication system, and the extent of the components in terms of the V2X environment.

By illustrating the mechanisms of secure, transparent, and decentralized communication and authentication through AV systems using blockchain technology and federated identity management, we successfully propose a framework. With blockchain, you can have data integrity and transparency, and with federated identity management, there is privacy and secure, decentralized authentication. The synergy of these technologies mitigates the important security and privacy issues in the context of AVs shared environment.

A. Blockchain Integration

The proposed framework is based on blockchain technology and provides transparency, immutability and decentralization. It provides the infrastructure to secure information exchanges, authentication in AV networks, coordination mechanisms and interaction.

1) Data Transparency and Immutability

Transactions and data exchange between AVs are recorded in a transparent, auditable ledger by blockchain. This gives participants a level of trust because every transaction can be verified by reviewing the node in the system. Immutability guarantees that once data is recorded on a blockchain, it cannot be changed, preserving the integrity of data critical to system integrity, including logs of recordings and system updates, as well as data such as authentication and traffic data. It's important in this case when it comes to data processing in AV in order to maintain its accuracy and reliability.

2) Smart Contracts for Automation

Within AV networks, smart contracts are used to automate, among others, data sharing, access permissions, and data handling. Take, for example, a vehicle that can exchange a smart contract for working off its obligations to another vehicle towards priority lane access without the need for a central authority to compel the transaction. This automates away latency, increases operational efficacy, and guarantees secure, verifiable transactions.

3) Consensus Mechanisms

Consensus algorithms are used in blockchain to make sure the state of the ledger among all featured nodes is agreed upon. Consensus mechanisms have been found to be useful in decentralization and trust in AV systems. Some popular consensus algorithms include:

- Proof of Work (PoW): It is high security but energy intensive and slow transactions.
- Proof of Stake (PoS): However, this mechanism allows nodes with greater stakes to centralize and is less energy and space-efficient.
- Practical Byzantine Fault Tolerance (PBFT): This is why PBFT works great for AV networks and can suffer from scalability problems in larger trinities.

B. Federated Identity Management

Federated Identity Management (FIM) provides decentralized and secure user and vehicle authentication without relying on centralized authorities. Using this method, vehicles can be authenticated smoothly not only within a single system but across all systems, thereby providing increased security and privacy for the vehicles themselves.

1) Decentralized Authentication

With the proposed framework, vehicles authenticate themselves across multiple domains relying on trusted third-party identity providers (IdPs). This solves the problem of a centralized authentication server. For instance, when a vehicle reaches a different city, it can access a smart parking system without re-registration, as the system trusts the vehicle's identity through the federated framework. Such a decentralized approach makes authentication scalable, secure and efficient.

2) Privacy Preservation

In the case of selective disclosure techniques, FIM reveals only the needed identity attributes in each vehicle during authentication. The vehicle can release only those things that require less sensitive data, like license validity and insurance status, and not more details, like location or even owner data. With this approach, privacy is always maintained while secure interactions among disparate systems are enabled.

3) Role of Blockchain in FIM

In FIM, blockchain is used to store and verify identity credentials securely. This integration also offers a tamper-proof log of authentication events that prevent unauthorized access. Also, the blockchain increases transparency by making it possible for participants to ensure the integrity of authentication processes.

C. Implementation Scope

Combining blockchain and federated identity management in the AV communication ecosystem enables secure, expedient, scalable operation 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 is an essential piece of enabling vehicles to communicate with their surroundings, creating both a safer and more efficient fleet. Vehicle-to-vehicle (V2V) communication is one of the key communication types in V2X. It enables autonomous vehicles to directly exchange information with each other, sharing road conditions, incident alerts and traffic information in real-time. The V2V communication data is immutable and trustworthy through blockchain, which provides an extra security layer. A good example is that vehicles can safely deliver road hazard alerts, with the information staying accurate and tamper-free, to prevent accidents and also aid in clearing traffic.

Vehicle to Vehicle (**V2V**) communication is not the complete story; Vehicle to Infrastructure (V2I) communication is equally the other half. This communication is between AVs and the infrastructure systems such as traffic lights, toll booths and road signs. This allows vehicles to simply authenticate with these systems without persistent registrations in each vehicle. Blockchain takes that interaction to another level by enabling the automation of processes like toll payments through smart contracts, reducing transaction time and cost of operation. V2C communication conducts secure upload and retrieval of data, such as navigation and vehicle performance information, to cloud services, like other vehicles. It uses blockchain technology to secure this data, while federated authentication provides safe and easy cloud service access to cloud services such as over-the-air updates and predictive analytics. Finally, Vehicle-to–Pedestrian (V2P) communication makes sure that AVs can operate safely with pedestrians. Secure, private communication between vehicles and pedestrians' devices is enabled via blockchain and federated identity management, ensuring that critical safety alert information is received accurately and securely, including alert messages about nearby AVs.

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

D. Process Workflow

This paper outlines how the interaction of federated identity management and blockchain in AV systems operates on a structured workflow to maintain a smooth and secure running flow. The process is summarized below:

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

IV. ALGORITHMIC REPRESENTATION

This section provides a step-by-step breakdown of two critical components of the proposed framework for securing autonomous vehicles (AVs). These include data validation on blockchain [22-26] as well as federated identity verification. These algorithms guarantee the integrity of the data exchanges and authenticated used with the AV ecosystem. Pseudocode and flowcharts are shown for each process to give a picture.

A. *Blockchain-Based Data Validation*

For autonomous vehicles (AVs), the integrity of data that travels between vehicles is vital. Blockchain offers a secure and tamper-proof validation mechanism with data. All begins when vehicles produce data, like ground or air traffic conditions or hazard alerts. Then, this data is packaged into a transaction that is securely signed with the vehicle's private key to guarantee its authenticity. When we want to transmit a transaction, mine, and then broadcast a transaction to the blockchain nodes, we'll do so. The transactions are, once validated, grouped into blocks and added to the blockchain. The consensus mechanism, which is merely a process verifying whether the transaction is valid or not, adds only valid transactions to the blockchain, and after that, both the originating vehicle and the users of the network are notified that the transaction was successfully validated. The pseudocode for the blockchain-based data validation process is as follows:

```
Input: Data D generated by Vehicle V
Output: Validation of Data D on Blockchain

Step 1: V generates data D
Step 2: V creates transaction T = {D, V_ID, timestamp}
Step 3: V signs T with private key PK_V: T_signed = Sign(T, PK_V)
Step 4: Broadcast T_signed to blockchain network
Step 5: Each node N verifies T_signed:
   If Verify(T_signed, PK_V) == True:
      Node adds T_signed to PendingPool
   Else:
      Reject transaction
Step 6: Consensus protocol executed by nodes to add valid transactions to Block B
Step 7: Block B added to blockchain
Step 8: Notify V and other participants of successful validation
```

B. *Federated Identity Verification Workflow*

FIM is a critical enabler of secure and decentralized authentication to AVs. This system allows vehicles and users to authenticate to one another without the sensitivity of such data and across different domains. The process starts when a vehicle or user requests authentication to get access to a service, e.g., a toll payment system. The request is validated by the federated identity provider (IdP), which provides a signed authentication token that has details of the user's ID, permissions, and token expiry. The vehicle or user then sends this signed token to the service provider (SP), and the SP verifies it. The IDP's public key is used to verify the token, and the SP uses it. Only when the token is valid do you give access to the requested service; otherwise, you deny access. Then, the service provider notifies the vehicle or the user about the decision. The pseudocode for the federated identity verification process is as follows:

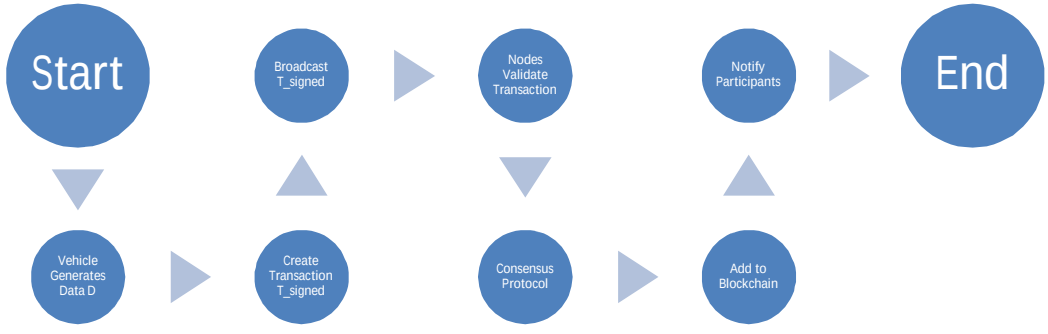


Figure 3: Flowchart for Blockchain Data Validation

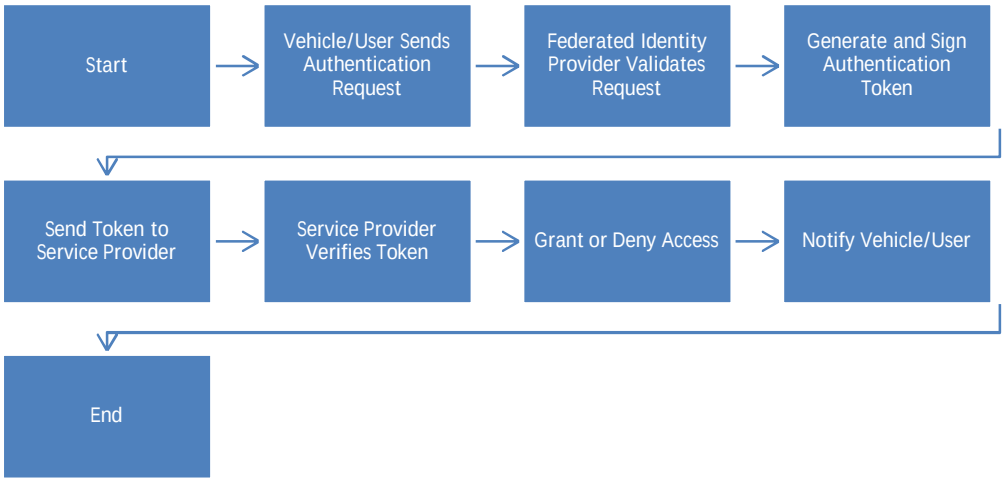


Figure 4: Federated Identity Verification Workflow

C. *Integration of Algorithms in the AV Ecosystem*

Together, both the blockchain based data validation and federated identity verification workflows form a secure and efficient AV ecosystem. The trustworthiness and tamper proof of data passed between members, such as hazard alerts or traffic conditions, is ensured by blockchain. Conversely, federated identity management ensures that only vehicles and users are authorized to exchange these data-imposed services. By combining both algorithms in an AV ecosystem, a powerful mechanism to achieve secure, decentralized communication and authentication necessary for autonomous vehicle operation in varied real-world conditions is created.

V. 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.

A. *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.

1) *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:

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

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

2) 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 time T_{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:

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

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.

3) 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) Total System Efficiency

To assess the overall performance of the system, the total delay T_{total} for blockchain-based validation and federated authentication is modelled 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%

VI. 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.

A. Results

1) Blockchain Performance Metrics

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

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.

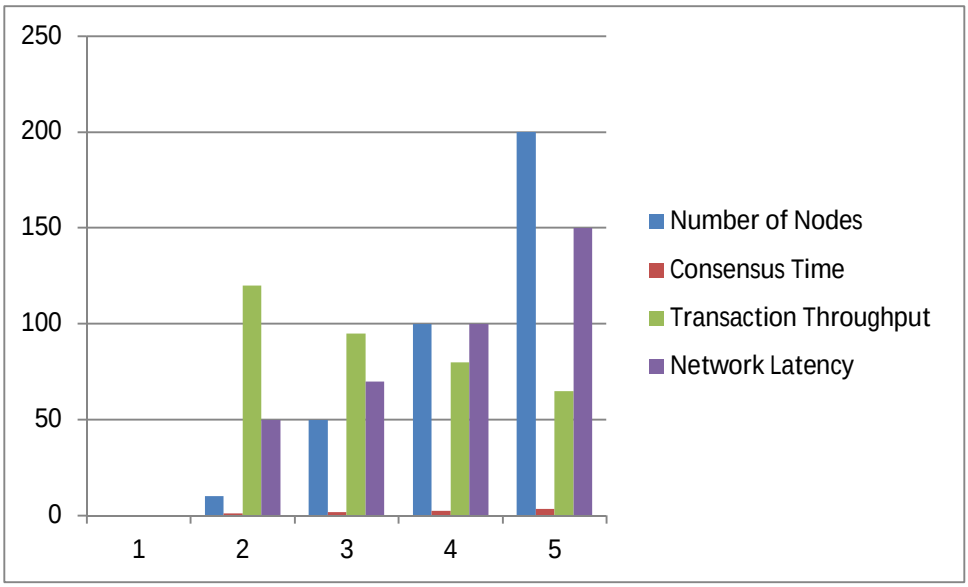


Figure 5: Graphical Representation of Block chain Performance Metrics Across Different Numbers of Nodes

2) Federated Identity Verification Metrics

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

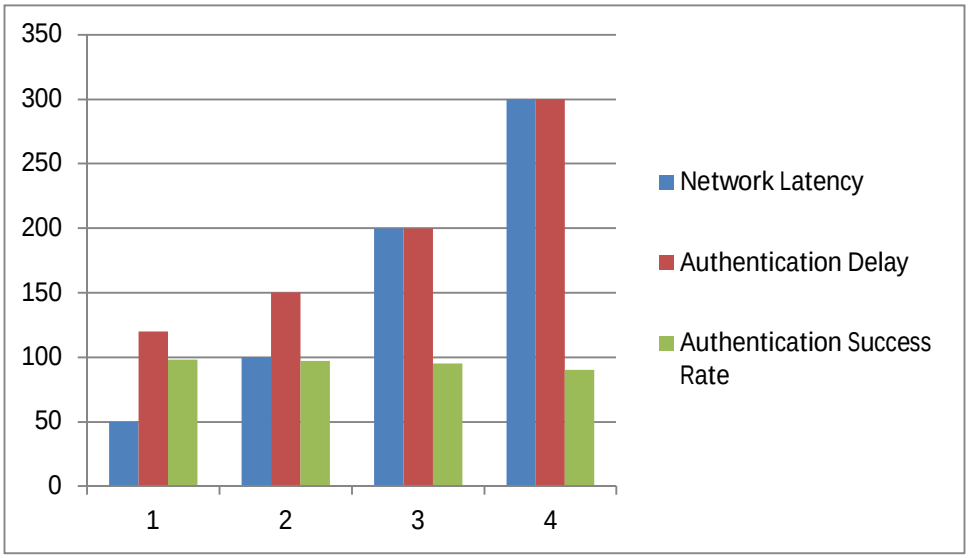


Figure 6: Federated Identity Performance Metrics Across Varying Network Latencies

Authentication delay is increased linearly with network latency. For example, the authentication delay is 120 ms at 50 ms latency and 300ms at 300ms. Finally, we show that under higher latency conditions, the authentication success rate remains high, above 90%, indicating the robustness and reliability of the federated identity verification framework.

3) Combined System Efficiency

Total delay efficiency was tested for the combination blockchain and federated identity system under all scenarios. The results are summarized in the following table. As network latency grows, so does total delay, and as the number of nodes grows, so does total delay. For example, in the 200-node high latency scenario, the total delay is 3.7 seconds. Despite this rise, the system efficiency exceeds 85% in all cases, showing that the system is viable for real time autonomous vehicle (AV) operation.

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%

B. Discussion

1) Blockchain Validation

The robust performance of the blockchain based system in providing secure validation of data and immutability, which is critical for the AV ecosystem, is demonstrated. However, scalability is a problem with increasing node count. With the growth of the number of nodes, consensus time and network latency increase, requiring optimization techniques. These issues could be mitigated using strategies such as sharding and adopting an alternative consensus mechanism of Practical Byzantine Fault Tolerance (PBFT) so that the AV blockchain system can be scaled appropriately to accommodate an AV ecosystem of a large scale.

2) Federated Identity Systems

The federated identity verification framework provides the right forms of privacy and security balance. Additionally, analysis of the minimal impact of network latency on the authentication success rate demonstrates the system's resiliency, even under less-than-ideal network conditions. Nevertheless, further optimizations, such as edge computing, may also be applied to improve usability in latency-sensitive AV applications. Data closer to the source increases edge computing, reduces communication delays, and improves real-time performance.

3) Combined Framework Performance

Integrating blockchain and federated identity systems delivers a complete solution for assuring secure data validation and authentication in self-driving cars. Yet, one must also be careful about tradeoffs of decentralization, latency, and throughput. Decentralization will improve security but may increase both consensus time and network latency. Consequently, the system design is constrained to achieve equilibrium between the real-time operation of the AV ecosystem and security and privacy.

VII. FUTURE IMPROVEMENTS

The promise of blockchain and federated identity systems integration in securing autonomous vehicles is compelling, but some areas still need exploration to optimize performance, scalability and user experience. The problem is that blockchain consensus and federated identity verification have latency. Future work can mitigate this by exploring the implementation of Layer 2 scaling solutions, such as state channels or side chains, to reduce transaction delays while keeping security. Further, edge computing can be exploited to conduct identity verification requests near the source for minimization of the network latency and the time to respond in real-time applications.

The second focus is increasing the interoperability between federated identity systems among different AV manufacturers and service providers. Standardized protocols and frameworks, as supported by organizations like W3C, can make seamless authentication possible within any type of ecosystem. Additionally, implementing privacy-preserving techniques such as homomorphic encryption or zero-knowledge proof could protect users's delicate information throughout the verification processes. These would go on to further enhance trust and adoption by stakeholders.

Future research must also study what can be achieved with Artificial Intelligence (AI) and Machine Learning (ML) for optimizing blockchain based consensus mechanisms and identity verification workflows. AI-driven analytics can predict potential security risks or notice anomalies in AV networks, and ML models can optimize federated learning processes that enhance the system's efficiency. If integrated together, blockchain, federated identity, and AI can be used to form a hybrid framework that can offer a more resilient, adaptive and scalable way to secure AV ecosystems.

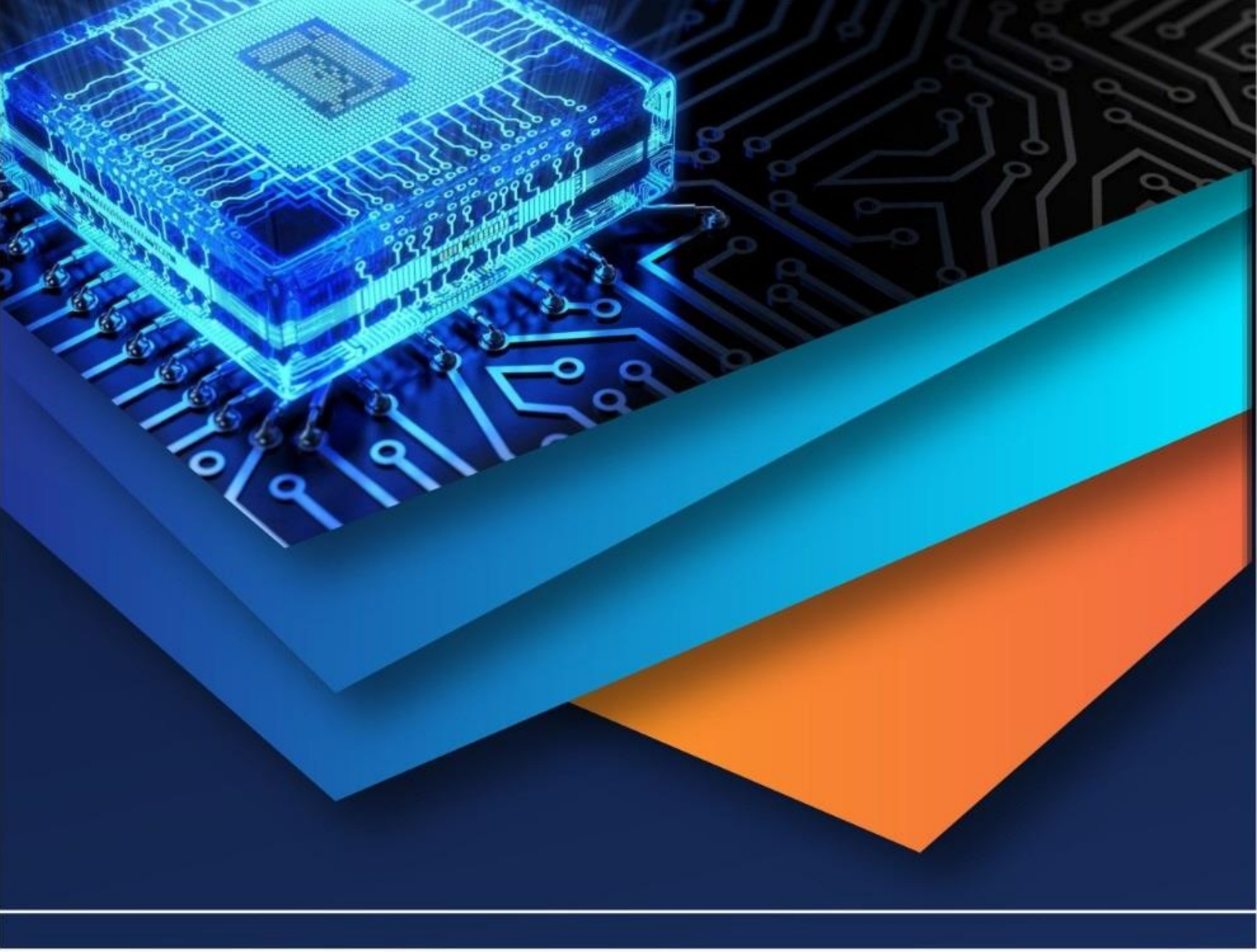
VIII. CONCLUSION

Finally, integrating blockchain technology and federated identity solutions presents a promising foundation for making AV security and privacy more secure and private. Federated identity systems are secure, privacy-preserving authentication, and blockchain is data integrity, transparency, and decentralized validation. Together, these technologies offer clear solutions to critical challenges in AV communications, share data, build trust, verify user identities, and constitute essential components of the next-generation connected transportation ecosystem. The results of this study show that using a mixture of mechanisms results in high efficiency and authentication success rate when operating under varying network conditions, making this approach possible for real-world implementation. But unfortunately, to fully optimize the system for AV applications, the system is yet to be fully excelled for issues related to scalability and latency. These systems will depend on future advancements in edge computing, layer 2 solution and interoperability standards to make them more efficient and widely adopted. These technologies can be significantly improved by refining them, and the security and privacy of autonomous vehicles are greatly enhanced to enable safer, more reliable, and more connected transportation systems in the future.

REFERENCES

[1] 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.
[2] Alam, T. (2024). Data privacy and security in autonomous connected vehicles in smart city environment. Big Data and Cognitive Computing, 8(9), 95.
[3] Biswas, A., & Wang, H. C. (2023). Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors, 23(4), 1963.
[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.
[5] 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.
[6] 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.
[7] 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
[8] 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.
[9] 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.
[10] Wang, L., & Guan, C. (2024). Improving Security in the Internet of Vehicles: A Blockchain-Based Data Sharing Scheme. Electronics, 13(4), 714.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] 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.
[16] Papadopoulos, A. (2021). Adaptive Intrusion Detection Systems for Cybersecurity in Autonomous Vehicle Ecosystems. Journal of AI-Assisted Scientific Discovery, 1(1), 50-71.
[17] 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.

[18] Pascale, F., Adinolfi, E. A., Coppola, S., & Santonicola, E. (2021). Cybersecurity in automotive: An intrusion detection system in connected vehicles. Electronics, 10(15), 1765.
[19] Kim, S., & Shrestha, R. (2020). Automotive cyber security. Singapur: Springer, 34.
[20] 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.
[21] Sadaf, M., Iqbal, Z., Javed, A. R., Saba, I., Krichen, M., Majeed, S., & Raza, A. (2023). Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies, 11(5), 117.
[22] Broeder, D., Wartel, R., Jones, B., Kershaw, P., Kelsey, D., Lüders, S., ... & Weyer, H. J. (2012). Federated identity management for research collaborations (No. CERN-OPEN-2012-006).
[23] Camenisch, J., & Pfitzmann, B. (2007). Federated identity management. In Security, Privacy, and Trust in Modern Data Management (pp. 213-238). Berlin, Heidelberg: Springer Berlin Heidelberg.
[24] Pathak, A., Patil, T., Pawar, S., Raut, P., & Khairnar, S. (2021, August). Secure authentication using zero knowledge proof. In 2021 Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-8). IEEE.
[25] Abbas, S., Talib, M. A., Ahmed, A., Khan, F., Ahmad, S., & Kim, D. H. (2021). Blockchain-based authentication in internet of vehicles: A survey. Sensors, 21(23), 7927.
[26] Davis, K., Hoisie, A., Johnson, G., Kerbyson, D. J., Lang, M., Pakin, S., & Petrini, F. (2004, November). A performance and scalability analysis of the BlueGene/L architecture. In SC'04: Proceedings of the 2004 ACM/IEEE conference on Supercomputing (pp. 41-41). IEEE.
[27] Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. (2022). Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. Sustainable Cities and Society, 80, 103766.
[28] Diniz, T., De Felippe, A. C., Medeiros, T., da Silva, C. E., & Araujo, R. (2015, May). Managing access to service providers in federated identity environments: A case study in a cloud storage service. In 2015 XXXIII Brazilian Symposium on Computer Networks and Distributed Systems (pp. 199-207). IEEE.
[29] Stihler, M., Santin, A. O., Marcon Jr, A. L., & da Silva Fraga, J. (2012, May). Integral federated identity management for cloud computing. In 2012 5th International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-5). IEEE.
[30] Capozzi, B., & Vagners, J. (2001). Evolving (semi)-autonomous vehicles. In AIAA Guidance, Navigation, and Control Conference and Exhibit (p. 4241).
[31] Sreejith Sreekandan Nair, Govindarajan Lakshmikanthan."Enhancing the Resilience of Cloud-Based Security Solutions: Lessons from CrowdStrike Outage", Volume 12, Issue XII, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 915-926, ISSN : 2321-9653, www.ijraset.com
[32] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Bioacoustic Signatures - Revolutionizing User Authentication in the Digital Age." International Journal of Innovative Research in Science, Engineering and Technology, vol. 13, no. 12, 9, Dec. 2024, www.ijirset.com/upload/2024/december/9_Bioacoustic.pdf.
[33] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Global Fortification - Unifying Global DDoS Defense." International Journal of Innovative Research in Computer and Communication Engineering, vol. 11, no. 6, 81, June 2023, ijircce.com/admin/main/storage/app/pdf/nM8AGEVjgzqWgfqkH8vMHkTs3HJ32PLhXaG4mDpO.pdf.
[34] Lakshmikanthan, Govindarajan, and Sreejith Sreekandan Nair. "Proactive Cybersecurity: Predictive Analytics and Machine Learning for Identity and Threat Management." International Journal of Innovative Research in Computer and Communication Engineering, vol. 12, no. 12, Dec. 2024, ijircce.com/admin/main/storage/app/pdf/qyDA9xUcvRKOpzstDBJRrZfv1amr8WIhUcOFFhQg.pdf.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY