Proceedings Paper:
Alhabib, Reem and Yadav, Poonam orcid.org/0000-0003-0169-0704 (2024) Hyperledger Fabric Platform for Secure and Efficient Data Sharing in Autonomous Vehicles. In: Zaidi, Syed Ali Raza, Ibrahimi, Khalil, El Kamili, Mohamed, Kobbane, Abdellatif and Aslam, Nauman, (eds.) Proceedings - 11th International Conference on Wireless Networks and Mobile Communications, WINCOM 2024. 11th International Conference on Wireless Networks and Mobile Communications, WINCOM 2024, 23-25 Jul 2024 Proceedings - 11th International Conference on Wireless Networks and Mobile Communications, WINCOM 2024 . IEEE Communications Society , GBR

https://doi.org/10.1109/WINCOM62286.2024.10657518

Hyperledger Fabric Platform for Secure and Efficient Data Sharing in Autonomous Vehicles

Reem Alhabib
Department of Computer Science
University of York
York, UK
reem.alhabib@york.ac.uk

Poonam Yadav
Department of Computer Science
University of York
York, UK
poonam.yadav@york.ac.uk

***Abstract*—Advancements in wireless communication, encompassing cellular and non-terrestrial networks, are empowering Autonomous Vehicles (AVs) to revolutionize transportation. The achievement of real-time data exchange and seamless communication with infrastructure promises a future of safer and more efficient travel. However, the significant challenge of efficiently managing the extensive data generated by AVs persists. This data includes sensor readings, information about the surrounding environment, and potentially user data. Consequently, addressing concerns related to data processing, sharing among various stakeholders, privacy, integrity, and security is of utmost importance. This paper tackles the data sharing challenge by proposing and evaluating a platform built on Hyperledger Fabric, a blockchain technology. This platform aims to facilitate secure and efficient data sharing between all parties involved with AVs. Our initial testing reveals that the number of simulated users (virtual user count) and the amount of data processed (data load) can negatively impact the system's performance. This highlights the need for further optimization to ensure the platform can handle large-scale data sharing effectively.**

***Index Terms*—Data sharing, Security, Privacy, Blockchain, Hyperledger, Autonomous Vehicle**

I. Introduction

The emergence of autonomous vehicles (AVs) marks a significant milestone in the automotive industry, promising both safety enhancement and economic growth. Autonomous Driving Systems (ADS) operation uses mobile communication and wireless technologies, facilitating the smooth exchange of real-time data from sensors and cameras to steer driving decisions. Within this technological innovation, though, managing vast volumes of data generated by these sensors and other environmental entities remains a significant challenge that calls for efficient handling, storing, processing, and sharing methods [1]. Specifically, extensive exploration of AV data emphasises the diverse stakeholders reliant on this data. As each party in this field independently manages its data, the lack of data sharing hinders collaborative efforts and holistic insights. For example, data sharing in case of accidents is essential for investigation purposes, enabling a comprehensive analysis and contributing to ongoing safety improvements through collective insights. This paper underscores the need for data-sharing frameworks prioritising security, privacy-preservation, and integrity. Conventional centralised platforms encounter numerous challenges, including potential security vulnerabilities, privacy concerns, and a lack of scalability in managing the growing volume of diverse data [2]. However, in recent years, alternative solutions have emerged that aim to overcome the limitations of centralisation, such as distributed ledger technology. The inherent characteristics of blockchain, including decentralisation, immutability, integrity, and auditability, position this as an ideal solution for developing a secure and reliable data-related application [3]. Blockchain has revealed promise in data sharing, although its feasibility and impact on AV on static data remain insufficiently investigated. Hence, the objective of the current study is to examine the feasibility of implementing a blockchain-based data-sharing system in the context of AVs. Hyperledger Fabric (HLF) blockchain technology [4] has been employed is a private blockchain solution known for its scalability and reliability. Leveraging HLF enhanced privacy and robust security, seamlessly integrating it with the InterPlanetary File System (IPFS) [5] cloud to achieve scalable data storage and a front-end application to enhance the overall user experience. Figure 1 is an overview of the three core components of the system. This investigation specifically focuses on assessing its performance, scalability, and maintaining the essential requirements for multi-party data-sharing systems, including robust security and regulatory requirements, with the current study's contributions as the following:

1) To build a fine-grained access control platform utilising Hyperledger blockchain that allows or denies requests to access data resources based on Attribute Based Access Control (ABAC) in restricting access to the specific user to have the necessary attributes in their certificate.
2) To conduct comprehensive performance assessments, including user experience and scalability by the concurrency scale of user interactions and data load.

In this study, the following vital components have been

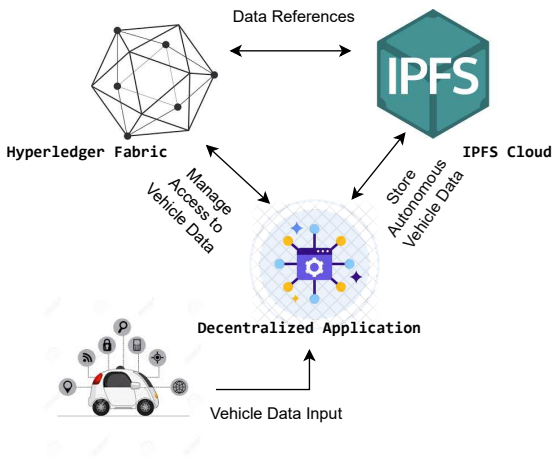

Fig. 1. **System Overview:** the synergy between the multi-party data sharing system's key components: Hyperledger, IPFS (InterPlanetary File System), and the application layer.

discussed: section II proposes the motivation for this research; section III provides brief background information; an exploration of related work in the field is in section IV; then section V rigorously explains the problem under investigation; an examination of the system architecture is explored in section VI, and VII delves into the evaluation framework, and methodically assesses the proposed solutions.

II. Motivation Scenario

Autonomous vehicles (AVs) provide extensive data, including raw and fusion data from cameras and sensors, with communication data with other vehicles and Road Side Units (RSU) contributing to a comprehensive dataset essential for understanding the environment during significant events. However, concerning data management and accessibility, two main gaps have been observed: Event Data Recorder (EDR) and Data Storage System for Automated Driving (DSSAD) in current AVs have limitations, making them ineffective even for accident-related use cases [6]. In an attempt to address some limitations, several approaches have been suggested [7]–[11], which are aimed at improving data integrity by assigning the records additional integrity levels. Additionally, the demand for AV data is significant across various domains, attracting multiple stakeholders, including government and legal authorities, Original Equipment Manufacturers (OEMs), suppliers, owners, insurance providers, testing organisations, road authorities, and researchers [12]. For example, analysing sensors' data is crucial for diagnostic purposes in autonomous cars, which rely on this data for insights into both internal system conditions and the external environment [13]. Thus, making this data available and accessible to the authorised parties is essential to feed and drive the ongoing improvement of this system in the future. Hence, the imperative for fine-grained access control for sharing this data with the authorised potential relevant stakeholders becomes vital to ensure AV data's responsible and effective utilisation across diverse applications. Subsequently, this research explores the efficiency of implementing existing data-sharing solutions, such as in [14]–[17] to address these gaps.

III. Background

This section briefly provides a contextual foundation to better understand the subject's theoretical and practical aspects.

A. Autonomous Driving System (ADS)

The National Highway Traffic Safety Administration (NHTSA) [18] defines AVs as "those vehicles in which at least aspects of a safety-critical control function (e.g., steering, throttle, or braking) occur without direct driver input". Thus, cars that alert drivers to potential dangers as a safety warning without control action are not regarded as automated. In the context of definition, the Society of Automotive Engineers (SAE) defined the international levels of driving automation. Consequently, this SAE's six-level taxonomy has become a widespread industry standard varying from level 0 (no driving automation) to level 5 (full driving automation) [19].

AVs can interact with any compatible systems, including infrastructure, pedestrians, etc. V2X technology, which stands for vehicle-to-everything communication, refers to this connection. These vehicles exchange the collected vital data in real time to make driving decisions swiftly and accurately.

B. Hyperledger Fabric (HF)

With the introduction of Bitcoin [20], one of the first real-world solutions to unresolved issues in distributed computing, the Blockchain (BC) concept was established. Hyperledger Fabric (HF) [4] is the most famous private and permissioned Blockchain that offers a platform for smart contract execution. This offers components that provide anonymity, flexibility, and scalability by defining roles between network participants.

C. Data Sharing Access Control Based on Blockchain

Attribute-Based Access Control (ABAC) is a flexible logical Access Control (AC) model limited only by the computational language and the richness of the available attributes [21]. This principle has been applied in Blockchain systems as part of the broader development of access control methods. ABAC, a concept in Blockchain data sharing control, ensures that only authorised individuals or entities can access the assets (data resources).

IV. Related Work

In this section, two key areas are examined: first, the studies that align with the current research's goal of making data events easily accessible for further investigation, and second, the current research that provides relevant insights to shape this project.

A. Critical Event Data

In analysing accident causes, data integrity preservation for AVs has been a goal for several studies that have presented frameworks based on various technologies for investigation purposes. For example, Hoque and Hasan have proposed the AVGuard tool [7], a forensic investigation framework for AVs. AVGuard is supposed to be integrated with the AV's system, and it is assumed that the AV has local storage to store the log provenance. AVs send log provenance to a remote cloud server via a Robot Operating System (ROS), using a publisher-subscriber architecture to collect logs from multiple driving modules. Correspondingly, Buquerin et al. [9] present a general concept for automotive forensics using Ethernet. Their implementation uses the onboard diagnostics interface, the diagnostics over internet protocol, and the unified diagnostic services for communication. Another work presented by Liu et al. [11] aims to safely store Event Data Recorder (EDR) data that is not open to manipulation. In their scheme, data is not only sent to the manufacturer's server as normal, but the vehicle also uploads the EDR data to a cloud server and sends the evidence of storage to the nearby vehicle through a vehicular ad-hoc network. Overall, while these studies and other existing studies in this field such as [8], [10], [22]] have contributed to ensuring the availability of event data for investigation, they fall short in facilitating effective data sharing. The researchers have primarily emphasised data integrity rather than addressing the need for sharing comprehensive and contextualised data. By acknowledging these factors, the approach in the current research stands as a pivotal effort to overcome this challenge.

B. Data Sharing

In the related literature, data management, sharing, and security have become one of blockchain's most practical research areas due to its ability to provide a secure, decentralised, and transparent framework [23], [24]. Accordingly, as shown by Alshalali et al. [14], a system for exchanging Electronic Health Records (EHR) based on Hyperledger Fabric was proposed to provide a secure way for patients to manage their data. Patients use the Hyperledger to generate cryptographic keys to enable protected data exchange and regulate patient data access. A pointer to the record is encrypted and saved on the Blockchain, while the patient's data and permissioned IDs for data access are stored in the healthcare institution's database. However, Guo et al. [25] suggested a strategy for controlling access to medical records by using Edge nodes to store EHR data. These nodes offer attribute-based access combined with blockchain in a hybrid architecture. Access Control Lists (ACLs) containing EHR data addresses are obtained on demand by healthcare providers, who then access the data using URLs. However, this hybrid design may require specialized technical knowledge for efficient operation.

Budel et al. [26] introduced an Ethereum and IPFS-based smart contract tool, vincy to guarantee data integrity and validation while investigating automated vehicle incidents in road trials, tackling uncertainties in real-world settings.

Similarly, Zhao et al. [27] offer decentralised attribute-based access control using smart contracts and symmetric key sharing across several characteristics to provide key security to prevent unwanted access. Moreover, a resource sharing on Hyperledger Fabric was presented by Liu et al. [16]. Using Blockchain technology and three various types of encryption techniques, the platform ensures the confidentiality and integrity of data. The current work shares a common objective with the research discussed in this section: to securely store the data while maintaining its integrity for analysis and other purposes. However, a distinct approach is taken by applying this goal specifically to the scenario under consideration. Hence, an investigation will determine the approach's potential to address the need for multi-party sharing in the AV context.

V. Problem Definition and Solution

While numerous objectives and entities seek access to all or part of the AVs' data, to our knowledge, no mechanism has yet been presented to bridge the need for the data-sharing gap. In the current research, the central goal is to bridge the existing gap in the literature while concurrently addressing and overcoming the limitations that have persisted, such as security, integrity, and privacy.

A. The Proposed Solution

This system is provided to develop a fine-grained access control data-sharing platform. The main components of this distributed system, which provides a secure environment for data sharing that is mainly divided into three modules:

1) **Web Module** is represented by the Decentralised Application (DApp), where the users, mainly individuals belonging to various stakeholders and organisations with different attributes, can register and interact with the system.
2) **Storage Module**, which utilises IPFS, provides users with a scalable and secure platform to upload their large data set and ensure data integrity.
3) **Network Module** is responsible for decentralisation, immutability, and governing secure access control.

On a Blockchain network, the DApp is software that offers decentralised and tamper-proof functionality. Users

can initiate transactions, access smart contracts, and securely manage assets through its interface, which functions as a 'bridge' for communication with the Blockchain. In the proposed system, the users can easily upload their data into the system storage module, which is the part that is responsible for the management of data. The IPFS protocol was adopted for distributed file storing and sharing, a system that uses a content-addressable system, allowing files to be located and recognised based on their content rather than their physical location. By utilising IPFS, the system can store and retrieve shared data effectively and robustly, minimising reliance and scalability. This proposed method generates a unique hash when stakeholders upload their data onto IPFS via the system. This hash is then kept on HLF, ensuring a secure and immutable record of the uploaded data. Thus, the solution adopts a hybrid storage strategy, with vital data on-chain for tampering protection and less critical data off-chain for cost efficiency and performance enhancements. The system's networking functions are handled by the Hyperledger Fabric, which is a restricted permissioned Blockchain used for data storage and sharing, allowing authorised participants to access sensitive information. The HLF platform offers the infrastructure and tools to build and maintain distributed ledger networks. In addition, it ensures secure communication and data transfer by smart contracts known as 'chaincode', consensus processes, and privacy controls. Within the HLF platform, organisations are encapsulated as network participants, each playing a vital role in the consensus and governance mechanisms. These organisations contribute to the integrity and transparency of the shared data ecosystem by engaging in transactions and endorsing smart contracts within the network. In the system, organisations represent the involved stakeholders, who serve as entities with a vested interest in the shared data. By integrating HLF into this system, access control policies are defined using Membership Service Providers (MSPs) and enforced by peers and ordering nodes. As a result, these features improve security and transparency, reducing tampering risk. In addition, leveraging HLF's features, such as immutability, consensus mechanisms, and smart contracts, improves the integrity. Furthermore, storing IPFS hashes on Hyperledger ensures that data remains unaltered.

The algorithm1 outlines the procedures for managing data access permissions within the system. The algorithm defines the data structures, access policies, and validation procedures necessary for ensuring secure data access.

Algorithm 1 Access Control

```
Data Structures: User: { id: string, org: string, attr: map⟨string, int⟩ }
DataItem: { id: string, owner: User, hash: string, metadata: map⟨string, string⟩, policies: list⟨Policy⟩ }
Policy: { AuthOrgs: list⟨string⟩, attrs: map⟨string, int⟩ }
Transaction: { cert: string, dataId: string }
Function AddPolicyToDataItem(dataItem, policy)
  dataItem.policies.append(policy)
Function ValidateAccess(tx, item): bool
  user = ParseCertificate(tx.cert) {Extract user information from certificate}
for policy in item.policies do
  if user.org in policy.AuthOrgs then
    authorized = true
    for attr in policy.attrs do
      if user.attrs[attr] not in policy.attrs then
        authorized = false
        break
      end if
    end for
    if authorized then
      return true
    end if
  end if
end for
return false {User not authorized}
```

B. The Proposed System Workflow

Based on the system structure shown in Figure 2, this section explains each component's role in detail.

1) The users in this system are:
   (a) The system administrator is responsible for issuing identity certificates and private keys for users, executing the chaincode on the HLF, and registering other users on the chaincode.
   (b) The system user (i.e. the stakeholder), who is the party that has the data resources to share, or needs the data resources.
2) Users initiate the process by accessing the system by their web browser. The user interface provides a seamless registration experience.
3) User Registration and Login:
   – Users register independently, and the admin monitors this step for validation.
   – Admin confirms user information for approval.
   3.1 Digital Wallet Creation:
   a) Following approval, the system automates the creation of a digital wallet associated with the user's account.
   b) The digital wallet serves as a secure container for cryptographic keys used in transactions and data access.
   3.2 Interaction with Certificate Authorities (CA):
   a) The system communicates with the Hyperledger Certificate Authority (CA) after being registered.
   b) By providing users with cryptographic certifi-

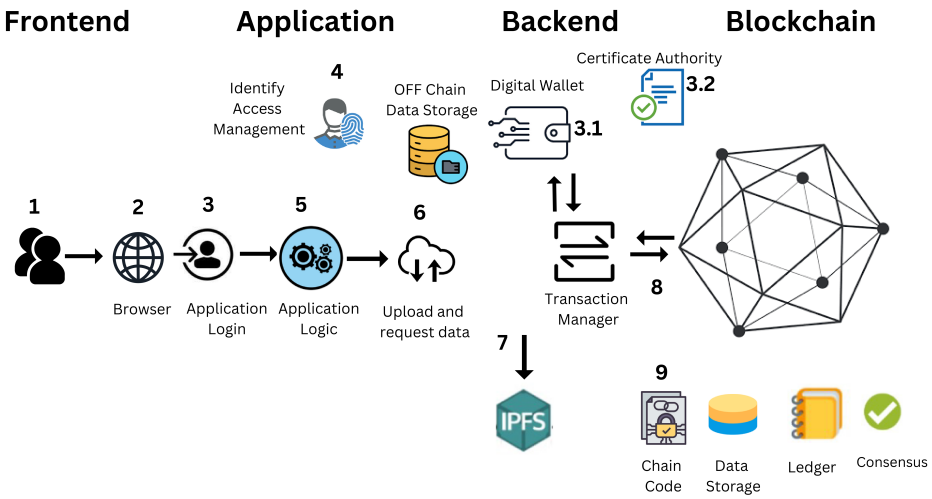

Fig. 2. **Workflow Overview**: The diagram encapsulates the entire lifecycle, from user access to secure data retrieval, emphasising the integration of Hyperledger and IPFS for a robust data-sharing experience.

cates, CA authenticates their identities on the Blockchain network. These certificates enhance the security and trustworthiness of user interactions within the network.

4) Then, user authentication is established with secure login credentials.
5) User interface interactions are handled and client-side processed within the DApp.
6) Data Upload with Policies:
   - Users who have authenticated their identity can become part of this channel, and they are granted access to the system features, including the ability to upload datasets seamlessly with the associated access policies. This process is facilitated through an intuitive frontend interface (see Figure 3-a).
   - Access policies include organisations permitted to access the data and attributes of users within those organisations.
   - Policies are kept on Hyperledger and cryptographically signed for integrity.
   - Users can edit the access policy for their uploaded data. They can access the "My Data List" section, view the previously assigned policy, and select a new access policy as required.
   - Users view a frontend board listing available datasets. (see Figure 3-b). They request access to a specific dataset by submitting a request.
   - The system checks the user's request for access against HLF's stored access policies. Access control logic ensures only authorised users can access the requested data (see Figure 3-c). For auditing purposes, HLF maintains an immutable record of access requests.
   - The system provides the user with the hash to ascertain data from IPFS if access is authorised.

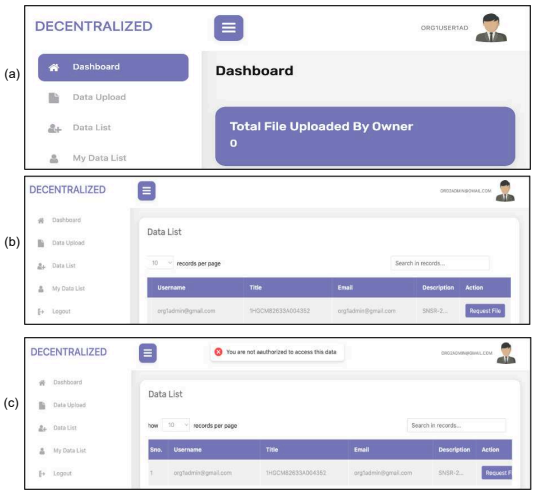

Fig. 3. **User Interface:** (a) The user dashboard to add and request data effortlessly. (b) View available data sets for request. (c) Highlight unauthorized data requests, emphasizing the need for access control.

7) On the IPFS network, the hash acts as a safe and distinct identifier for the submitted dataset.
8) For a tamper-proof record, the IPFS hash and access policies are stored on HLF.
9) Data integrity and storage policies are enforced via HLF chaincode.

VI. Implementation and Experiment Setup

Within the Hyperledger setup, the aim was to configure the Hyperledger channel with five organisations within

the same channel for streamlined governance and efficient consensus decision-making, as well as minimising the complexity of the network while maintaining a balance between decentralisation and manageability. Each organisation had distinct characteristics and users with specific roles. The manufacturer(Org1) represents the organisation with the highest amount of data, and the remaining four organisations represent different stakeholders or regulators interacting within the system. In particular, having different MSP service providers is essential to ensure that each organisation has control over its members and their identities. The independent management enhances the network's overall security and robustness, contributing to an additional layer of trust and integrity and reinforcing the reliability of the Blockchain infrastructure in this use case. Furthermore, the Raft consensus algorithm was selected to facilitate the agreement and replication of the distributed ledger across the nodes in the current network. Raft offers a reliable and resilient consensus method that guarantees all nodes agree to the Blockchain's current state; ensuring the integrity and consistency of the shared ledger is crucial. Additionally, the CouchDB database has been included in the configuration. CouchDB acts as Hyperledger's state database, keeping track of the Blockchain's current state and facilitating quick and easy data indexing and searching. Its decentralised and document-oriented design complements the Hyperledger tenets, offering the distributed ledger an adaptable and scalable storage option.

During the development of creating the environment, the services provided by Amazon Web Services (AWS) were utilised to facilitate the deployment and configuration process. The configuration consists of Ubuntu 18.04 LTS Operating System, Hyperledger Fabric (v 2.2.4), Docker (17.06.2-ce), Go Language (1.11.x), Node.js (8.x), NPM (5.x), Python (2.7.x).

Moreover, during the implementation phase, to ensure scalability and efficiency and facilitate the use of IPFS, Pinata [28] was integrated as a service that provides additional features and tools to simplify the process of managing content on the IPFS network. Within the framework of this project, four distinct chaincodes have been implemented to oversee, promote code separation, and improve overall maintainability. Each chaincode aims to address distinct functionalities: Register_User, Save_Hash, Get _IPFS_Hash, and Update_Policies. This design decision supports the best practices in distributed ledger architecture, fostering a modular and organised approach to smart contract development and management. Moreover, for evaluation, the dataset is the V2X-Sim Dataset [29].

VII. Evaluation and Discussion

In this assessment section, we evaluate the performance of both the front-end and back-end systems in terms of average response time (latency) relative to varying user loads.

A. Front-End

User satisfaction and adoption of Blockchain applications could be improved by evaluating the frontend's usability, user experience, responsiveness, and accessibility. The system, evaluated using JMeter [30] and k6 [31], highlights a connection between user demand and system performance. This connection is illustrated in the registration module by the effect of user concurrency on average response time, as depicted in the bar chart in Figure 4. The average response time can be noted as rising as the number of users increases from 1 to 1000. Furthermore, as shown in Figure 5, the tests reveal a significant difference in average response time between 1000 users uploading 3 GB and 3 KB, emphasizing the impact of uploaded data.

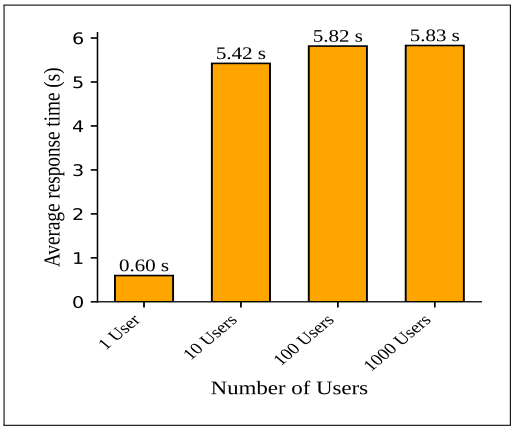

Fig. 4. **Response Time vs Users:** The average response time with user count, from 1 to 1000 for the *R*egister _*U*ser Module.

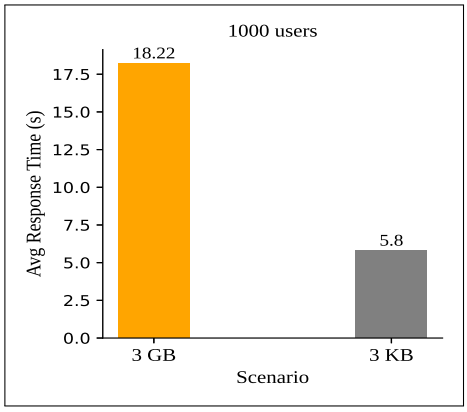

Fig. 5. **Impact of Data Upload Size on Average Response Time:** The figure demonstrates the variation in response time when uploading 3 GB and 3 KB for *S*ave _*H*ash module.

B. Blockchain Performance

For the chaincode testing, the performance has been tested by the Hyperledger Caliper tool [32]. It is a

Blockchain performance benchmarking tool that helps to provide valuable insights into the system's performance across various modules, with the metrics that are shown in table I, including success rate, fail rate, send rate, latency, and throughput, all measured in *Transactions Per Second* (TPS), offering a comprehensive view of the system's behaviour.

TABLE I
KEY PERFORMANCE METRICS AND EXPLANATIONS

Metric	**Explanation**
Success	Refers to the number of successful transactions completed during the test.
Fail	Refers to the number of failed transactions.
Send Rate (TPS)	Refers to the number of transactions sent per second.
Avg Latency (s)	Refers to the average time it took for a transaction to be completed in seconds.
Throughput (TPS)	Refers to the number of transactions completed per second.

The results suggest that the system's performance is impacted by the number of virtual users. For example, Figure 6 demonstrates a decrease in throughput with increased users in the Register _User chaincode. That could be attributed to potential scalability challenges within the system as more users join the network, causing an increase in transaction complexity. In this figure, the three lines link markers at user counts of 10, 100, and 200, each representing a distinct TPS number (50, 100, and 200). Even with varying TPS scenarios, this chart represents how throughput is impacted by different user loads.

The investigation extends to the performance analysis over the system's modules, with the tests showing that the system with some modules achieved high send rates and throughput. In contrast, others had higher latency and lower success rates. Based on the report, it is evident that different modules exhibit varying performance levels. The observed differences in throughput between chaincodes under the same conditions offer an intricate illustration of the system's operation in Figure 7. This discrepancy underscores the interplay between algorithms and computational efficiency, suggesting that system throughput might be contingent upon the fundamental structure and complexity of chaincodes. In the realm of evaluation, modules such as "Register_User" demonstrate high success rates and low latency, indicating efficient processing and execution. In comparison, modules such as "Get_ipfs_Hash" and "Save_Hash" may have slightly higher latency. For example, Figure 8 shows a comparison of the Average Latency for two chaincodes: "Register_User" and "Save_Hash" with the same test scenarios of 200 virtual users and 200 TPS. Proceeding to evaluate success and fail rates, while the chain code modules: "Get _IPFS _Hash" and "Update _Policies" have almost similar Send Rates and Maximum Latency, they present clear variations in success and fail rates. Figure 9 illustrates the relationship between the failure rate for the "Update_policies" chaincode and the number of users in a system under different TPS scenarios. In Figure 9, the failure rate also rises as the number of users increases. This can be observed through the bar graph where the x-axis represents the number of users, and the y-axis represents the failure rate percentage. Further, for more complex Hyperledger Fabric transactions, there is an observed increase in latency, causing a potential impact on throughput [33].

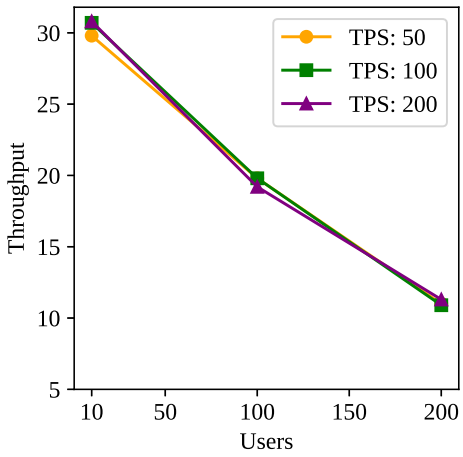

Fig. 6. Throughput (transaction per second) vs Concurrent Users for Different TPS scenarios for *R*egister _*U*ser Module.

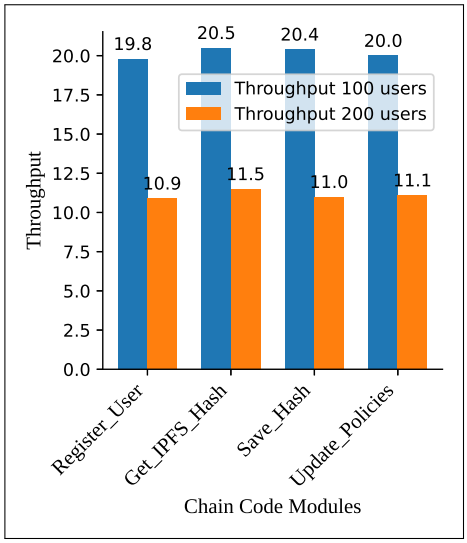

Fig. 7. **Throughput Variations in Chaincodes in Uniform Scenarios.** The figure embodies the distinct throughput outcomes observed across various chaincodes within identical operational scenarios: 100 users and 200 users.

From these figures, it can be observed that the TPS represents another factor that impacts the Failure Rate. For example, Figure 9 shows that the failure is higher with

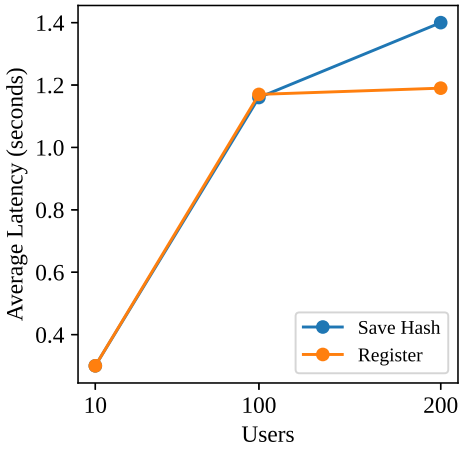

Fig. 8. **Average latency for different modules as the number of users increases**: The figure shows a comparison between the average latency for "Save _Hash" and "Register _User" operations, revealing trends across user counts.

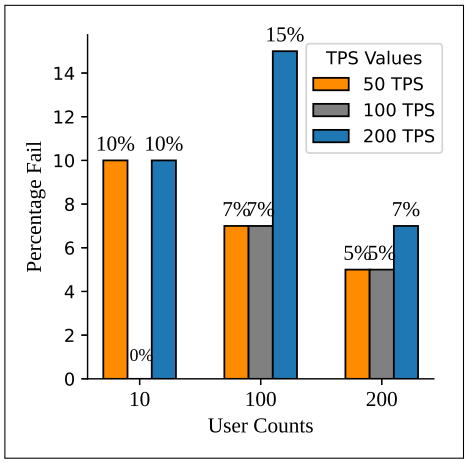

Fig. 9. Percentage Failure in the *Update_policies* chaincode under Different TPS Values and User Counts.

100 users than 200 users if the TPS configuration is 200 during the test, indicating that the system is under greater pressure and more challenges at higher transaction rates. Therefore, the findings imply that the quantity of virtual users affects the system's performance. The studies also revealed that while some system modules had higher send rates and throughput and lower failure rates, others had higher delays.

C. System Usability

In 1996, John Brooke introduced the System Usability Scale (SUS) as a straightforward and economical single-dimensional measure of usability [34], [35]. SUS scores range from 0 to 100, with higher scores indicating better usability. Upon conducting this scale on this system, the obtained score is 66.9, based on the current data available, which falls just above the 60 benchmark for acceptable usability. Hence, this score reflects the usability of the system based on user feedback collected until the present moment.

VIII. Conclusion and Future Work

This paper presents an initial feasibility study on a collaborative data-sharing platform for the Autonomous Vehicle (AV) ecosystem. This platform utilizes Hyperledger Fabric for attribute-based access control and IPFS for scalable data storage, ensuring secure and efficient data sharing among all stakeholders. This approach effectively addresses the challenge of data sharing in AVs, thereby improving the efficiency of intelligent transportation systems that rely on wireless communication. Future work will focus on evaluating and enhancing the system's scalability for managing larger volumes of AV data. This could involve incorporating efficient data compression encryption and exploring other innovative techniques.

IX. Acknowledgment

This work is supported, in part, by EPSRC & DSIT funded projects (EP/X040518/1), (EP/Y037421/1), (EP/X525856/1), and (EP/Y019229/1) and Shaqra University and the Saudi Arabia Cultural Bureau.

References

[1] R. Alhabib and P. Yadav, "Data authorisation and validation in autonomous vehicles: A critical review," 2024. [Online]. Available: https://arxiv.org/abs/2405.17435

[2] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," *Cluster Computing*, vol. 24, no. 4, pp. 2841–2866, 2021.

[3] R. Song, B. Xiao, Y. Song, S. Guo, and Y. Yang, "A survey of blockchain-based schemes for data sharing and exchange," *IEEE Transactions on Big Data*, 2023.

[4] H. Fabric, "A blockchain platform for the enterprise: Hyperledger fabric," 2019.

[5] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[6] J. Gwehenberger, O. Braxmeier, C. Lauterwasser, M. A. Kreutner, M. Borrack, C. Reinkemeyer, L. Wech, M. Weyde, and P. Salzberger, "Needs and requirements of edr for automated vehicles-analysis based on insurance claims reported to allianz germany."

[7] M. A. Hoque and R. Hasan, "Avguard: A forensic investigation framework for autonomous vehicles," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[8] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," *arXiv preprint arXiv:1802.05050*, 2018.

[9] K. K. G. Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to automotive forensics," *Forensic Science International: Digital Investigation*, vol. 36, p. 301111, 2021.

[10] S. Lee, W. Choi, H. J. Jo, and D. H. Lee, "T-box: A forensics-enabled trusted automotive data recording method," *IEEE Access*, vol. 7, pp. 49 738–49 755, 2019.

[11] W. Liu, W. Shen, L. Harn, and M. Luo, "A fast vanet-assisted scheme for event data recorders," *Security and Communication Networks*, vol. 2022, 2022.

[12] J. T. Correia, K. A. Iliadis, E. S. McCarron, M. A. Smolej, B. Hastings, and C. C. Engineers, "Utilizing data from automotive event data recorders," in *Proceedings of the Canadian Multidisciplinary Road Safety Conference XII, London Ontario*, 2001, p. 18.

[13] Y. Fang, H. Min, X. Wu, X. Lei, S. Chen, R. Teixeira, and X. Zhao, "Toward interpretability in fault diagnosis for autonomous vehicles: Interpretation of sensor data anomalies," *IEEE Sensors Journal*, vol. 23, no. 5, pp. 5014–5027, 2023.

[14] T. Alshalali, K. M'Bale, and D. Josyula, "Security and privacy of electronic health records sharing using hyperledger fabric," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2018, pp. 760–763.

[15] A. Alniamy and B. D. Taylor, "Attribute-based access control of data sharing based on hyperledger blockchain," in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, 2020, pp. 135–139.

[16] S. Liu and Y. Shang, "Secure resource sharing on hyperledger fabric based on cp-abe," in *2021 The 3rd International Conference on Blockchain Technology*, 2021, pp. 203–209.

[17] A. Reem and Y. Poonam, in *NDSS VehicleSec 2024*. Usenix, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-9-poster.pdf

[18] E. Thorn, S. C. Kimmel, M. Chaka, B. A. Hamilton *et al.*, "A framework for automated driving system testable cases and scenarios," United States. Department of Transportation. National Highway Traffic Safety ..., Tech. Rep., 2018.

[19] S. International, "Sae levels of driving automation™ refined for clarity and international audience," 2021, available from SAE International. [Online]. Available: https://www.sae.org/standards/content/j3016_202104/

[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[21] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[22] T. Abera, R. Bahmani, F. Brasser, A. Ibrahim, A.-R. Sadeghi, and M. Schunter, "Diat: Data integrity attestation for resilient collaboration of autonomous systems." in *NDSS*, 2019.

[23] V. Baraku, I. Paraskakis, S. Veloudis, and P. Yadav, "Responsible information sharing in the era of big data analytics facilitating digital economy through the use of blockchain technology and observing gdpr," in *Proceedings of the 14th International Conference on Cloud Computing and Services Science - CLOSER*, INSTICC. SciTePress, 2024, pp. 257–264.

[24] Q. Zeng, M. Zhao, P. Liu, P. Yadav, S. Calo, and J. Lobo, "Enforcement of autonomous authorizations in collaborative distributed query evaluation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 4, pp. 979–992, 2015.

[25] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 44–51.

[26] A. Budel, R. Alhabib, M. Nicholson, and P. Yadav, "Vincy: A smart-contract based data integrity and validation tooling for automated vehicle incident investigation," 2023. [Online]. Available: https://arxiv.org/abs/2311.13728

[27] X. Zhao, S. Wang, Y. Zhang, and Y. Wang, "Attribute-based access control scheme for data sharing on hyperledger fabric," *Journal of Information Security and Applications*, vol. 67, p. 103182, 2022.

[28] Pinata, "Ipfs api amp; ipfsnbsp;gateway," 2018, accessed on June 10, 2023. [Online]. Available: https://www.pinata.cloud/

[29] Y. Li, D. Ma, Z. An, Z. Wang, Y. Zhong, S. Chen, and C. Feng, "V2x-sim: Multi-agent collaborative perception dataset and benchmark for autonomous driving," *IEEE Robotics and Automation Letters*, 2022.

[30] E. H. Halili, *Apache JMeter*, 2008.

[31] "Load testing for engineering teams grafana k6." [Online]. Available: https://k6.io/

[32] "Caliper: An open-source performance testing tool for evaluating system scalability," 2023. [Online]. Available: https://github.com/hyperledger/caliper/

[33] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability," in *2019 IEEE international conference on blockchain (Blockchain)*. IEEE, 2019, pp. 536–540.

[34] J. Brooke, "Sus: a quick and dirty usability," *Usability evaluation in industry*, vol. 189, no. 3, pp. 189–194, 1996.

[35] J. A. Brooke, "Sus: A retrospective," *Journal of Usability Studies*, vol. 8, no. 2, pp. 29–40, 2013.