DATA SHARING IN AUTONOMOUS VEHICLES

Hyperledger Fabric Platform for Secure and Efficient Data Sharing

Reem Alhabib
reem.alhabib@york.ac.uk

Poonam Yadav
poonam.yadav@york.ac.uk

1. Problem Statement

Autonomous vehicles (AV) systems make driving decisions using data from sensors and cameras, crucial for later processes such as validation, improvement, training, and addressing accident legal liability. Thus, this data is crucial for various stakeholders such as government, owners, and insuance providers [1]. Accordingly, in this work, a Hyperledger based solution has been implemented enabling Attribute-BasedAccess Control (ABAC) for efficient data-sharing

2. Motivation

Autonomous vehicles generate crucial data with diverse applications from accident investigation to informing regulations and advancing technology. However, the current research on autonomous vehicle data faces two main gaps. Firstly, limitations in the existing records, specifically Event Data Recorder (EDR) and Data Storage Systems for Automated Driving (DSSAD) in autonomous vehicles, make them ineffective even for accident-related use cases. Secondly, there is a lack of efficient solutions addressing the fine-grained access control platform needed to responsibly share this valuable data with authorized stakeholders across various domains. This research aims to investigate the efficiency of implementing existing data-sharing solutions to address this gap

The Need for Data Sharing Among Various Stakeholders

3. Objectives

- Build a fine-grained access control platform utilizing Hyperledger blockchain technology. This platform will enable the granting or denies requests to use the assets (data resources) based on Attribute Based Access Control (ABAC) for restricting access to the specific users having the necessary attributes in their certificate.
- Conduct comprehensive performance assessments, including scalability, by the scale of concurrency of the user interactions and data size.

4. Proposed Solution

As illustrated in Figure 2 and 3, the system is mainly divided into three modules:

1. **Decentralised Application (DApp):** With a user-intuitive interface and robust API, the system prioritizes user-friendliness and straightforward maintenance. Furthermore, users can initiate transactions, access smart contracts, and securely manage assets through its interface, which functions as a bridge for communication with the blockchain.
2. **Network Module:** The Hyperledger Fabric platform offers the infrastructure and tools needed to build and maintain a distributed ledger. This restricted permissioned blockchain is utilized for data storage and sharing, allowing authorized participants to access sensitive information. In addition, to improve security and transparency, access control policies are defined and enforced, allowing for controlled and authorized access to data.
3. **The storage module:** The InterPlanetary File System (IPFS) is utilized as the foundation for scalable data storageenabling robust and secure data retrieval. For integrity and immutable records the generated unique hash is stored on Hyperledger once the stakeholders upload their data set on the system

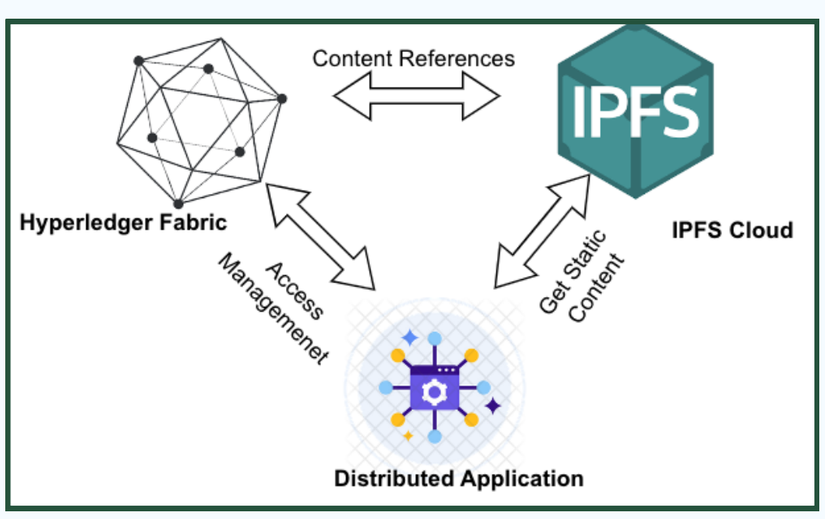

Figure 2: The three core components of the system: Web Module, Network Module, and Storage Module.

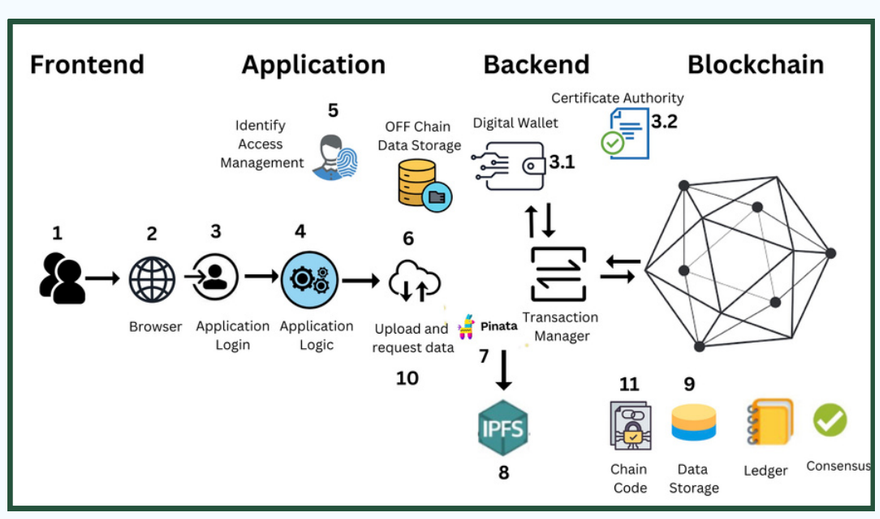

Figure 3: The proposed system structure and the entire workflow.

5. Evaluation

In the blockchain evaluation, we utilize the **Hyperledger Caliper** [2] benchmarking tool to evaluate the system's four chaincode: ***Register_User,Get_IPFS_Hash,Save_Hash, and Update_Policies.***

The results indicate that the system's performance is impacted by the number of virtual users. For example, the send rate increases consecutively with user counts ranging from 10 to 200.

In addition, for all modules, a decrease in throughput was observed with an increase in the number of users. That could be imputed to probable scalability challenges within the system, as more users join the network, causing an increase in the transaction complexity. Figures 4 and 5 illustrate the main findings.

This integrated approach of multi-party data sharing fosters collaboration, security, privacy, and safety improvements in AV. In the next phase of evaluation, the focus is on testing the scalability of our system in terms of processing large volumes of AV data.

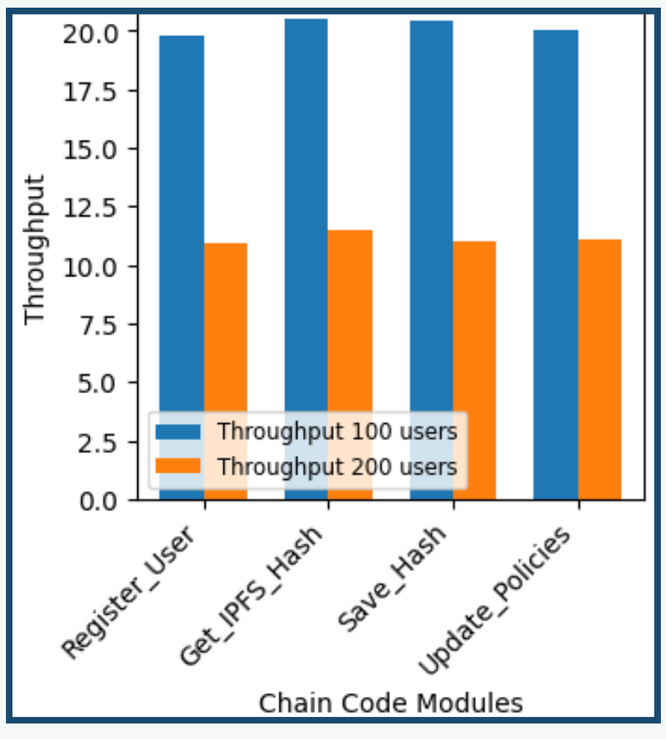

Figure 4: The throughput varies in the chain codes among the same test scenario. As observed in the figure the throughput varies across various modules within operational scenarios: 100 users and 200 users.

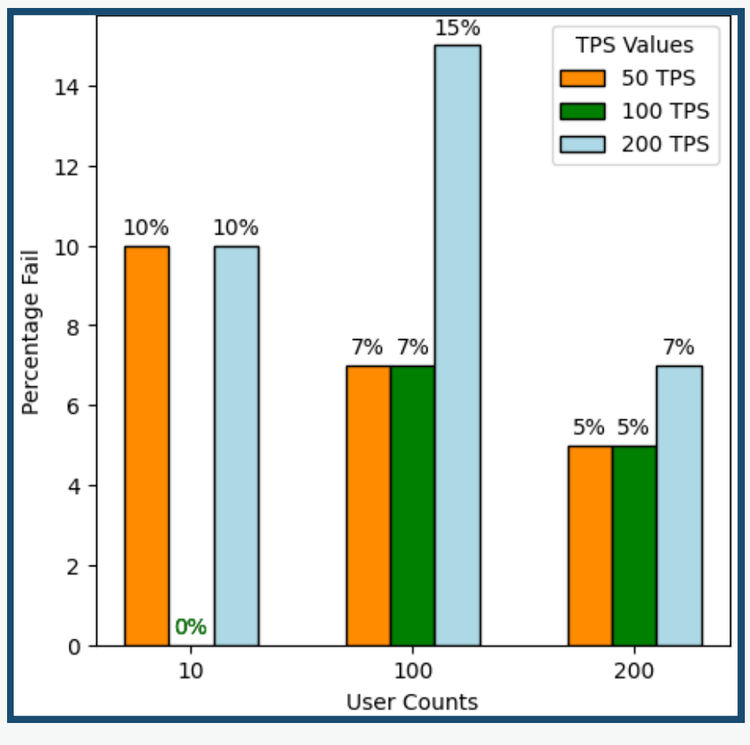

Figure5: The relationship between the failure rate for the "Update_policies" chain code, and the number of users in a system under different transactions per seconds (TPS) scenarios. In the figure, as the number of users increases, the failure rate also rises. Complex chaincode in Hyperledger Fabric may affect throughput, affect transaction processing speed, and overall efficiency.

6. Acknowledgment

This work is supported, in part, by EPSRC \& DSIT TMF-uplift: CHEDDAR: Communications Hub For Empowering Distributed ClouD Computing Applications And Research (EP/X040518/1), (EP/Y037421/1), EPSRC IAA (EP/X525856/1), and EPSRC REMOTE (EP/Y019229/1) and Shaqra University and the Saudi Arabia Cultural Bureau.

REFERENCES

[1] 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.
[2] "Caliper: An open-source performance testing tool for evaluating system scalability," 2023. [Online]. Available: https://github.com/hyperledger/caliper