Journal of Information Security and Applications 67 (2022) 103179

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G

Riya Kakkar [a], Rajesh Gupta [a], Smita Agrawal [a,*], Sudeep Tanwar [a,*], Ravi Sharma [b]

[a] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
[b] Centre for Inter-Disciplinary Research and Innovation, University of Petroleum and Energy Studies, P.O. Bidholi Via-Prem Nagar, Dehradun, India

ARTICLE INFO

Keywords:
Blockchain
Random forest
Latency
Scalability
Edge intelligence
5G

ABSTRACT

This paper proposes a blockchain-based secure and reliable data sharing scheme for autonomous vehicles (AVs). It aims to secure data sharing among AVs. We integrate the fifth-generation (5G) communication network with the proposed blockchain-based scheme to enable ultra-low latency, high reliability, and availability. We have incorporated the edge intelligence nodes (EINs) with blockchain for efficient data processing. We have used a random forest classifier model (RFCM) on the road accidents dataset to predict the accident severity, i.e., fatal, serious, and slight. It is based on road type, light condition, and vehicle movement to be shared among other AVs. We have considered various scenarios and performed the predictive analysis that needs to be secured by using blockchain technology. Results of the study demonstrate the accuracy of RFCM as 93%, the precision of 98%, 97%, and 87% for fatal, serious, and slight categories of accident severity, respectively. The results show that the proposed scheme with RFCM yields better accuracy of 93% than other existing classification algorithms such as Decision tree, Naive Bayes, and AdaBoost. The blockchain-based proposed system has been compared with the traditional approach based on parameters such as network latency, scalability, computation time, delay comparison for node validation, data storage latency, and data storage cost. Obtained results show that the proposed scheme enables the data sharing reliable, secure, and efficient for AVs and outperforms the blockchain and non-blockchain systems in terms of security and efficiency.

1. Introduction

In recent years, the automobile industry is gradually evolved from traditional transportation systems to intelligent transportation systems (ITS) [1]. The amalgamation of ITS and automated technology is the main reason for the emergence of autonomous vehicles (AVs). This draws the attention of manufacturers and industrialists towards self-driving cars [2]. AVs are embedded with various intelligent vehicle technologies like driver assistance systems, sensors, radars, GPS, etc. These provide vehicles with dynamic and adaptive environments without any interference from humans. As per the report [3], 60% of the transportation system will be dependent on AVs by 2045. With the exponential increase in the adoption of AVs, a huge amount of data has been generated by the sensors about the road, traffic, street light, and weather conditions. It needs to be managed and processed efficiently in real-time scenarios [4]; otherwise, it can lead to severe accidents. So, AVs need to share accident and traffic information so that they can make the decision accordingly to prevent further road accidents [5]. AVs help to prevent traffic fatalities caused due to driver's mistake(s) and also reduce greenhouse gas emission [6].

AVs also prove to be beneficial for handicapped or visually challenged people who cannot drive vehicles [7]. Motivated by the aforementioned benefits, many researchers across the globe have given various data sharing schemes among AVs. But, they have presented their scheme at the core-cloud servers, i.e., in a centralized architecture. It can cause severe privacy and security issues such as data manipulation, data spoofing, single point of failure, and many more [7]. These issues can mislead AVs from their path leading to severe accidents.

It is essential to introduce a secure and transparent system to improve the security and confidentiality of data sharing among AVs to lessen the number of road mishappenings [8]. Fig. 1 shows the analysis of accident deaths in Tesla in the different countries, which has been increased over the years [9]. To minimize the road fatalities and security issues in AVs, a decentralized and verifiable blockchain-based model is required [10]. Some of the research works in the same field are as follows: Chen et al. in [11] proposed a peer-to-peer (P2P) decentralized model, i.e., Byzantine fault-tolerant (BFT) federated learning model to offer security to the AVs for data sharing. Finally, the results

* Corresponding authors.
E-mail addresses: 21ftphde56@nirmauni.ac.in (R. Kakkar), 18ftvphde31@nirmauni.ac.in (R. Gupta), smita.agrawal@nirmauni.ac.in (S. Agrawal), sudeep.tanwar@nirmauni.ac.in (S. Tanwar), ravisharmacidri@gmail.com (R. Sharma).

https://doi.org/10.1016/j.jisa.2022.103179

Available online 22 April 2022