scientific reports

Check for updates

OPEN

A secure and efficient blockchain enabled federated Q-learning model for vehicular Ad-hoc networks

Huda A. Ahmed[1], Hend Muslim Jasim[2], Ali Noori Gatea[3], Ali Amjed Ali Al-Asadi[4] & Hamid Ali Abed Al-Asadi[2]✉

Vehicular Ad-hoc Networks (VANETs) are growing into more desirable targets for malicious individuals due to the quick rise in the number of automated vehicles around the roadside. Secure data transfer is necessary for VANETs to preserve the integrity of the entire network. Federated learning (FL) is often suggested as a safe technique for exchanging data among VANETs, however, its capacity to protect private information is constrained. This research proposes an extra level of security to Federated Q-learning by merging Blockchain technology with VANETs. Initially, traffic data is encrypted utilizing the Extended Elliptic Curve Cryptography (EX-ECC) technique to enhance the security of data. Then, the Federated Q-learning model trains the data and ensures higher privacy protection. Moreover, interplanetary file system (IPFS) technology allows Blockchain storage to improve the security of VANETs information. Additionally, the validation process of the proposed Blockchain framework is performed by utilizing a Delegated Practical Byzantine Fault Tolerance (DPBFT) based consensus algorithm. The proposed approach to federated Q-learning offered by Blockchain technology has the potential to develop VANET safety and performance. Comprehensive simulation tests are performed with several assessment criteria considered for number of vehicles 100, Throughput (102465.8 KB/s), Communication overhead (360.57 Mb), Average Latency (864.425 ms), Communication Time (19.51 s), Encryption time (0.98 ms), Decryption time (1.97 ms), Consensus delay (50 ms) and Validation delay (1.68 ms), respectively. As a result, the proposed approach performs significantly better than the existing approaches.

Keywords Vehicular Ad-hoc networks (VANETs), Blockchain system, Federated Q-learning, Extended elliptic curve cryptography (EX-ECC), Interplanetary file system (IPFS), Delegated practical byzantine fault tolerance (DPBFT).

Vehicle ad hoc networks (VANETs) are a kind of mobile ad hoc network that facilitates communication between automobiles and roadside equipment[1]. Drivers can benefit from the speed and safety that VANETs offer through their convenience and security applications[2]. An ambulance, for instance, may use communication with all other vehicles in the immediate area to establish the fastest path during an emergency, which would speed up the arrival time[3]. Additionally, in a weather-related situation, automobiles might provide real-time information regarding road conditions, assisting drivers in making decisions and possibly lowering the chance of collisions[4]. Applications involving collision avoidance, vehicle-to-vehicle communication, and traffic data in real-time are examples of such applications[5]. Big Data advancements have made it possible for VANETs to collect enormous volumes of unique traffic data, process it with Machine learning (ML)/Deep Learning techniques (DL), and deliver precise, low-latency operations[6]. However, VANETs require improved network safety and increased communication effectiveness[7].

A massive system consisting of many nodes associated with a network including smart vehicles either driven by individuals or their own, infrastructure that has been integrated with V2X communication, mobile computing, and cloud-based computing systems. In an attempt to deliver complex intelligent usage, it depends

[1]College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq. [2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq. [3]Advanced Electronics and Communication Technology, Istanbul Okan Üniversitesi, Istanbul, Türkiye. [4]Computer Science Department, American University of Science and Technology, Beirut, Lebanon. ✉email: hamid.abed@uobasrah.edu.iq