Federated Learning and Blockchain Applications in Vehicular Networks

Subjects: Computer Science, Artificial Intelligence

Contributor: Thippa Reddy Gadekallu , Abdul Javed , Muhammad Abul Hassan , Faisal Shahzad , Waqas Ahmed , Saurabh Singh , Thar Baker

The Internet of Things (IoT) revitalizes the world with tremendous capabilities and potential to be utilized in vehicular networks. The Smart Transport Infrastructure (STI) era depends mainly on the IoT. Advanced machine learning (ML) techniques are being used to strengthen the STI smartness further. However, some decisions are very challenging due to the vast number of STI components and big data generated from STIs. Computation cost, communication overheads, and privacy issues are significant concerns for wide-scale ML adoption within STI. These issues can be addressed using Federated Learning (FL) and blockchain. FL can be used to address the issues of privacy preservation and handling big data generated in STI management and control. Blockchain is a distributed ledger that can store data while providing trust and integrity assurance. Blockchain can be a solution to data integrity and can add more security to the STI. While transmitting data, valuable information can be disclosed through the model parameters by reverse engineering. The disclosure of valuable data motivated researchers and developers to adopt known security and privacy defense methods, e.g., functional encryption and differential privacy, to FL.

blockchain federated learning intelligence transportation system vehicular internet of things

1. Federated Learning and Blockchain for Security in Vehicular Networks

The fundamentals of information security CIA must be adhered to by the FL developers and adopters. Many end devices are included in the exposure and training of model characteristics through a decentralized approach, making FL vulnerable to several open risks and attacks. Current research regarding vulnerabilities and frameworks for mitigating risks in the FL technology is limited.

By using BC technology, several researchers and developers made efforts to improve the security of the VANET in recent times. Reference [1] proposed a novel secure spectrum sharing technique for VANET cellular networks based on blockchain; the proposed technique is for VANET and network operators where a new Stackelberg framework is presented for the optimal spectrum approaches. Reference [2] presented BC-as-a-service (BaaS) for IoT devices cohesive with MEC. VANET is used as a base station in the proposed framework, and BC is used for computation-intensive task offloading. For IoT networks based on MEC, [3] proposed a framework for secure data collection. In the proposed framework for authentication, end devices transfer private data to MEC servers. A BC-based decentralized framework is proposed by [4] for the ground to air data sharing in IoT networks. A Cournot

framework is designed to achieve maximum advantages from the ground to air sensors. For efficient and secure key distribution and recovery in VANET, [5] proposed an essential distribution technique based on the decentralized group by exploiting mutual healing and private BC protocol. For the security of VANET, several frameworks are proposed by different researchers based on the BC technique; some of the proposed frameworks are based on the BC network implementation under the FL framework for the applications of MCS. Reference [6] proposed a novel technique of privacy-preserving and secure FL for VANET. The author also presented a decentralized FL framework based on the BC techniques focused on user privacy to protect data contribution verification and data training between VANET. **Table 1** provides solutions to FL limitations.

Table 1. Blockchain-enabled federated learning.

Limitation of FL	Solution Provided by Blockchain-Enabled FL
FL is not suitable for the aggregating updates while selecting vehicles and maintain GM.	Blockchain provides a solution to all these problems through its decentralized storage and further maintaining the FL model. Blockchain can be used to store GM.
High speed is required for the server to gather information and update vehicles (clients).	
Express bandwidth is required.	
Skewing in GM can also be expected because of biasness.	
FL cannot detect the internal attacks by malicious node while updates are gathered from every vehicle in a network causing GM unable to link up.	

2. Federated Learning and Blockchain for Privacy Preservation in Vehicular Networks

Shortcomings of VANET are privacy, availability, integrity, identification, and confidentiality prevention from incoming attack [7][8]. Authentication of each vehicle in a network is a key security feature that must be ensured while spreading data within or across the network. Previously, the identification system was based on Public Key Infrastructure (PKI), where each vehicle in a system exchanges its private encrypted identification message to the Local Authentication Center (LAC), which takes enough time to identify a single vehicle. Periodic encryption and decryption create overhead problems in a network, which in return affect the efficiency and reliability of a network [9].

Privacy assurance is becoming the primary concern as technology is intervening in our daily life [10]. Due to the limitation of mobility and resources of vehicles in VANET, there are two main problems with deploying special data privacy system [11][12]. To ensure vehicles' data privacy and reduce latency, FL enables several entities with fewer resources, e.g., RDUs and vehicles, to combine and train a general model using local data of devices. During the

data transformation process, to preserve data privacy, the raw data of the network is distorted by plotting this in different models with less sensitive information [13]. Leveraging FL, the integration of two different components can mitigate data privacy problems in VANET [14], as can be seen in **Figure 1**.

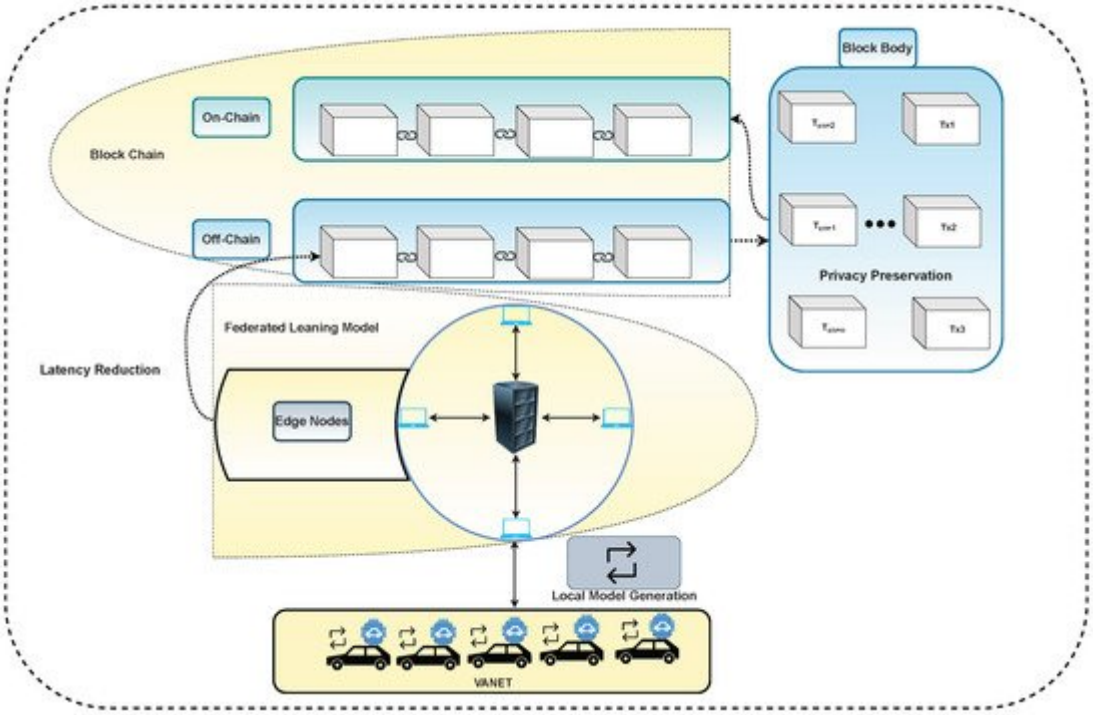

Figure 1. Integration of FL and blockchain in the VANET environment.

To address the privacy issues in VANET, various researchers tried to solve the issues from various research angles. Existing privacy frameworks: the differential privacy framework [15], its extensions [16], and the classic privacy framework are not sufficient to solve the privacy issues in VANET. To date, researchers did not find an optimal global solution for data privacy, and utility protection [17]. Ref. [18] proposed a encryption-based technique to solve the privacy issues. The proposed technique is helpful to a satisfactory level, but the proposed technique does not help in big data situations. FL can accomplish effective communication by transferring updated data between global models and local models [19][20]. FL solves the privacy issues to the maximum level, but another issue can arise: if the central model is poisoned or compromised, the adversaries may launch successful attacks. To solve the trust issues in FL, blockchain technology is introduced in such situations [21]. By forcefully incorporating privacy solutions through blockchain, it will decrease the efficiency of the application. FL overcame several data privacy issues by dividing the data into two parts: global aggregation and local training in the learning phase, but several other security issues arose. **Table 2** presents the literature review of security, privacy, and energy efficiency in the VANET environment.

Table 2. Literature review of security, privacy, and energy efficiency.

Ref.	Contribution	Environment	Focused Area
[22]	In this research work, the author proposed a privacy reserving communication scheme based on VANET. The proposed framework meets the contextual and content privacy requirements. It used identity-based encryption and an elliptic curve cryptography scheme.	ITS	Security and Privacy
[23]	In this research work, the author proposed a contest-aware quantification technique to overcome security issues in VANET based on the Markov chain method.	VANET	Security
[24]	Based on wireless communication, the author presents a literature review of existing work related to VANET technology. The author also presents research directions and open issues for the integration of SDN with VANET.	SDN, IoT	Security
[25]	The proposed work addressed different privacy and security issues regarding VANET. The paper also presents the solutions to privacy and security issues.	VANET	Security and Privacy
[26]	The proposed work presented an overview of secure and smart communications using the IoT-based VANET technique to overcome traffic congestions in CPS, known as networks of IoV.	CPS, IoV	Security
[27]	The author made different clusters of vehicle packets of the specific cellular tower in an IoT environment. This process simplified communication, and VANET architecture reduces energy consumption and network delays.	IoT	Energy efficiency
[28]	The author proposed a lightweight end-to-end security solution for SDNV. The proposed objectives are achieved on two-level: RSU-based authentication technique and personal IDS. The lightweight security solution will also provide privacy.	SDNV	Energy
[29]	The author proposed a source location privacy preservation method based on smart energy for sustainable city roads. The proposed technique hides source location based on acceleration, distance, speed, and trust.	IoT	Energy and Privacy
[30]	The author proposed a new algorithm for multi-hop transmission called fuzzy clustering routing. The author also analyzed clustering limitations, which are performed through different algorithms. To transfer data, multi-hop routing was used.	IoT	Energy
[31]	This paper presented the different notions of blockchain and its usability in IoT networks. The author presented different privacy issues regarding the implementation of blockchain in IoT. The author presented FL usability in IoT networks, privacy risks, and taxonomy.	IoT	Privacy
[32]	Among different elements elaborate to manage a group of vehicles containing data, the author proposed a blockchain framework. The author	VANET	Privacy

Ref.	Contribution	Environment	Focused Area
	integrates VPKI for blockchain to provide privacy and membership association.		
[33]	The author presented the fundamentals of IoT and blockchain. Then, the author presented a comprehensive literature review based on blockchain techniques for VIoT through the technical issues and problems. At the end of the paper, the authors present the future research direction regarding VIoT and blockchain.	VIoT	Energy and Privacy
[34]	The proposed research work analyzed and described existing supply chain, healthcare, VANET, and IoT access control through blockchain security methods. The author also presents a comprehensive survey regarding blockchain security.	IoT	Security and Privacy
[35]	The author proposed a new technique called FL-Block (blockchain FL) to overcome the existing issues in FL privacy. The local learning update is transferred to global learning using blockchain through this technique.	Fog computing	Privacy

3. Islam, A.; Shin, S.Y. BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things. J. Commun. Netw. 2019, 21, 491–502.
4. Zhu, Y.; Zheng, G.; Wong, K.K. Blockchain-empowered decentralized storage in air-to-ground industrial networks. IEEE Trans. Ind. Inform. 2019, 15, 3593–3601.
5. Li, X.; Wang, Y.; Vijayakumar, P.; He, D.; Kumar, N.; Ma, J. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad hoc network. IEEE Trans. Veh. Technol. 2019, 68, 11309–11322.
6. Wang, Y.; Su, Z.; Zhang, N.; Benslimane, A. Learning in the Air: Secure Federated Learning for UAV-Assisted Crowdsensing. IEEE Trans. Netw. Sci. Eng. 2021, 8, 1055–1069.
7. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. Veh. Commun. 2014, 1, 53–66.
8. Isaac, J.T.; Zeadally, S.; Camara, J.S. Security attacks and solutions for vehicular ad hoc networks. IET Commun. 2010, 4, 894–903.
9. Akhter, A.; Ahmed, M.; Shah, A.; Anwar, A.; Zengin, A. A secured privacy-preserving multi-level blockchain framework for cluster based VANET. Sustainability 2021, 13, 400.
10. Ahmed, W.; Shahzad, F.; Javed, A.R.; Iqbal, F.; Ali, L. WhatsApp Network Forensics: Discovering the IP Addresses of Suspects. In Proceedings of the 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 19–21 April 2021; pp. 1–7.
11. Lu, Y.; Huang, X.; Li, D.; Zhang, Y. Collaborative graph-based mechanism for distributed big data leakage prevention. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–7.

12. Pan, X.; Cai, X.; Song, K.; Baker, T.; Gadekallu, T.R.; Yuan, X. Location Recommendation Based on Mobility Graph With Individual and Group Influences. IEEE Trans. Intell. Transp. Syst. 2022, 1–12.
13. Ahmed, W.; Rasool, A.; Nebhen, J.; Kumar, N.; Shahzad, F.; Rehman Javed, A.; Gadekallu, T.R.; Jalil, Z. Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. arXiv 2021, arXiv:2105.12097.
14. Lu, Y.; Huang, X.; Dai, Y.; Maharjan, S.; Zhang, Y. Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems. IEEE Netw. 2020, 34, 50–56.
15. Li, X.; Zhang, H.; Ren, Y.; Ma, S.; Luo, B.; Weng, J.; Ma, J.; Huang, X. PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs. IEEE Internet Things J. 2020, 7, 11789–11802.
16. Lyu, L.; Nandakumar, K.; Rubinstein, B.; Jin, J.; Bedo, J.; Palaniswami, M. PPFA: Privacy preserving fog-enabled aggregation in smart grid. IEEE Trans. Ind. Inform. 2018, 14, 3733–3744.
17. Qu, Y.; Yu, S.; Zhou, W.; Peng, S.; Wang, G.; Xiao, K. Privacy of things: Emerging challenges and opportunities in wireless internet of things. IEEE Wirel. Commun. 2018, 25, 91–97.
18. Lin, X.; Lu, R. ECPP: Efficient Conditional Privacy Preservation Protocol; Wiley-IEEE Press: Hoboken, NJ, USA, 2015.
19. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. Knowl.-Based Syst. 2021, 216, 106775.
20. Bennis, M. Federated Learning and Control at the Wireless Network Edge. GetMobile Mob. Comput. Commun. 2021, 24, 9–13.
21. Ren, P.; Yan, T. Latency Analysis of Consortium Blockchained Federated Learning. arXiv 2021, arXiv:2105.04087.
22. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Yassin, A.A. Vppcs: Vanet-based privacy-preserving communication scheme. IEEE Access 2020, 8, 150914–150928.
23. Wang, J.; Chen, H.; Sun, Z. Context-Aware Quantification for VANET Security: A Markov Chain-Based Scheme. IEEE Access 2020, 8, 173618–173626.
24. Al-Heety, O.S.; Zakaria, Z.; Ismail, M.; Shakir, M.M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. IEEE Access 2020, 8, 91028–91047.
25. Kohli, P.; Painuly, S.; Matta, P.; Sharma, S. Future trends of security and privacy in next generation VANET. In Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 3–5 December 2020; pp. 1372–1375.

26. Kumar, S.; Singh, J. Internet of Vehicles over Vanets: Smart and Secure Communication using IoT. Scalable Comput. Pract. Exp. 2020, 21, 425–440.
27. Channakeshava, R.; Sundaram, M. A Study on Energy-Efficient Communication in VANETs Using Cellular IoT. In Intelligence Enabled Research; Springer: Berlin/Heidelberg, Germany, 2021; pp. 75–85.
28. Raja, G.; Anbalagan, S.; Vijayaraghavan, G.; Dhanasekaran, P.; Al-Otaibi, Y.D.; Bashir, A.K. Energy-Efficient End-to-End Security for Software Defined Vehicular Networks. IEEE Trans. Ind. Inform. 2020, 17, 5730–5737.
29. Khalil, A.; Farman, H.; Jan, B.; Khan, Z.; Koubâa, A. A Smart Energy-based Source Location Privacy Preservation (SESLPP) Model for IoT-based VANETs. In Transactions on Emerging Telecommunications Technologies; Wiley: Hoboken, NJ, USA, 2020; pp. 1–14.
30. Memon, I.; Hasan, M.K.; Shaikh, R.A.; Nebhen, J.; Bakar, K.A.A.; Hossain, E.; Tunio, M.H. Energy-Efficient Fuzzy Management System for Internet of Things Connected Vehicular Ad Hoc Networks. Electronics 2021, 10, 1068.
31. Ali, M.; Karimipour, H.; Tariq, M. Integration of Blockchain and Federated Learning for Internet of Things: Recent Advances and Future Challenges. Comput. Secur. 2021, 108, 102355.
32. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun. Mag. 2018, 56, 50–57.
33. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Alvin Yau, K.L.; Ji, Y. Blockchain for vehicular Internet of Things: Recent advances and open issues. Sensors 2020, 20, 5079.
34. Patil, P.; Sangeetha, M.; Bhaskar, V. Blockchain for IoT Access Control, Security and Privacy: A Review. Wirel. Pers. Commun. 2020, 117, 1815–1834.
35. Qu, Y.; Gao, L.; Luan, T.H.; Xiang, Y.; Yu, S.; Li, B.; Zheng, G. Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet Things J. 2020, 7, 5171–5183.