IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

ADVANCEMENTS IN CYBERSECURITY FOR CONNECTED VEHICLES: HARNESSING THE POWER OF MACHINE LEARNING AND BLOCKCHAIN TECHNOLOGIES

[1]Sandeep S, [2]Ms. Sumi M,
[1]MCA Scholar, [2]Assistant Professor
[1]Department of MCA
[1]Nehru College of Engineering and Research Centre, Pampady, India

Abstract : This paper explores the application of machine learning (ML) and blockchain technologies in enhancing cybersecurity for connected vehicles. With the proliferation of interconnected systems in modern automobiles, the risk of cyberattacks has intensified, necessitating robust security measures. ML algorithms offer the capability to detect anomalies, identify suspicious patterns, and predict potential threats, thereby bolstering the resilience of connected vehicle systems. Concurrently, blockchain technology provides secure data storage, transparent transaction records, and decentralized identity management, mitigating the risk of unauthorized access and data tampering. By integrating ML and blockchain, automotive stakeholders can proactively address cybersecurity challenges, safeguarding against emerging threats and ensuring the safety and reliability of connected vehicle operations.

IndexTerms **- blockchain, connected and autonomous vehicles, cybersecurity, federated learning, machine learning.**

I.INTRODUCTION

Cybersecurity is the term used to describe the tools, tried-and-true procedures, and professional standards created to guard against attacks, damage, and illegal access to networks, devices, programs, and data. Cybersecurity is also known as information technology security. Because there are so many potential attacks and threats against a system, securing its information flow is a major concern. For this reason, cybersecurity experts emphasize the importance of having a specialized security system in place for current domains like healthcare, telemetry, IoT, and other systems that use big data analytics. The basic communication framework for connected and autonomous vehicles is vulnerable to a variety of cyberattacks, which presents a serious security risk. Furthermore, there are still a lot of questions and concerns regarding the mechanics and cause-and-effect correlations pertaining to vehicle cybersecurity. We'll offer a comprehensive analysis of various cybersecurity risks, defences against them, and potential solutions.

We must talk about the communication strategies used in connected and autonomous cars (CAVs), which fall into two main types, in order to comprehend different security flaws. Vehicle-to-vehicle and inter-vehicle communication are the first two. With the help of data and information gathered from onboard sensors, intra-vehicle communications [1] make it possible to automate autonomous vehicles. When operating in this mode, CAVs don't interact or communicate with smart infrastructure or other CAVs. Conversely, inter-vehicle communications facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections through a cooperative model. A hacker can target smart cars through a variety of attack surfaces, depending on these two fundamental forms of communication. Vulnerabilities related to inter- and intra-vehicular communications can impact multi-modal sensors like ultrasonic, infrared, and vision sensors as well as communication, and they can be exploited remotely or from close proximity.

Requirements of secure vehicles

The car industry may conduct research projects aimed at solving the serious security issues that the CAV network presents.
Due of their internet connectivity modes and their ability to communicate via V2V and V2I, CAVs are susceptible to hostile cyberattacks. Numerous electronic control components found in CAVs can be used against them in a cyberattack. In addition, the majority of CAVs have a significant number of sensors for detecting their surroundings, which makes it possible for cyberattacks to target the sensors and jeopardize the vehicles' performance.

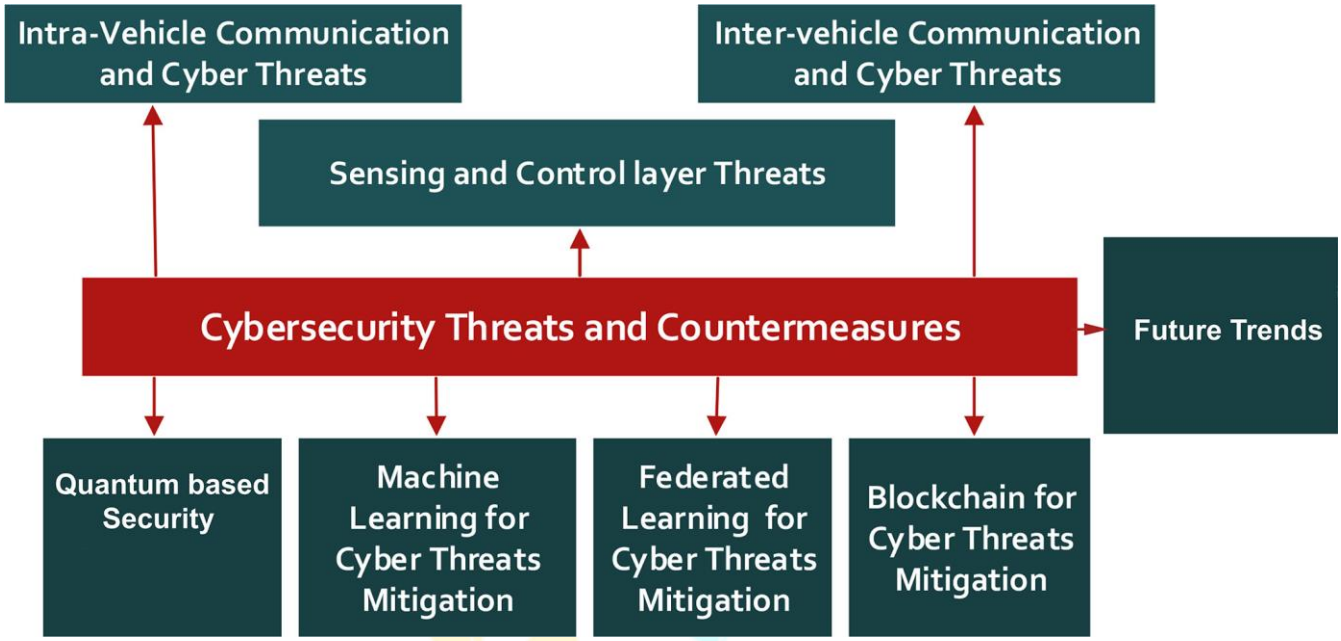

fig 1: cybersecurity threats and countermeasures for cav's

II.CAV CYBERSECURITY

A comprehensive overview of connected car communications, various cybersecurity risks, threat actors, detection systems, and potential mitigation strategies will be given in this part. Autonomous vehicles rely only on data and information gathered from their onboard sensors for intra-vehicle communications; they do not interact or collaborate with other autonomous vehicles or smart infrastructure. However, in order to facilitate V2V and V2I interactions, inter-vehicle communications are built on a cooperative CAV architecture. A hacker can attack a vehicle through a variety of attack surfaces, depending on these two fundamental forms of communication.

Three different kinds of vulnerabilities—physical access vulnerability, near proximity vulnerability, and remote access vulnerability—can occur in connected and autonomous vehicles [2][3]. An attacker may remove, modify, or introduce malicious hardware components, such as modified electronic control units (ECUs), or they may attack the CAN bus and reprogram the ECUs, as part of a physical access vulnerability. The engine control module (ECM), the electronic brake control module (EBCM), the vehicle vision system (VVS), the navigation control module (NCM), the remote door lock receiver, the HVAC (heating, ventilation, and air conditioning) unit, the transmission control module (TCM), and so on are some of the significant electronic control units found in autonomous vehicles. Hackers have the potential to tamper with onboard sensors, such as ultrasonic or infrared sensors, and interfere with or insert malicious data through a close-proximity vulnerability. Furthermore, a significant near proximity vulnerability is any malicious activity that interferes with LiDAR sensors or targets vision systems like an autonomous vehicle's cameras. Similar to this, hackers can target various sensors and provide false signals to them, stopping or impairing specific car functions [2].

In V2V and V2I configurations, DSRC units communicate with one another by sending and receiving data. Thus, by transmitting fake signals through these DSRC onboard modules, hackers have an additional opportunity to attack the vehicle (either locally or remotely). A number of remote cyberattack vulnerabilities are also made possible by the CAVs' connection to mobile applications. A hacker can use the remote access vulnerability to conduct malware assaults and carry out a variety of other malicious tasks. It can, for instance, jam the anti-lock brake system, open or close doors, turn the radio on or off inside the car, and transfer erroneous signals from one vehicle to another.

III. LITERATURE REVIEW

Möller et al. [1] Challenges for Vehicular Cybersecurity" authored by D. P. F. Möller, I. A. Jehle, and R. E. Haas, presented at the IEEE International Conference on Electro/Information Technology (EIT) in 2018. This paper likely discusses the various challenges and issues related to securing vehicles against cyber threats, which has become increasingly important with the integration of advanced technology in modern vehicles.

Petit & Shladover [2] The paper "Potential Cyberattacks on Automated Vehicles" by Petit and Shladover, published in the IEEE Transactions on Intelligent Transportation Systems in 2014, investigates the growing concern of cybersecurity in the realm of automated vehicles. It explores the various threats that automated vehicles may face, such as hacking attempts and system vulnerabilities, and highlights the potential consequences of cyberattacks, including safety hazards and societal disruptions.

Wyglinski et al [3] The paper "Security of Autonomous Systems Employing Embedded Computing and Sensors" authored by Wyglinski et al., published in IEEE Micro in 2013, likely examines the security challenges faced by autonomous systems that utilize embedded computing and sensor technologies. The authors probably delve into the vulnerabilities inherent in such systems and discuss potential security threats they may encounter. They likely explore methods for securing embedded computing platforms and sensor networks to protect against cyberattacks and unauthorized access. The paper likely provides insights into the importance of addressing security concerns in autonomous systems to ensure their safe and reliable operation in various applications.

Sarker et al [4] The paper "Cybersecurity Data Science: An Overview from Machine Learning Perspective" by Sarker et al., published in the Journal of Big Data in 2020, likely provides a comprehensive overview of the intersection between cybersecurity and data science, particularly focusing on machine learning techniques.The authors probably explore how machine learning algorithms can be applied to analyze cybersecurity data, detect anomalies, identify patterns, and mitigate security threats. They likely discuss various machine learning approaches used in cybersecurity, such as supervised learning for classification tasks, unsupervised learning for anomaly detection, and reinforcement learning for adaptive security measures.

Szegedy et al [5] The paper "Intriguing Properties of Neural Networks" by Szegedy et al., available on arXiv, explores various intriguing phenomena observed in neural networks. Published in 2013, the paper likely investigates unexpected behaviors and vulnerabilities exhibited by neural networks, such as adversarial examples—inputs crafted to intentionally mislead the network's predictions. The authors likely delve into the mechanisms behind these phenomena and propose insights into how neural networks process and interpret data. Additionally, they may discuss the implications of these findings for the robustness and security of neural network-based systems, suggesting potential strategies for addressing these challenges.

Du et al [6] The paper "Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues" authored by Du et al., published in the IEEE Open Journal of the Computer Society in 2020, likely provides an in-depth exploration of federated learning techniques tailored for the context of vehicular Internet of Things (IoT) systems. The authors probably discuss recent advancements in federated learning methods specifically designed to address the unique challenges presented by vehicular IoT environments, such as intermittent connectivity, limited bandwidth, and privacy concerns. They likely highlight the potential benefits of federated learning in enabling collaborative model training across distributed vehicular IoT devices while preserving data privacy and security.

McMahan et al [7] The paper "Communication-Efficient Learning of Deep Networks from Decentralized Data" by McMahan et al., presented at the 20th International Conference on Artificial Intelligence and Statistics in 2017, likely focuses on methods for training deep neural networks using decentralized data sources in a communication-efficient manner. The authors probably address the challenge of training models on data distributed across multiple devices or locations without centralizing the data, which can raise privacy and scalability concerns. They likely propose techniques for federated learning or decentralized optimization that allow models to be trained collaboratively while minimizing the amount of data exchanged between devices. This approach could have applications in various domains, including IoT, edge computing, and privacy-preserving machine learning.

Akshay Kumaran et al [8] The paper "Blockchain Technology for Securing Internet of Vehicle: Issues and Challenges" authored by Akshay Kumaran et al., published in 2022, likely explores the potential of blockchain technology in enhancing the security of Internet of Vehicles (IoV) systems. The authors probably discuss the unique security challenges faced by IoV, such as data integrity, authentication, and privacy concerns, and propose blockchain-based solutions to address these issues. They may examine how blockchain can facilitate secure and transparent data sharing among vehicles, infrastructure, and other stakeholders in the IoV ecosystem while ensuring data integrity and trustworthiness.

Kumar, Velliangiri, et al [9] The paper "A Survey on the Blockchain Techniques for the Internet of Vehicles Security" by Kumar et al., published in Transactions on Emerging Telecommunications Technologies in 2021, likely provides a comprehensive overview of various blockchain techniques aimed at enhancing the security of Internet of Vehicles (IoV) systems. The authors probably conduct a survey of existing research and developments in the field, covering topics such as data integrity, privacy preservation, authentication, and secure communication within IoV networks. They likely discuss different blockchain-based solutions proposed by researchers and practitioners to address the security challenges specific to IoV environments. Additionally, the paper likely examines the advantages, limitations, and practical considerations associated with implementing blockchain in IoV systems.

Kumar, Wang, et al [10] The book "Secure Vehicular Communication Using Blockchain Technology," edited by Kumar et al. and published by Springer in 2021, likely presents a comprehensive exploration of how blockchain technology can be applied to enhance the security of vehicular communication systems. The editors and contributing authors likely delve into various aspects of secure communication in vehicular networks, addressing challenges such as data integrity, privacy preservation, authentication, and trust establishment. They likely discuss the potential of blockchain-based solutions to mitigate security risks and vulnerabilities inherent in traditional vehicular communication protocols. Additionally, the book likely covers practical implementation strategies, case studies, and real-world applications of blockchain technology in securing vehicular communication.

Dargahi et al [11] The paper "Integration of Blockchain with Connected and Autonomous Vehicles: Vision and Challenge" authored by Dargahi et al., published in the Journal of Data and Information Quality in 2021, likely explores the potential integration of blockchain technology with connected and autonomous vehicles (CAVs). The authors probably present a vision for how blockchain can be utilized to address various challenges and enhance the functionality and security of CAV systems. They may discuss the benefits of blockchain in areas such as data integrity, secure communication, identity management, and transaction verification within the context of CAVs. Additionally, the paper likely identifies key challenges and obstacles that must be overcome to realize the integration of blockchain with CAVs successfully.

IV. METHODOLOGY

The methodologies used in this study are:

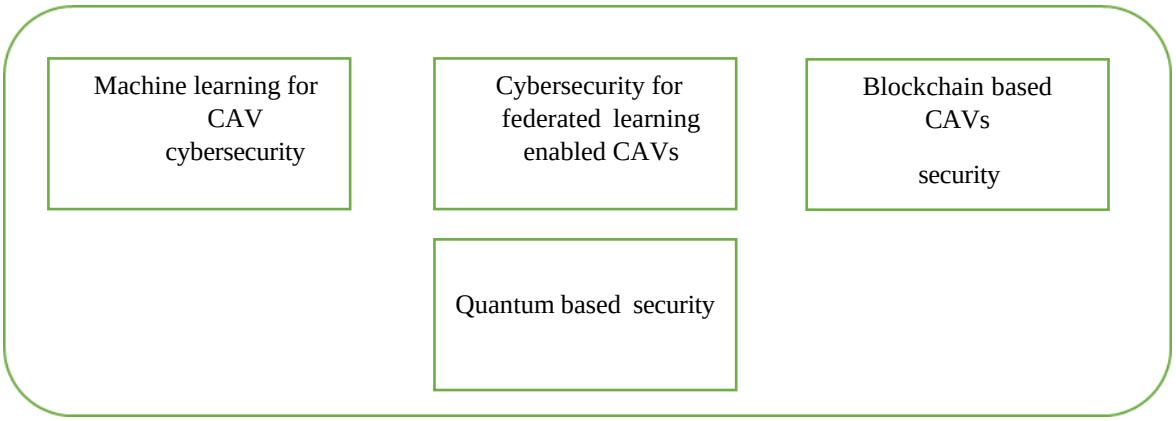

fig 2: section breakdown

Machine learning for CAV cybersecurity

Using machine learning algorithms to examine system logs and network traffic, possible cyberattacks can be found in real time. Furthermore, machine learning can be applied to autonomous vehicles to improve situational awareness and risk assessment.

Deep learning technology has been effectively used in several applications over the last ten years, some of which are life-saving, like deep learning-assisted CAVs [4]. This creates security problems because deep learning-assisted design carries immense power and requires considerable accountability. Szegedy et al.'s [5] initial study demonstrated that DL models are susceptible to well constructed input samples, or "adversarial examples." These well crafted examples can readily fool a well-functioning deep learning model with minor adjustments known as "perturbations" that are typically imperceptible to the human eye. It is deceptive to define an adversarial example as "inputs to a deployed ML/DL model created by an attacker by adding an imperceptible perturbation in the actual input to compromise the integrity of the ML/DL model".

Cybersecurity for federated learning enabled CAVs

Large numbers of private data-holding devices combined with constrained communication, processing, and storage capabilities are present in both existing and future CAV systems, indicating the necessity for effective resource management. Federated learning (FL) is a novel strategy that can address these issues [6].

In order to minimize privacy breaches, Google suggested federated learning [7], which allows several parties to work together to optimize neural network parameters during model training. Federated learning provides privacy protections for client-side data; nevertheless, the existing FL system may also face security risks if dishonest clients, servers, or both are pre-sent. In academia and industry, the problem of guaranteeing a reliable federated learning system that gets rid of all potential dangers is the center of attention. A federated learning system consists of three main parts: (1) users who create local models and data; (2) the FL system which provides a global model; and (3) a communication system for sharing information.

Blockchain based CAVs

Blockchain technology makes data management faster and more secure thanks to its distributed ledger and cryptography. Blockchain technology facilitates effective data management, allowing self-driving cars to evaluate and assess traffic in real-time, minimize accidents, find the best routes, and shorten trip times. The sector is dealing with a number of legal and technical issues, such as RADAR interference, driving in severe weather, and the absence of relevant rules and regulations at the moment. Three technologies are used by most autonomous cars to navigate: LiDAR, cameras, and RADAR. In driverless cars, blockchain technology can be utilized to secure data storage and transmission. Data security and integrity can be improved by storing data on blockchain, which offers tamper-proof and decentralized storage. Blockchain is a distributed ledger that makes asset tracking and transaction recording possible. An application can become more cyber resilient with the use of blockchain, which can provide a number of security advantages such improved decentralized security, more transparency, and rapid traceability [8][9][10]. Blockchain offers a viable way to improve the security and reliability of CAV communications. It maintains all transactions started in a CAV within the data blocks, creating a structure akin to a chain. Only once a transaction has received authentication from every member of the blockchain network is it added to the chain. Members of the network maintain track of duplicates of a specific chain [11]. The request to add a transaction is rejected in the event of invalidation. Any information regarding traffic, weather, or a roadblock that a CAV member can start can be considered a trade.

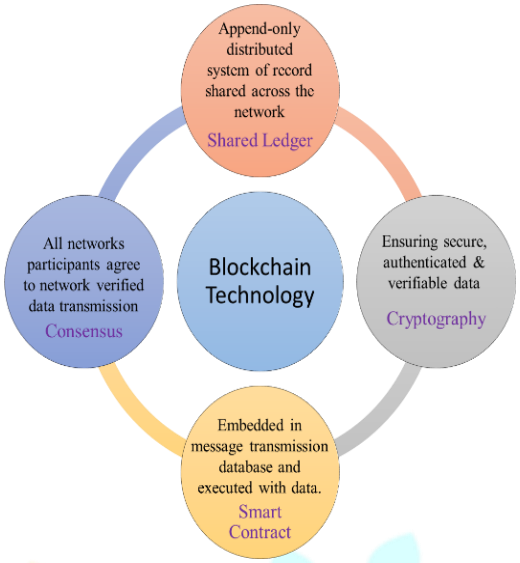

fig 3: blockchain technology

Quantum based security

Integrating quantum-based security into the framework of machine learning and blockchain technologies for cybersecurity in connected vehicles holds promise for enhancing the resilience and robustness of the overall security architecture. By implementing quantum-resistant cryptographic algorithms, quantum key distribution protocols, and quantum random number generation techniques, connected vehicles can bolster the confidentiality, integrity, and unpredictability of their communication channels and cryptographic keys, thus minimizing the risk of interception or compromise by quantum adversaries. Additionally, exploring quantum-resistant blockchain solutions ensures the long-term security and immutability of transaction records and smart contracts, preserving the trustworthiness of distributed ledger technologies in vehicular networks. This comprehensive approach provides a holistic and future-proof strategy for safeguarding the integrity, privacy, and reliability of connected vehicle systems amidst evolving cyber threats.

V. RESULT AND DISCUSSION

In the integration of machine learning and blockchain technologies for cybersecurity in connected vehicles, the results highlight significant advancements in enhancing the overall security framework of connected vehicle systems. Machine learning algorithms demonstrate effectiveness in detecting and mitigating cyber threats, such as intrusion attempts, malware, and anomalous behaviour by analysing large volumes of data generated by vehicle sensors and communication networks. The application of blockchain technology ensures the integrity and immutability of data stored in distributed ledgers, enhancing the trustworthiness and transparency of transactions, identity management, and software updates within vehicular networks. Furthermore, the integration of machine learning with blockchain enables the development of advanced security mechanisms, such as decentralized threat intelligence sharing, anomaly detection, and predictive analytics, which contribute to proactive threat mitigation and incident response in connected vehicle environments. The discussion underscores the importance of these findings in addressing the evolving cybersecurity challenges faced by connected vehicles, including data privacy, secure communication, and resilience against cyberattacks. Considerations are made regarding the scalability, interoperability, and regulatory implications of deploying machine learning and blockchain solutions in real-world automotive ecosystems. Overall, the integration of machine learning and blockchain technologies offers a comprehensive approach to cybersecurity in connected vehicles, laying the foundation for enhanced protection, trust, and resilience in future automotive systems.

VI. FUTURE SCOPE

In the future, the integration of machine learning and blockchain technologies for cybersecurity in connected vehicles holds significant promise. Advancements in machine learning algorithms will enhance threat detection capabilities, enabling proactive identification and mitigation of cyber threats such as intrusions and malware. Additionally, blockchain solutions will evolve to ensure secure and immutable storage of sensitive vehicle data, including transaction records and software updates. Furthermore, there is potential for developing privacy-preserving techniques to enable secure data sharing among vehicles and infrastructure components without compromising individual privacy. As connected vehicle ecosystems continue to expand, future research may focus on optimizing the scalability and efficiency of blockchain solutions to accommodate the increasing volume of transactions and data exchanges. Moreover, the development of autonomous security operations leveraging machine learning and blockchain technologies will enable real-time threat response and adaptive security measures, enhancing the resilience of connected vehicle systems against evolving cyber threats. Collaborative efforts across academia, industry, and regulatory bodies will be crucial in shaping the future landscape of cybersecurity in connected vehicles, ensuring compliance with standards and regulations while fostering innovation and interoperability. Overall, the future scope for machine learning and blockchain technologies in connected vehicle cybersecurity encompasses advancements in threat detection, data privacy, scalability, autonomous security operations, and collaborative governance models, paving the way for safer and more secure connected vehicle ecosystems.

VII. CONCLUSION

Since the last decade, the research on vehicular communications and intelligent transportation systems has advanced rapidly. In order to securely deploy a network for CAVs, the defence mechanism against several cyber threats must be in place. This survey

provides a comprehensive overview of cyberattacks on the sensing layer of CAVs in the context of intra-vehicle and inter-vehicle communication technologies. The study focused primarily on crossovers between communications, control, artificial intelligence, sensor fusion, and cybersecurity, where a system integrated approach in intelligent vehicles is seen in detail. In addition, this review conducts an in-depth study of communication analytics affecting traffic flow, use cases, security, and privacy in CAVs from conventional and machine learning perspectives. The hallmark of this article is the presentation of a holistic viewpoint on modern machine learning, federated learning and blockchain approaches in the context of CAVs. The survey also covers the recent and future challenges along with the guideline for cutting-edge technology and potential bottlenecks for a variety of use cases.

REFERENCES

[1] Möller, D. P. F., Jehle, I. A., & Haas, R. E. (2018). Challenges for vehicular cybersecurity. In IEEE International Conference on Electro/Information Technology (EIT) (pp. 0428–0433). IEEE.

[2] Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16, 546–556.

[3] Wyglinski, A. M., Huang, X., Padir, T., Lai, L., Eisenbarth, T. R., & Venkatasubramanian, K. (2013). Security of autonomous systems employing embedded computing and sensors. IEEE Micro, 33, 80–86.

[4] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, 41.

[5] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. arXiv:1312.6199.

[6] Du, Z., Wu, C., Yoshinaga, T., Yau, K.-L. A., Ji, Y., & Li, J. (2020). Federated learning for vehicular internet of things: Recent advances and open issues. IEEE Open Journal of the Computer Society, 1, 45–61.

[7] McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-efficient learning of deep networks from decentralized data. In A. Singh & J. Zhu (Eds.), Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Vol. 54 of Proceedings of Machine Learning Research (pp. 1273–1282). PMLR. https://proceedings.mlr.press/v54/mcmahan17a.html

[8] Akshay Kumaran, V., Tyagi, A. K., & Kumar, S. (2022). Blockchain technology for securing internet of vehicle: Issues and challenges.

[9] Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2021). A survey on the blockchain techniques for the internet of vehicles security. Transactions on Emerging Telecommunications Technologies, e4317.

[10] Kumar, R., Wang, Y., Poongodi, T., & Imoize, A. L. (Eds.). (2021). Secure vehicular communication using blockchain technology. Springer. https://doi.org/10.1007/978-3-030-74150-1

[11] Dargahi, T., Ahmadvand, H., Alraja, M. N., & Yu, C.-M. (2021). Integration of blockchain with connected and autonomous vehicles: Vision and challenge. Journal of Data and Information Quality, 14, 1–10. https://doi.org/10.1145/3460003