A research on Security enhancement in Automobile Industry using the blockchain concept and Artificial Intelligence

Abburi Sampath
[1] Student, B.Tech, Dept of Mechanical Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana
Jawaharlal Nehru of Technological University Hyderabad, Telangana

Abstract *- Nowadays autonomous vehicles and security measure improvements in automobile industry are attracting lot of attention. For addressing the security and safety several articles are reviewed in this study. Before the autonomous vehicles' wide adoption, blockchain technologies are utilized in various fields. This paper presents the Security enhancement related with autonomous vehicles using the blockchain concept and also discussed about various techniques like Artificial intelligence, Deep learning and machine learning algorithms in automobile industry. This proposed review articles have covered the countermeasures, blockchain enabled automotive/vehicle networks and several attacks. Blockchain based data storage, handling security attacks, security countermeasures and authentication process have been analysed in this study for automobile organization enhancement. The comparative analysis has been made to address the benefits and limitations of the various technologies used. However, the above mentioned challenges have been overcome by the blockchain with distributed framework. This study significantly focused on blockchain approaches for adapting the information accessing for entities limits in ecosystem of connected vehicle. Among the roadside and vehicles, the challenge response based data exchange are utilized. It leads to vehicle internal state monitoring for in-vehicle identification. For valid and authentic communication blockchain is the better approach in vehicular network, according to this study. Compatible storage and appropriate response time ensured by the blockchain technologies. Several significant functions like vehicular forensics and trust management are exhibited for vehicular networks security stated from other articles which have been used machine learning and deep learning approaches.*

Key Words**: Automobile industry, Blockchain, Artificial intelligence, Deep learning, Machine Learning**

Date of Submission: 23-07-2021 Date of acceptance: 08-08-2021

I. INTRODUCTION

The automobile industry is in a track of technological progression. The modern cars have advanced security features, but they are a bit costlier. So, the common man who can afford low-end automobiles needs to compromise on the latest features such as advanced safety, voice commanding, connected cars, etc. Due to this, road safety and user-friendliness are decreasing, which is having a substantial adversarial impact on our society. Smart vehicles are equipped with different sensors and wireless communication modules that allow vehicles to sense various information, such as road conditions, traffic rates, accident reports, etc.[1]. This sensory information is shared with other smart vehicles and Road Side Units and is known as Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Road-Side-Unit (V2R) communication, respectively. During the last few years, smart vehicles have gained much popularity due to their excellent features and capabilities. The huge increase in the number of smart vehicles leads to the generation of huge amount of real-time sensory data, which become quite difficult to handle as the time progresses. To store this huge data in a secured manner, a secure communication channel is required. The traditional centralized systems lack in providing essential functionalities. Therefore, to overcome the above mentioned limitations, there is a need for a decentralized architecture that fulfils the VN's requirements. However, decentralized systems still face some issues like lack of security and privacy, lack of trust, etc.[2, 3].

To provide security, ensure privacy and establish trust between entities, blockchain technology was introduced by Satoshi Nakamoto in 2008. It is an increasing list of records, stored in the form of blocks, which are joined together in a chronological order to form a chain using cryptographic hashes. Each block contains multiple components, such as a cryptographic hash of the previous block, timestamp at which block is generated, transaction data in the form of Merkle root tree and nonce, which is an arbitrary number used for mining process. The basic structure of the block is shown in Figure 1[4].

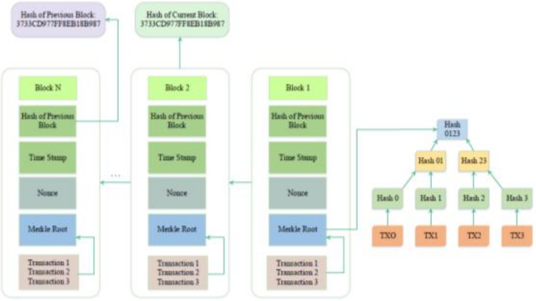

Fig.1. Structure of blocks

With the invention of blockchain, limitations of centralized architecture are eliminated. Blockchain ensures security, privacy preservation, decentralized architecture and data integrity. Due to the exceptional features of blockchain, it is being utilized in several fields of today's world like Internet-of-Things (IoT), smart grids, VNs, etc. Secure data sharing amongst smart vehicles is also made possible due to the use of blockchain technology.
Apart from blockchain, Machine learning and deep learning technologies have also been implemented in certain articles for enhancing the automobiles industry[5, 6]. The major contribution of this study involves,

- To review the various challenges associated in the automobile industry
- To analyse the blockchain technologies implementation in the autonomous vehicles and handling the various counter measures in vehicular networks.
- To compare the existing studies with respect to their benefits and limitations associated with automobiles.

The following section discussed about the significant part of the review like various techniques applicable in automobile industry. Followed b the comparative analysis has been tabulated. Finally, the paper is concluded and future enhancement is described.

II. Automobile Industry- Comprehensive Review

2.1 Challenges in Automobiles industry related with various framework adoption

In this review article various challenges have been exhibited with respect to the UK automotive industry of blockchain framework. This study evaluated nearly 71 articles and depicted the management and technical challenges providing the blockchain adoption with respect to operational excellence. Meta-analysis can be done in future. However, this study has mainly focused only on UK automotive industry and thus other industries and countries generalization have been limited. The sample size has been affected with respect to operational excellence since there are lot of journals lacking in blockchain or recent advancement technologies specifically in automotive industry. Higher priority has been given to TOE approach gives significant to legal issues and government regulatory without any competitive and customer pressure[7]. In smart society, intelligent transport system has been attained lot of popularity. The autonomous vehicles interconnection has been made through Uber, Google and Toshiba like global automotive stakeholders which have been utilized for road traffic management refer as connected AV. It has been susceptible to several security and safety problems, timing attacks, man-in-middle attacks, denial of service attacks resulted in specific areas concerns. However, the single point failure considered as centralized systems. Security and privacy issues have been having been analysed. the defence mechanism is required for the CAV system and thus blockchain mechanism has been used. it can handle all type of attacks, privacy and security issues have been mitigated. This study has been evaluated on the communication and computation stud on smart city incorporation using the edge computing. Reliability and low-latency has to be focused in future[8].

Innovative feature needed for improvising the automobiles at lesser cost. This study integrated the Google assistants with the smart accident precognition system for limit the number of accidents and improvising the passengers safety. Various factors have been considered like insurance remainders, low fuel remainder, lock and unlock, alerts, speed, safety measures like airbags, handbrakes, seatbelts and door locks usages. All these factors have been checked automatically and the proposed system has been detected accidents and modified with respect to several conditions. This kind of vehicle authentication is secure due to RFID keyless entry stated in this study. Positive impacts recorded through this proposed system in society and automobile industry[9]. For the vehicular network blockchain based secure data mechanism and resource efficiency integration has been established in this study. For handling the centralized storage system distributed file storage system refer as IPFS has been introduced. IVTP utilized for the fair payments and vehicles trust values. Resource utilization optimized b blockchain technology and this study's system established the secure data sharing surroundings. This article reviewed the ever edge vehicle nodes and their reputation has evaluated. Secure and efficient data sharing strategy has implemented for vehicular network. When data size increases, vehicle authentication cost increases. Various algorithms have been required for maintain the data size and system cost[10].

Artificial intelligence has been prospering recent days in Indian market but it started globally around 20th century. Higher end result has been obtained while using the artificial intelligence. In IoT also higher experience has been gained. For customers mobile applications to support automobiles provided significant space and it has been considered as higher choice. This study reviewed the tesla cars manufacturing organization. The AI introduction to Tesla has been studied. However the major drawback is this study has been limited to tesla cars and artificial intelligence[11]. High stake vehicles compromising ahs considered as challenging and to overcome this soft security improvisation has been utilized in this study as block verification and minor selection. Secure miner selection ensured b voting scheme which has security based. Historical interactions utilized for the reputations and other vehicles opinions suggested. In earlier stage, standby miners and Active miners considered as candidates with greater reputation. Among active miners, internal collusion prevented in next stage, standby miners audited and verified the new generated blocks. Standby miners and active miners interactions modelled b the contrast theory. The delay and verification of block security considered as another concern. Security and efficiency are attained from this proposed system[12].

In case of attacks execution in smart vehicles, connectedness and automation increase can elaborate the surface of attacks. Thus the malicious entry has been successful attained. For securing the smart vehicles, blockchain framework has been established in this study as B-FERL. It utilized blockchain approaches for adapting the information accessing for entities limits in ecosystem of connected vehicle. Among the roadside and vehicles, the challenge response exchange of data utilized. It leads to vehicle internal state monitoring for in-vehicle identification. For valid and authentic communication blockchain is the better approach in vehicular network, according to this study. For identified attacks, B-FERL system is resilient. Compatible storage and appropriate response time ensured by the B-FERL system. Several significant functions like vehicular forensics and trust management are exhibited for vehicular networks security[13]. For the cyber attacks identification and mitigation, innovative methods have been focused recently. Several challenges have been recorded and the security concerns have been considered based on attacker information. From the connected automated vehicles, security enhancement is important. These challenges are considered as better practices in CAV organization[14].

Table 1. Challenges facing in automobile industry confronted with blockchain technologies

Specific challenges[15]	Stake-Holder
Transparency lacking with respect to car history. Repairs and maintenance costs-unpredictable and sometimes lack of trusts Informed buying lacking Car insurance lacking. IoT connected and autonomous vehicles- lack of trust	Car buyers/owners/sellers
Expensive car rides. Higher maintenance required Common mobility provider lacking. Instant payment lacking.	Car sharing/ car lending/ ride hailing
Claim management- expensive and inefficient. Information sharing lacking Inaccurate customer policy	Insurance companies
Customer retention Low margin Brand confidence lacking	Independent repair shops
Updated purchase, car ownership, maintenance records. Higher warrant claim Cyber attacks	Car dealer/manufacturer/suppliers
Updated state registers Current legislation compliance Traffic congestions and road conditions compliance	Public and Govt organization

Decision making and machine learning is helpful in bigdata analysis. For IoV networks performance enhancement several potential applications have been followed. In higher density IoV networks, the congestion issues have been addressed which attained experience and quality services. This study analysed the data flow, resource tools, network management control, site forecasting and communication networks. The performance are based on the automated learning applications. Smart integrated systems generated with respect to machine learning and parallel computing which are build with energy efficiency and immense parallel processing. Various operations related with IoV exhibited like signal or image processing which is multidimensional[16]. The recent business models and manufacturing operation mode transformed in automotive industry due to the latest technologies and digitalization. The manufacturing, maintenance services, government regulations, insurance have been disrupted sue to autonomous cars adoption. For the sustainable smart city ecosystem, blockchain technology has been implemented in automotive industry. Miner node selection framework utilized for the architecture of blockchain based distributed networks. Ethereum blockchain are used and simulation has been performed for the mined blocks in smart cities [17].

2.2 Attacking Scenarios

When an intruder needs to do certain malicious process in the network, various attacking strategies has been adopted. Compromises of following

- Sensors or IoT devices
- Rating modifications provided by riders
- Traffic Jams
- Data falsification are the few problems which could be easily developed by the intruders for fulfilling their needs. The following are the attacking scenarios between the vehicle and the user during a ride.

Inclusion of compromised IoT by the intruders

When registration of compromised IoT was done by the intruder for the execution of passive or active attacks, BC neighbouring nodes detects the malpractice immediately through checking its actions such as stealing.

Misbehaviour with the user

If a user asks for a trip and the driver too agrees to start the ride, but during the ride, if the driver misbehaves with the user by altering the route selected by the user. Then the corresponding IoT sensors that monitors continuously or tracing the precise location will take cation for preventing the mis-happenings. Then the cab driver must be at the receiving end of punishment with necessary actions such as punishment with degradation.

Rating Modification

When the ratings are submitted to any cab driver, it could not be modified even after successfully compromising of IoT devices.

Data falsification attacks

It is one of the predominant problems in CAV in which the vehicles depend on the data received from neighbouring vehicles.

Traffic Jam

Here, the intruders might try to take diversion of the path suggestions on roads with own advantages. But for preventing these attacking techniques, the study[18] suggested a secured cab sharing and riding mechanism by means of block chain. But for validating the suggested mechanism, an analytical simulation was performed on several parameters for proving the efficiency of the suggested framework. The paper [18]considered IoV application and suggested a security process for the linked autonomous vehicle services with BC method. For providing the transparency and secrecy among the cab drivers and the customers, every activity of the entity in accordance with the IoT devices has been recorded and traced inside the BC. The BC process has been utilized for extracting the IoT data and store the records for ensuring the safety of the customer and the security of the devices by offering transparency among several authorities. This study considerably decreased the fake request of the user, IoT compromising and the modification in the stored user ratings.

The results simulated against several parameters depicted around 80% success rate in the framework when compared with the prevailing approach against the specified parameters. The system against a huge number of nodes and the transaction alteration stored already at BC network would be presented in case of future communications. Furthermore, techniques like deep and reinforcement learning has been adopted for increasing the system intelligent.

2.3 Block chain technology in securing autonomous vehicles

The rapid growth of IoV led to huge difficulties in storing enormous information while responding in real time. [19]. The study [20] suggested a robust distributed digital forensics method for auto-insurance liability setup for expected autonomous vehicles which provide untampered proof to process auto insurance claims and in the settlement of disputes. This study avoids the possibility of single trust point allowing multiple subjects to agree simultaneously on the evidence required for processing compensation claims. This work has been found to be based on an authorized BC that is divided to restrict communication to the targeted participants. Furthermore, the study offered a new liability attribution setup for autonomous vehicle, detected key requirements and described the threat model. The study also described the evidence structure including the process of verification and validation by the entities in the suggested model. Apart from that, the study also conducted an analysis for depicting the resilient effectiveness against possible attacks from the corresponding entities. The study also attempted to continue the work to health insurance and accidental reconstruction in the future.

Similarly [21] developed a framework for the autonomous cars for establishing trusted parties by integrating the distributed ledgers and self-driving cars in traffic for providing a public trust. This framework depends on providing decision logs of such autonomous vehicles and also provides a reliable solution for the operation of autonomous cars in untrusted environment without the requirement of central authority. This framework could also be developed and implemented to other such unmanned systems.

[22] suggested a BC inspired event recording system for the vehicles. Particularly the study designed the proof of event for obtaining indisputable accident through the provision of verifiable and trustable event data. The results of the frame work are found to be feasible and effective in the generation of storing accidental records in the BC based vehicular networks.

[23] explored the process of blockchain technology expansion in the use of transport networks, particularly considering the distributed and secured big data storage. The paper performed performance analysis and theoretical modelling of vehicle network systems, from which this article could be potentially used as a guide for analysing block chain IoV technologies. Similarly [24] suggested a safe EV charging system based on the blockchain that ensured safe mutual authentication, key security, perfect direct secrecy, and anonymity as well as effective charging. For testing the efficiency of the suggested solution, the authors compare it with existing ones and proved to be effective. [25] indicated that the research corresponding to electric vehicles (EV) is predominantly focused on hardware, like the battery charging, and there is still not adequate software research, like a billing system, that is required to be developed. The authors suggested an intelligent contract BC for the safe charging of electric vehicles. The study considered a blockchain system combined with EV and CS (charging system). Then an algorithm has been presented to obtain consensus for the effective exchange of energy in the BC. Next, several terms of the contract are analysed for satisfying the individual energy consumption preferences of EV and maximize the operator utility. The article of [26]is devoted to the EV charging system that presents the concept of using a BC technology when charging electric vehicles. The paper depicted the concept of a framework in which using chains of blocks it would be possible to calculate the sale and purchase of electricity in the charger. This technology could allow partial or fully decentralization of process, full automation without the involvement of the intermediate devices. This article also depicted how such operations *might be* carried out automatically and without supervision that allows the application of established principles, rules and assumptions on the basis of smart contracts. The use of blockchain technology for modelling the electricity metering system during the charging process, as well as the possibility of participating in the market of infrastructure under construction, goes beyond the financial application of the technology. Aspects for which the blockchain could become a factor in modifying the business models are more secure and efficient applications, elimination of unnecessary intermediaries or more number of innovations. The article of [19] presented a new decentralized and secured architecture for the protecting data of the connected vehicles, on the basis of the blockchain paradigm. The authors believed that the study would serve as the first step for introducing the blockchain technology from cryptocurrency systems for traffic management systems. The authors created a prototype block network and an agreed protocol and depicted how, by converting the original centralized car network to decentralized network, the original vulnerable system could be protected from hacker attacks. As [27] indicated, the joint vehicle usage by passengers reduced the travel time, congestion and carbon emissions. But, since passengers usually search for drivers through a cloud server, this leads to pointless communication overhead and surge in the reply latency. The advent of fog computing for the local processing of data with considerably low latency lead to security and confidentiality issues, since when users share it, personal information of users can be disclosed. The authors believed that the consortium BC might provide a reliable solution if the different carrier companies work together for serving the users, and user privacy and the company confidentiality has also been considered.

Table 2: Comparative analysis

S.No	Author	Description	Benefits	Limitations
1	[28]	This paper disables automatically the vehicle engine. It Detects the theft of vehicle theft. It also transmits the vehicle coordinates to mobile phone.	This method of tracking enables the recovery of vehicle. It employs facial recognition and malware detection.	GSM messages may be jammed. The study used facial recognition could be tricked in few instances with high resolution owner copies.
2	[29]	The study utilize fingerprint for authenticating the user. Also it employs password as backup system.	The biometrics improve the conventional security. The password offers contingency.	Easily susceptible for fingerprint spoofing. Biometrics bypass would be enables during access to password by attacker.
3	[30]	When vehicle is lost the study uses password system with artificial intelligence.	This study provides effective tracking capabilities	With just a key the whole security system could be destroyed.
4	[31]	-Uses identification information on a transceiver to validate user.	-Augments traditional security	Susceptible to interception
5	[32]	This method checks the information sent to CAN bus by means of security process	It prevents and protects the vehicular system from unauthorized accession	Easily susceptible to spoofed information from the attackers
6	[33]	The study used GPS and accelerometer for the detection of vehicle location and movement. - -	It leads to easy tracking of vehicles	This study could not avoid unauthorized accession by the intruders

III. CONCLUSIONS

Intelligent automotive technology has been developing to a great extent, and recent advances suggested that autonomous vehicle security is more necessary. This study addressed the safety and security of autonomous vehicles with the employment of various articles like artificial intelligence, machine learning, deep learning, Blockchain technology etc. Various countermeasures, and attacks have been discussed in detail in this study. Furthermore, limitations and benefits of the prevailing studies are also provided. This study significantly focused on Blockchain methods for adapting the accessing information connected vehicle. Similarly, importance has also been provided to vehicular forensics and trust management are presented for vehicular networks security. This research will serve as significant step towards the enhancement of a traffic control system for the autonomous vehicles that helps to resolve the problem of cybersecurity.

Since blockchain is still in its nascent stage, it is obvious from the present study that there is limited research in exploring categories and differentiate its technological and management challenges and opportunities based on the analysis conducted for the present study. However, this provides many directions for future research. The blockchain technological and management challenges and opportunities for operational excellence in the context of the automotive industry have not received increase attention compare to other industries such as the financial industry across the globe. Exploring more study in this area can provide the automotive industry with an insight into the uses of blockchain. Also, blockchain technology has received increasing attention from different researchers in the financial institutions, business and management etc, more study can also be explored in the automotive industry.

ACKNOWLEDGEMENT

REFERENCES

[1]. A. Chandak, S. Chandak, and A. Dalpati, "A study of impact of supply chain strategy on supply chain performance: An empirical investigation on automobile industry in India," Journal of Supply Chain Management Systems, vol. 7, no. 3, p. 1, 2018.

[2]. Z. Yang, K. Zheng, K. Yang, and V. C. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), 2017: IEEE, pp. 1-5.

[3]. J. Bhatia, Y. Modi, S. Tanwar, and M. Bhavsar, "Software defined vehicular networks: A comprehensive review," International Journal of Communication Systems, vol. 32, no. 12, p. e4005, 2019.

[4]. V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," IEEE Vehicular Technology Magazine, vol. 13, no. 2, pp. 121-127, 2018.

[5]. F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," Proceedings of the IEEE, vol. 108, no. 2, pp. 292-307, 2019.

[6]. Q. Rao and J. Frtunikj, "Deep learning for self-driving cars: Chances and challenges," in Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems, 2018, pp. 35-38.

[7]. A. Upadhyay, J. O. Ayodele, A. Kumar, and J. A. Garza-Reyes, "A review of challenges and opportunities of blockchain adoption for operational excellence in the UK automotive Industry," Journal of Global Operations and Strategic Sourcing, 2020.

[8]. R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," Transactions on Emerging Telecommunications Technologies, p. e4009, 2020.

[9]. V. G. Menon, S. Jacob, S. Joseph, P. Sehdev, M. R. Khosravi, and F. Al-Turjman, "An IoT-enabled intelligent automobile system for smart cities," Internet of Things, p. 100213, 2020.

[10]. M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," Applied Sciences, vol. 10, no. 6, p. 2011, 2020.

[11]. P. Ajitha and A. Nagra, "An Overview of Artificial Intelligence in Automobile Industry–A Case Study on Tesla Cars," Solid State Technology, vol. 64, no. 2, pp. 503-512, 2021.

[12]. J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906-2920, 2019.

[13]. C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," Information Processing & Management, vol. 58, no. 1, p. 102426, 2021.

[14]. M. Chowdhury, M. Islam, and Z. Khan, "Security of connected and automated vehicles," arXiv preprint arXiv:2012.13464, 2020.

[15]. P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," IEEE Access, vol. 7, pp. 17578-17598, 2019.

[16]. E. S. Ali et al., "Machine Learning Technologies for Secure Vehicular Communication in Internet of Vehicles: Recent Advances and Applications," Security and Communication Networks, vol. 2021, 2021.

[17]. P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4197-4205, 2018.

[18]. G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," Sensors, vol. 19, no. 14, p. 3165, 2019.

[19]. S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova, and A. Pashkevich, "Blockchain technology on the way of autonomous vehicles development," Transportation Research Procedia, vol. 44, pp. 168-175, 2020.

[20]. C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," arXiv preprint arXiv:1802.05050, 2018.

[21]. S. Ayvaz and S. C. Cetin, "Witness of Things: Blockchain-based distributed decision record-keeping system for autonomous vehicles," International Journal of Intelligent Unmanned Systems, 2019.

[22]. H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Proof-of-Event Recording System for Autonomous Vehicles: A Blockchain-Based Solution," IEEE Access, vol. 8, pp. 182776-182786, 2020.

[23]. T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640-4649, 2018.

[24]. C. Matthes et al., "The Collaborative Virtual Reality Neurorobotics Lab," in 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), 2019: IEEE, pp. 1671-1674.

[25]. U. Asfia, V. Kamuni, A. Sheikh, S. Wagh, and D. Patel, "Energy trading of electric vehicles using blockchain and smart contracts," in 2019 18th European Control Conference (ECC), 2019: IEEE, pp. 3958-3963.

[26]. A. Zielińska, M. Skowron, and A. Bień, "The concept of the blockchain technology model use to settle the charging process of an electric vehicle," in 2019 Applications of Electromagnetics in Modern Engineering and Medicine (PTZE), 2019: IEEE, pp. 271-274.

[27]. M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4573-4584, 2018.

[28]. A. S. Krishna and S. A. Hussain, "Smart vehicle security and defending against collaborative attacks by malware," Int. J. Embed. Softw. Comput, 2015.

[29]. K. Mawonde, B. Isong, F. Lugayizi, and A. M. Abu-Mahfouz, "A survey on vehicle security systems: Approaches and technologies," in IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, 2018: IEEE, pp. 4633-4638.

[30]. F. Shaikh, N. Chikhal, and S. Joshi, "Advanced Vehicle Security and Safety System for Two Wheelers," International Journal of Engineering and Management Research (IJEMR), vol. 6, no. 2, pp. 28-30, 2016.

[31]. J. Harvey, T. F. Doyle, and M. L. Segal, "Vehicle security system and method," ed: Google Patents, 2014.

[32]. T. R. Markham, "Vehicle security module system," ed: Google Patents, 2018.

[33]. K. E. Flick, "Vehicle control system including accelerometer based security warning and related methods," ed: Google Patents, 2016.