Journal of
Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777229

BLOCK CHAIN FRAMEWORK FOR VEHICLE COLLISION AVOIDANCE: A BREAKTHROUGH IN VEHICULAR INTERNET OF THINGS

S.Sharanya[1], SV. Shri Bharathi[2], *R.Radha [3]
[1, 2, 3] Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, Chennai- - 603203, India.
*Corresponding author-Mail id: radhar@srmist.edu.in

Abstract:
Recent times have witnessed tremendous development in the genre of autonomous vehicles. The rampant evolution in Information and Communication technologies, Internet of Things, Artificial Intelligence and Block Chain has changed the human lifestyle. The profound impact of these technologies has raised the market of building safe and reliable vehicles. The proposed framework taps the Block chain technology, a decentralized ledger scheme with high degree of reliability in developing a spatio-temporal collision avoidance system. The heterogeneous sensors deployed at every vehicle monitors the motion of vehicle and forewarns all the nodes connected to the system about the chances of collisions based on individual vehicle's motion and proximity. This framework can be implemented on the existing network infrastructure. The design challenges discussed in the latter part offers a wide scope for future researchers in building autonomous vehicles with ensured safety.
Keywords: Block chain technology, Vehicular IoT, Road Side Units, transaction, Collision avoidance, Sensors

Introduction

The technological advancements have increased the autonomy of smart vehicles by integrating Internet of Things (IoT), edge computing and communication systems. Automotive IoT or Vehicular IoT(VIoT) focus on designing and building new automobiles that makes them smart with intact intelligence thus fostering more comfortable and safe driving experience. VIoT opens doors for new welcoming technologies like Big Data, Block Chain (BC), Edge Artificial Intelligence (Edge AI) etc to improve the vehicular quality of service [1]. The interconnection and commutation have become very intense, as the world steadily shrinks to the notion of achieving Global Village. Vehicle to Everything (V2X) is an effective communication system that enables data transfers from a vehicle to any other system, that may be related with vehicular traffic to assure safer travel at cheaper costs with better traffic management [2]. This is an initiative for installing a more robust and versatile on road infrastructure that streams voluminous quantity of useful data. The so obtained heterogeneous data can be leveraged to create ingenious but useful applications to aid mankind [7]. These applications many be inclined to focus on traffic management, congestion control, diagnostic systems, physical security devices, temperature-control sensors, enhanced communications systems, worker safety devices, mobile computing devices, product-tracking capabilities, or environmental aspects by harnessing pioneering technologies like Block chain, IoT, Artificial intelligence and cloud computing.

Deploying IoT in Vehicular Adhoc Networks (VANETs) is looked upon as a significant transition in building smart cities with intelligent vehicles [6]. Vehicular IoT is perceived as a wireless communicative hub that heads towards next generation networks. The VIoT follows the best practices of generic IoT with additional measures to combat the unique challenges like metal surfaces, signal congestion within confined space, change in radio frequency dynamics in adherence to the vehicle model, attenuation, external antennas etc. Besides these hurdles, the major provocation confronted by VIoT is the anticipation of Futureproofing that focuses on frequent updating of sensors, edge devices and Information and Communication Technology (ICT).

The recent trends in VIoT have facilitated the automotive with many sensors with enhanced communication to avoid traffic jams and even collisions. But the visibility of proximal vehicles are limited by factors such as low resolution and flawed camera, high dynamism, disruptive communication, network latency etc. This article focus on presenting a framework for vehicle collision avoidance system.

1.1 Types of Collision avoidance systems

The collision avoidance systems are divided into three types based on the source of information [4]:

- Type I: Obtain information from surroundings of the subject vehicle
- Type II: Obtain information from other vehicles
- Type III: Receive information from surrounding infrastructure

1.2 Working of Collision avoidance systems

There are four major types of collision avoidance systems available in the market. Fig 1 shows a sample collision avoidance system. Their functionality is described below:

- **Forward-collision Warning (FCW):** This system issues warning to the driver either through sound or light. This is a well proven system with high reliability.
- **Blind-spot Warning (BSW):** This system indicates the obstacles or other vehicles in the blindspot of the driver.
- **Cross Traffic Warning:** This issue an alert signal when the obstacle is out of the camera's range.
- **Lane Departure Warning (LDW)**: This issues light or sound signals when the driver is crossing the lanes.

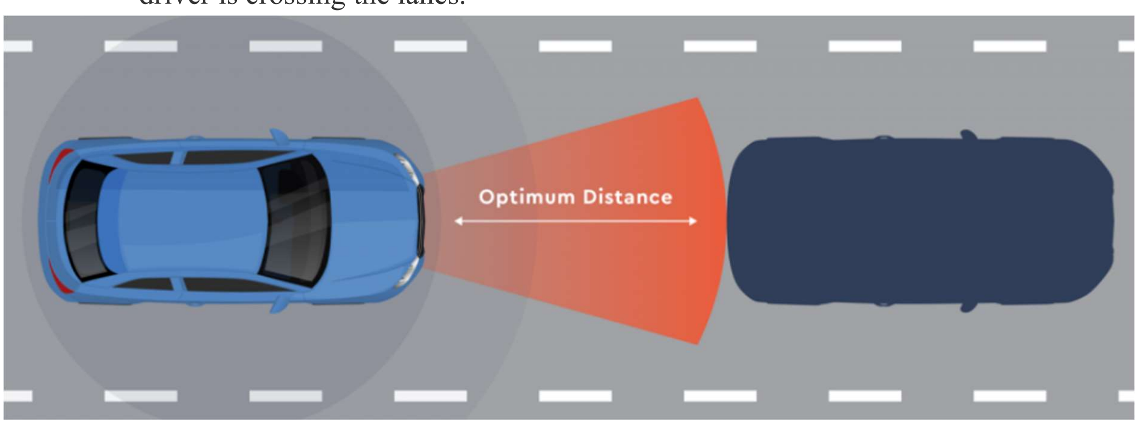

Fig 1: Collision Avoidance at optimum distance

Modern computing technologies like IoT, AL, ML and block chain can augment the efficacy of VIoT based collision avoidance systems. This work presents a novel, comprehensive framework that integrated IoT with Block Chain, a futuristic technology that acts as a system to store and evolve decentralized ledger information to avoid vehicle collision is presented in this article. This is an in-place data access mechanism, more commonly used in transactions of cryptocurrencies. The deployment of BCT is not limited within the scope of crypto currencies. The ability of block chains to maintain data integrity finds its applications in almost all domains. Data from the sensors or other elements of IoT are recorded as a transaction in a block along with a nuance or timestamp. These blocks are chained together by a hash algorithm. All the blocks are synchronized, thus the data available at all the parties are always valid [3].

1.3 Block Chain: A brief introduction

Blockchain or Distributed Ledger Technology (DLT) is sharable means of recording information such that the data entering in it is immutable. It can be perceived as a distributed, digital ledger that tracks transactions between the nodes that are connected. Every node is entitled to make a transaction into a data structure called block, which is apparently transparent to all the other nodes in the network. The privacy and integrity of the data is ensured by linking the blocks with immutable cryptographic hash algorithm. Thus, for an attacker to compromise the entire system, he must modify at least 51% of entries in the block chains that demands computation of hash function for every entry, which is highly impractical.

The essential properties of block chain are enumerated below:

- Distributed: All the parties possess a copy of the ledger with complete transparency
- Immutable: The records are irreversible. The entries cannot be changed
- Time-Stamped: The time of the transaction or event in a block is recorded.
- Unanimous: All the parties have to give consensus to each entry made in the block chain
- Anonymous: The identity of the parties is maintained as anonymous.
- Programmable: Block chains can be programmed to act in a specific manner in a specific contexts. These are called contracts.
- Secure: Every transaction is encrypted.

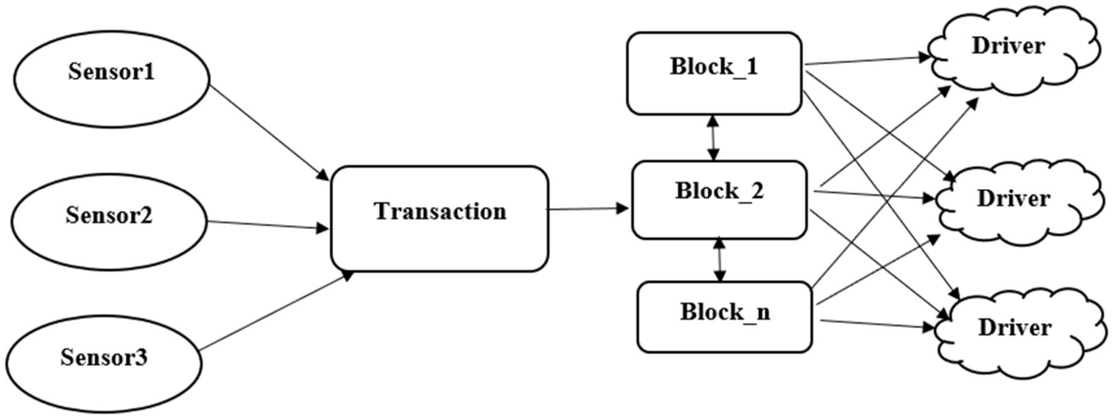

Fig 2: Formation of Vehicular Block chain

Block Chain technology finds its application in almost all areas where reliable data communication is the primal goal. Vehicular collision avoidance is one such area that demands handling and exchange of voluminous on road sensor data with high reliability in a confined location [5]. So, block chain technology dells in a natural solution to build more efficient and reliable vehicular collision avoidance by leveraging VIoT. Fig 2 shows the formation of Block chains of vehicular data that can be tapped to detect and avoid on road collisions.

2. LITERATURE SURVEY

The area of VANETs has tremendously changed the operation of logistics and goods movement. This is further enhanced by the development of BCT. Some of the prominent works are discussed here.

A comprehensive review was made by Abdul Rehman Javed et al., by exploring various capabilities and opportunities to use BCT in VIoT networks [8]. This work revitalizes the Smart Transport Infrastructure by harnessing advanced AI and ML techniques. This work delineates the challenges such as computation cost, communication bottlenecks, and other related privacy as potential research areas for further development in the domain. A novel spectral-efficient hybrid beamforming method is proposed by Bushra N. Alsunbuli et al. as an attempt to enhance the network connectivity as well as the performance. Multi-objective Squirrel search optimization is deployed at relay nodes of the vehicular network along with dynamic Shannon entropy-based Fuzzy VIKOR to improve the connectivity between the vehicles. The MATLAB simulation shows that the proposed model showed improved efficacy with low latency than other state of art methods.

The rationale of using BCT in building including Autonomous Electric, underwater, aerial and guided vehicles is studied by Saurabh Jain et al. [10]. A detailed comparative analysis of multiple BC based structures are isolated and investigated based on the sensors, architectures, infrastructure requirements, type of vehicle, driving modes, target tracking etc in the genres employing intelligent contracts, data handling, in industry-specific use cases. As a measure to impact security in Vehicular networks by limiting the third party requests only

a properly verifiable record will be permitted to communicate in the network [11]. This approach is observed to be resilient to attacks, which is determined used quantitative

experimentation. A trusted environment in BC especially in building a vehicular network is very important. Madhusudan Singh et al. proposed secure, and decentralized communication mechanism between vehicles without the need to share the personal information [12] through a local yet dynamic blockchain. This approach is powered by unique, secure crypto ID to ensures trustworthiness among vehicular nodes. In addition to this, the work used, LDB branching for efficient communication.
Vasiliy Elagin et al. studied telecommunications-based intelligent transport systems with special focus on safety and resilience [13]. As BCT is distributed, few acute issues like security and privacy preservation must be ensured in operation of transport networks through the usage of contemporary technologies which are discussed in this work. Another significant work by Chao Wang et al. enumerated and explained the potential applications of BCT in Vehicular IoT. The work reviews the prominent literature in data management, privacy protection and monetization of data in the perspective of vehicular network [14]. A detailed analysis of authentication, availability and accountability of BCT in building vehicular networks is done by Rajesh Gupta et al. [15]. This work also highlights the countermeasures that could be included in BC based framework to combat security issues.

A framework that uses fog cloud network to monitor vehicular networks at much minimized communication and computation cost is designed by Abdullah Lakhan et al. [16]. This follows a mobility aware offloading scheme with proof of work and creditability. A new reputation system with data credibility assessment is proposed by Zhe Yang et al. where the message reception rate is based on the traffic conditions [17]. A temporary central node is chosen from vehicles which is made responsible for broadcasting the reception rate to the connected blocks. A novel block chain framework for vehicular network communication with incentive, reputation and priority schemes is used in this work [18]. This model encompasses multiple types of nodes such as minor, controller, and ordinary node with specific values. Pradip Kumar Sharma et al. created a new model titled Block-VN which is accustomed to control the vehicular traffic using BCs in more secure, intelligent, autonomous and distributed transport system [19]. This work also discusses various scenarios along with new design principles destined for the proposed network.

3. BLOCK CHAIN BASED VEHICULAR COLLISION AVOIDANCE SYSTEM

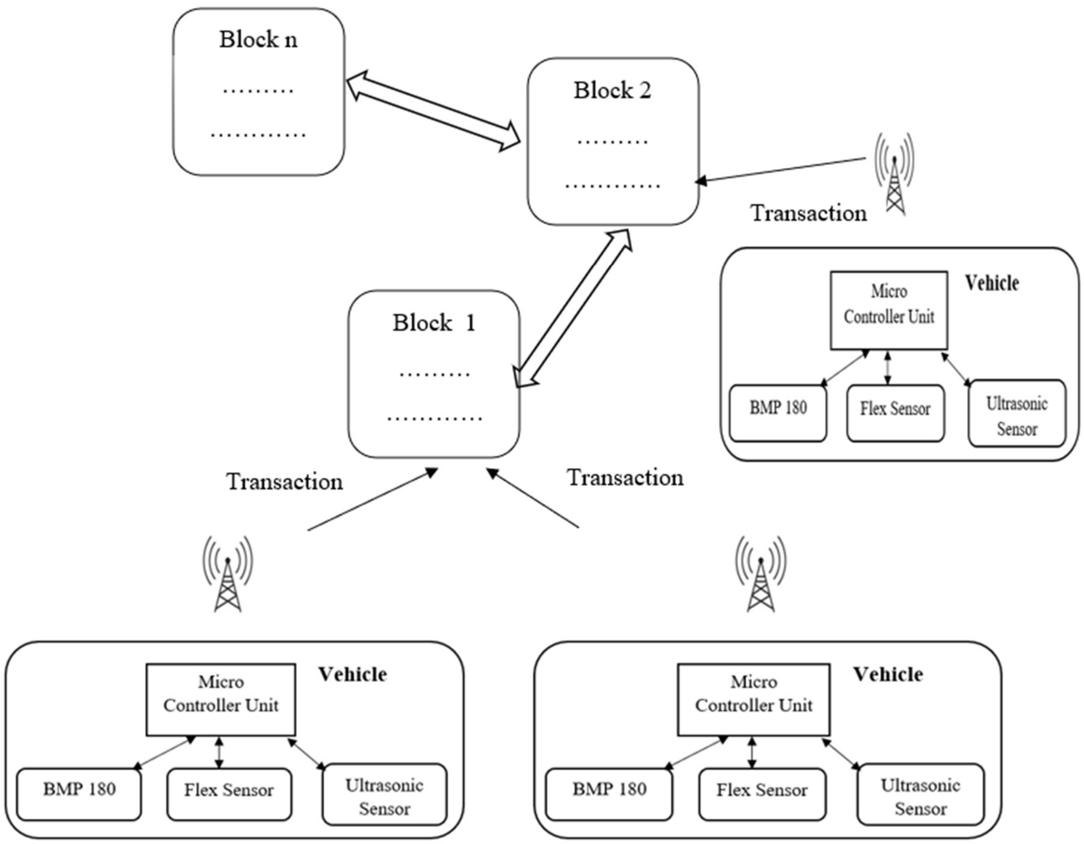

Fig 3: Block Chain framework for Vehicle Collision Avoidance

The proposed block chain-based collision avoidance system also acts as collision detection system and is shown in Fig 3. The vehicular nodes are embedded with the following sensors:

- BMP 180: This sensor monitors the physical quantities such as
    - ✓ Tire Pressure
    - ✓ Distance between vehicles
    - ✓ Tire temperature
- Flex sensor: The sensor measures the position of accelerator pads in vehicles
- Ultrasonic sensor: This sensor ensure that the vehicles move within safe distance limits

The VIoT emanates high volume of heterogenous sensor data that must be managed and handled efficiently to avoid collisions. The data from every node is entered as a transaction in a block. The proposed framework exploits the spatio-temporal existence of vehicles in a particular region. The generated data from the vehicles is semantic only for proximally placed Road Side Units (RSUs). Proof of Existence method, that finds the hash of the transaction and stored as a part of the transaction, is used for verifying the validity of the transactions entering into the blocks [20].

The sensor readings from the vehicles is authenticated using Proof of Existence and a fresh block for the transaction is created. The newly created block (validator) is send to all the other nodes in the VANET and the current transaction has to be validated by other nodes also. When the block is validated by every node, then it is chained to the existing block chain. Augmentation of a node inside the bock chain is communicated across vehicles in the network. This marks the end of the transaction in a block. All the vehicles are aware of every other vehicle's activity, hence collisions can be avoided. The creation of block chain initially, does not require any authentication or Proof of Work. As the vehicles on the road will be continuously mobile, the transactions will be initiated in regular time intervals. A typical transaction is shown in Fig 4.

Timestamp	Vehicle registration number	Tire Pressure	Distance between Vehicles	Tire temperature	Position of accelerator pads	Hash value

Fig 4: Tuples in a typical Transaction

The RSU's ensures confidentiality by generating public and private keys for communication between any two RSU's. Also, RSU's are responsible for maintaining the integrity of the vehicular transaction by digitally signing them with hash value. In the receiving end, the RSU's verifies the authenticity and integrity of the received message by checking the hash value. Then it decrypts the transaction received form other RSU.

Thus, the proposed framework enables every node on the road to analyse the driving pattern of other vehicles in proximity. When a node with an abnormal pattern transacts in the block chain network, then its behavior is propagated to all the other nodes, thus keeping the driver well informed about the situation.

4. PROOF OF EXISTENCE

PoE in this work is involved in recording as well as proving whether certain data about a vehicle exist in the network or not. This includes a timestamp associated with a signature to verify and prove that only the authorized users or vehicles are created. The vehicle's registration number is the unique identifier to track the existence of a vehicle in the network. Also, its speed, pace and other entities are measured to alert the other nodes in the network. A hash value must be verified by atleast 50% of the nodes in the BC networks, as a measure of validating the nodes. Only the verified nodes can enter the BC network, which concludes the proof of existence and the entire process in shown in Fig 5.

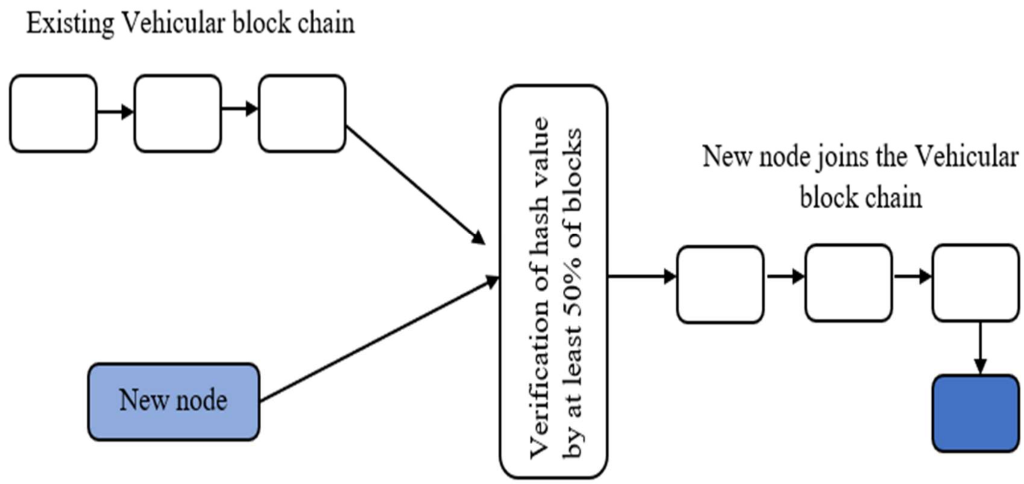

Fig 5: A new node joining the existing vehicular network

4. ADVANTAGES OF BLOCK CHAIN BASED COLLISION AVOIDANCE SYSTEM

The proposed block chain-based collision avoidance systems provides the following advantages in managing intelligent and automated vehicles on road:

- **Avoids obstacles:** The ultrasonic sensors embedded in every vehicle effectively traces the presence of obstacles in the driving lane. This can be intimated to the driver by interfacing a communication module in the framework. Also, since the data about the obstacle is also a part of the transaction, all the vehicles connected to the network will be aware about the obstacle.
- **Avoids faulty data:** Since any data entered into the block chain must be validated by all other nodes, the chances of faulty or compromised data becoming a part of block chain are very merger.
- **Avoids redundancy:** The block chains ensure that every data is unique. Hence there is no duplication of data, which mitigates the size of block chain.
- **Authoritative data access:** The RSU's are responsible for authenticating the transactions flowing through it. This imparts authoritative data access in block chain-based collision avoidance system.
- **Traceability of events:** All the transactions are entered as blocks. Hence it is easy to trace the behavior of every node.
- **Heterogeneous sensors:** The VIoT nodes are built with multiple heterogenous sensors that can effectively track individual vehicles route course apart from monitoring the data traffic.
- **Offloading the computation:** The RSU's of the proposed framework is concerned with providing confidentiality and integrity of transactions. This avoids unnecessary computations at the nodes.

5. DESIGN CHALLENGES

The proposed framework of block-chain based collision avoidance system is an attractive option for implementing a decentralized collision avoidance system with the feasibility of deploying it in legacy frameworks. There are some design challenges, which are actually blessing in disguise. They emanate as future research directions:

- As a greater number of nodes join the network, the computations become harder.
- Verifying and validating the transaction in spatio-temporal genre imposes high workload on the RSUs.
- Fault tolerant sensors are quintessential for the efficient implementation of the system.
- Improper selection of consensus mechanism can deteriorate the overall performance of the system
- The overall time complexity of the system is dependent on the tuple size
- The communication network and infrastructure should be compatible to the block chain technology.

6. CONCLUSION

This article proposes a novel framework for block-chain based collision avoidance system, which is decentralized and deployable on existing VANET infrastructure. This framework leverages VIoT technology in vehicles to detect possible collisions by measuring the tire temperature, pressure and obstacles in path which is stored as transactions in block chains periodically. The inherent security mechanisms of block chain increases the reliability of the system at much reduced computational costs. The RSU's combinedly work to build a consistent database that is transparent to all the nodes in the network. Thus the proposed framework can open a new era in automated vehicles, which is the hot trend in the automobile industry.

REFERENCES

[1]	Contreras-Castillo, J., Zeadally, S., & Ibañez, J. A. G. (2016). Solving vehicular ad hoc network challenges with big data solutions. *IET Networks*, *5*(4), 81-84.
[2]	Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. *IEEE internet of things journal*, *1*(4), 289-299.
[3]	Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access*, *8*, 18207-18218.
[4]	Takatori, Y., & Hasegawa, T. (2006). Stand-alone collision warning systems based on information from on-board sensors: Evaluating performance relative to system penetration rate. *IATSS research*, *30*(2), 39-47.
[5]	Kim, S., Lee, S., Yoon, I., Yoon, M., & Kim, D. H. (2011, May). The vehicle collision warning system based on gps. In *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering* (pp. 263-264).
[6]	Sharanya, S., & Karthikeyan, S. (2006). Classifying malicious nodes in VANETs using support vector machines with modified fading memory.

[7]	NandigalaVenkatAnurag, Y., & Sharanya, S. (2021). Air Quality Index Prediction with Meteorological Data Using Feature Based Weighted Xgboost.
[8]	Javed, A. R., Hassan, M. A., Shahzad, F., Ahmed, W., Singh, S., Baker, T., & Gadekallu, T. R. (2022). Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors*, *22*(12), 4394.
[9]	Alsunbuli, B. N., Fakhruldeen, H. F., Ismail, W., & Mahyuddin, N. M. (2022). Hybrid beamforming with relay and dual-base stations blockage mitigation in millimetre-wave 5G communication applied in (VIOT). *Computers and Electrical Engineering*, *100*, 107953.
[10]	Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and autonomous vehicles: Recent advances and future directions. *IEEE Access*, *9*, 130264-130328.
[11]	Smys, S., & Wang, H. (2021). Security enhancement in smart vehicle using blockchain-based architectural framework. *Journal of Artificial Intelligence*, *3*(02), 90-100.
[12]	Singh, M., & Kim, S. (2018). Branch based blockchain technology in intelligent vehicle. *Computer Networks*, *145*, 219-231.
[13]	Elagin, V., Spirkina, A., Buinevich, M. and Vladyko, A., 2020. Technological aspects of blockchain application for vehicle-to-network. *Information*, *11*(10), p.465.
[14]	Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: applications of blockchain in the internet of vehicles. *EURASIP Journal on wireless communications and networking*, *2021*, 1-16.
[15]	Gupta, R., Tanwar, S., Kumar, N., & Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering*, *86*, 106717.
[16]	Lakhan, A., Ahmad, M., Bilal, M., Jolfaei, A. and Mehmood, R.M., 2021. Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), pp.4212-4223.
[17]	Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017, October). 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)* (pp. 1-5). IEEE.

[18]	Arshad, U., Shah, M. A., & Javaid, N. (2021). Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture. *Vehicular Communications*, *31*, 100386.
[19]	Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of information processing systems*, *13*(1), 184-195.
[20]	M. S. Amin, M. A. S. Bhuiyan, M. B. I. Reaz, and S. S. Nasir, (2013).GPS and Map matching based vehicle accident detection system. *2013 IEEE Student Conference on Research and Development*, Putrajaya, 2013, pp. 520- 523.