SecVT: Securing the Vehicles of Tomorrow using Blockchain Technology

Amit Kumar Tyagi [0000-0003-2657-8700]

School of Computer Science and Engineering, Vellore Institute of Technology, Chennai
Corresponding author: amitkrtyagi025@gmail.com

Abstract. Internet of Things (IoT) is one of the fields which has flourished to a great extend over the years because of its varied use cases and versatility. One of the fields which has flourished technologically is the automotive industry where the main focus is not just on improvising the vehicles internally but also to develop communication and interaction between vehicles on the road so as to facilitate a network of interconnected vehicles. However, the exchange of large volumes of data often poses a huge threat to security and privacy and necessitates the incorporation and integration of intense cybersecurity measures to ensure that the system and network is safe from attacks. Blockchain however has proven to be one of the useful techniques in terms of protecting data This chapter mainly deals with the implementation of securing the information regarding next generation intelligent vehicles.

Keywords. Internet of Things (IoTs), Automotive, Communication, Cyber-Security, Blockchain, Next Generation Vehicles.

1 Introduction - Future Vehicles

The development in the transportation and automobile industry has been massive in the recent years. It has acquired new standards with the help of global enhancements and technological growth. This mainly covers concepts such as autonomous vehicles, smart cars, hybrid vehicles, vehicular networks, etc. Computer vision, image processing, sensors, and network-based algorithms are the major arenas that have contributed for such developments [1].

a) Hybrid Intelligent Vehicles and Connected Vehicles

Connected Automated Vehicles (CAV) are the ones that are instrumented with techniques like vehicle-to-vehicle or vehicle-to-internet networks [2]. They mainly consist of sensory networks to detecting trajectories and objects along with the feature of establishing interconnections with other vehicles. This is extremely useful for traffic forecast, predicting motion in surrounding environment, and to increase the accuracy of such information obtained [3,4]. This is the foundational logic of cyber physical systems which utilize physical apparent parameters for controls through interaction and forecasting strategies. The supervision and control of CAV's are done at numerous junctions, freeways, service roads, interjunctions, etc. This definitely helps in improving the efficiency, performance, etc. while also reducing the pollution and fuel consumption [5].

b) Autonomous Vehicles

A step further from the conventional vehicles leads to Autonomous Vehicles (Avs) and is capable of manoeuvring and navigating roads in driverless conditions. This mainly helps in reducing the possibility of human errors, decreases accidents, etc. Many companies and organizations, including tech giants, have invested on AVs so as to reduce the stress and tension caused by driving. However, there's also a sceptical notion about the possibility of such AVs completely losing control on road and causing mishaps [7].

c) Autonomous Intelligent Vehicles (AIV)

Autonomous intelligent vehicles which are intelligent and automated and take action instantly over the road network to avoid any type of accidents or improve the transportation journey. These types of vehicles use Machine Learning, Deep learning, etc., techniques to improve its communication. In near future, AIV will use few emerging technologies like blockchain, edge computing, digital twin, etc., to improve its basic features. Few objectives, scope, etc., of Autonomous Intelligent Vehicles can be discussed in [27]. The possibility of developing a vehicle which is completely automated is highly likely provided it has access to information such the current environment, the route to take, and driving decisions. Robocars or robotaxis are smart vehicles that make use of a combination of sensors, processors, etc. to depict control and supervision over the driving abilities. Vehicles that are integrated with such innovative technologies also have certain unique points of interest. The ultimate aim of such vehicles is to limit accidents and energy consumption while reducing discharges. The key factors that influence such vehicles decisions include:Perception

a) Motion Preparation - (direction) steering, pace
b) Navigating
c) Behaviour- study of lanes, overtaking

The points mentioned above are targets for real-world users of autonomous vehicles. Now, possible uses of Future Vehicles in near future are (also refer figure 2):

- e-healthcare

Smart and autonomous vehicles are particularly useful in the health sector. In cases of accidents and emergencies, such vehicles can reduce latencies and reach the desired destination with ease in case of unavailability of drivers. Many a times, people affected by accidents are exposed to further critical conditions because of the lack of sufficient care and health support at the right time. Ambulance getting delayed due to heavy traffic, lack of coordination among drivers and hospitals, etc. also contribute to the above-mentioned cause. The fact the smart vehicles can predict traffic, road scenarios, and engage in interconnection networks, are highly efficient to ensure a safe and sound health support being recruited to the patients within very less time. The mini versions of CAV robots are also utilized for hospital sectors to deliver surgical and medical equipment which are required for surgeries, operations, etc. [8].

- Supply chain

The process of supply chain is pretty lengthy which starts with extraction and retrieval of raw materials all the way to delivering the products to consumers. The initial

stages very often include the transportation of resources such as iron, metal, wood, etc. along with commuting the final goods. This aspect is extremely crucial in supply chains and it's highly important to ensure that the goods are delivered to the customers at the right time, specifically in the food industry. Delays and latencies can often lead to spoilage of food and its wastage. The presence of different sensors in CAVs can make sure that the quality of food is maintained by controlling the ambient temperature and adjusting it as required [9]. This would also motivate consumers to order such products in reduced quantities which in turn decreases the stocks in inventory, benefiting both the employers and customers.

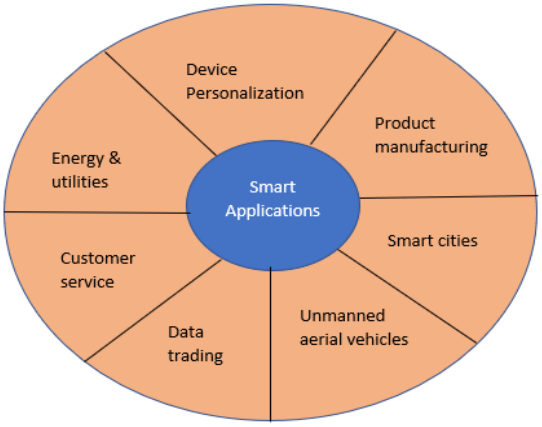

Figure 2: Smart Applications in Current Scenarios

The detailed description about progress/ evolution of connected vehicles (2000 onwards) can be found in [26].

1.1 Blockchain/ Distributed Ledger Technology:

The infamous decentralized and distributed ledger technology [25, 28, 30] called Blockchain is being heavily used across various application aspects, which is immutable and is used for storing information in block like structures which are encrypted. The possibility of using Blockchain in various disciplines is highly probable in the near future. There are a number of parameters that make Blockchain systems unique and distinctive. Few of the pertinent characteristics are as follows:

- Private, Public, and Permission Blockchain.
- Centralization and Decentralization
- Persistency
- Validity
- Anonymity and Identity
- Immutability

Other application of blockchain in this current smart era can be found in [14, 29]. Apart from this, the main advantages of Blockchain are as follows:

- Enhanced transparency and flexibility of shipment procedures
- Development in reliability and loyalty with recorded logs of transactions

- Increased levels of precision and accuracy to combat with IoT
- Users can integrate this to enhance business using IoT applications

With the help of Blockchain technology, it is possible to generate high levels of security and satisfactory levels of trust pertaining to the data stored in the distributed and centralized database.

1.2 Organisation of this work

Note that in this work, Future Vehicles or Vehicles of Tomorrow or Autonomous vehicles, etc., terms have been used interchangeably (all terms have the similar meaning).

2. Role of Internet of Things in Future Vehicles

IoT is all about the interconnection of devices and gadgets that operate via the internet and is often used in the transportation sector. Intelligent transportation systems basically include a smarter and intelligent way of controlling the automobile sector in fields of traffic and signal management, accident control, road safety, etc. The growing number of vehicles have posed sufficient number of challenges to the people and government from the viewpoint of increasing fuel consumption, pollution and traffic jams. Just like how IoT was easily compatible with various other industries, its integration with the automobile industry would lead to rapid advancements and developments. With the help of IoT, a number of features such ass connectivity, cloud services, smart sensors, etc. could be added which in turn betters the performance and quality control. This powerful combination would lead to an organic interaction between people, roads, and vehicles and can provide a great solution to traffic issues and pollution [10].

3. Motivation

IoT allows for a quicker and safer exposure for pedestrians and drivers because they get sufficient information on road condition, traffic details, performance of vehicles, and energy consumption. However, with increasing usages of IoT for modernizing the vehicular sector, there's an increase in malicious attacks and data breaches. The umbrella term of Internet of Vehicles (IoV), often termed as the future of vehicles, is consolidated with V2V networks and various sensors for information and data gathering. In case of an event where any one of the components fail, it can result in the failure of the whole system [11]. This is a huge vulnerability and when considered along with the lack of succinct privacy techniques to preserve data securely is addressed with the help of Blockchain technology. Protection and preserving privacy of databases and devices in IoT and related applications is one of the areas that is incorporated with this technology [12]. This paper discusses the possible strategies and uses of safe and secure decentralized blockchain environment. We also discuss the challenges in current vehicles and how smart and secure hybrid vehicles can help to solve these issues.

4. Issues, Constraints, Challenges with Current Vehicles

In the Vehicular Adhoc network VANET context [23, 24, 25 and 26] or current vehicles, we can distinguish several problems/ issues:

- Key agreement vs. key transport: Because VANET groups are scattered, key agreement is the most common method for establishing a new key. Each approach requires that all players broadcast numerous rounds of information in succession. While this method can be terminated in one round, it places most of the computational burden on the group leader, which is also a single point of failure, key transport involves allowing a group leader, either chosen by the specific application or chosen at random, to create and broadcast a group key to all members.
- Join/Leave operations: Group membership is subject to rapid change in VANETs. As a result, the effective administration of new members' join and exit procedures is an additional problem in safe group management. Existing keys may be transferred to a new member using simple methods such as key transport, but new keys must be computed and redistributed whenever a member leaves the system. A portion of keys may need to be re-computed for both actions in protocols based on key trees; although this adds complexity, it spreads the computation work better than simple key transfer. Because most VANET cars will have comparable degrees of security, the development of secure groups will simply help reduce security overhead, rather than establishing distinct levels of security across VANET members. This is critical to remember. The usage of secure groups, like digital signatures, secures the network from outsiders, not insiders as stated, just like digital signatures. This means that although it is still essential to renew or transfer current keys when new members join, the group key should not be updated automatically when a member quits.
- Definition of group memberships: The VANET mobility concept, as previously indicated, is very dynamic. Even while some cars may travel close to one other for many kilometres at a time, others may rapidly overtake them or join the self-formed groups they have created. Group boundaries are exceedingly difficult to establish in these situations. Some members of the platoon may be unaware of a new vehicle joining from behind if the platoon is dispersed across multiple wireless hops. It will be time- and message-consuming and inefficient to perform group rekeying based on tree recomputation and rebalancing or key agreement. Keys might be transferred from the new member's next-door neighbour as a straightforward solution in this instance. But if a group's borders aren't clearly defined, cars that aren't part of the group may be caught up in a critical establishing effort. Additionally, even though these cars lack the group key, they are still required to receive safety warnings, necessitating the continual use of broadcasts with digital signatures. Group borders may be preloaded into vehicles in order to reduce the issue of changing group boundaries. Groups may be constructed based on cell membership, for example, by dividing highways into geographic cells.
- Others: Many attacks like Denial of Service, Distributed Denial of Service (DDoS), Man in Middle Attacks, timing attacks, transition attacks, etc., are mitigate over VANET/ current vehicles in Today’s scenarios.

5. Proposed System Model - Securing Future Vehicles

To proceed further for proposed work, first we need to explain the problem raised in the recent decade with vehicles or autonomous vehicles.

Problem Definition: One of the various crucial aspects is the leakage of a user's personal data [24-28]. Similarly, preserving the privacy of consumers and building their trust with respect to the service provider can be very tedious in the modern era.

Algorithm 1: Data Encryption

1: **function** ENCRYPTION (data_ file)
2: **if** user confirm data preservation over blockchain **then**
3: Generate a symmetric key ksym
4: C ←Encrypts (data_ file, ksym)
5: Ck ← Encrypts (ksym, rkpub)
6: **else**
7: Do nothing
8: **end if**
9: end function

Algorithm 2: Ring Signature and Public key sharing

1: **function** SIGNATURE (data_ file)
2: **if** user chose anonymity over blockchain **then**
3: Generate an asymmetric public-private key pair sks pub, skspriv
4: hash p← calculate hash of the data_ file
5: Create the **Digital Signature** using hash p and signers private key skspriv
6: Share the public key skspub to the receiver using **Diffie–Hellman key exchange**
7: Mix the signature with another network group to form a ring
8: **end if**
9: end function

Algorithm 3: Data Decryption

1: **Input:** Encrypted file C, Encrypted symmetric key (Ck)
2: **Output:** Decrypted data_ file
3: **function** DECRYPTION (C, Ck, rkpriv, ksym)
4: ksym ←Decryptasym (Ck, rkpriv)
5: data_ file ←Decryptsym (C, ksym)
6: end function

Algorithm 4: Signature Verification

1: **Input:** Encrypted file C, Signers Public key (skspub)
2: **function** VERIFICATION (C, skspub)
3: hashc ← calculate hash of the received encrypted data file C to be verified
4: Using Public key skspub of signer, extract hashp of senders file
5: **if** hashc = hashp**then**
6: return C
7: **else**
8: return "Signature incorrect"
9: **end if**
10: end function

Block.java | Blockchain.java

Source | History

```
1  package blockchain;
2  import java.util.*;
3  import java.text.*;
4  public class Blockchain {
5      ArrayList<Block> blockchain = new ArrayList<>();
6      public static void main(String[] args) {
7          String[] genesisTransaction = {"Meghna1", "Harika1"};
8          Block genesisBlock = new Block(0, genesisTransaction);
9          System.out.println("Hash of Block 1:");
10         System.out.println(genesisBlock.getBlockHash());
11         //digitial signature of the block created
12
13         String[] block2Transaction = {"Meghna2", "Harika2"};
14         Block block2 = new Block(genesisBlock.getBlockHash(), block2Transaction);
15         System.out.println("Hash of Block 2:");
16         System.out.println(block2.getBlockHash());
17
18         String[] block3Transaction = {"Meghna31", "Harika3"};
19         Block block3 = new Block(block2.getBlockHash(), block2Transaction);
20         System.out.println("Hash of Block 3:");
21         System.out.println(block3.getBlockHash());
22
23     }
24 }
```

Fig. 3 Java code for creating a Blockchain

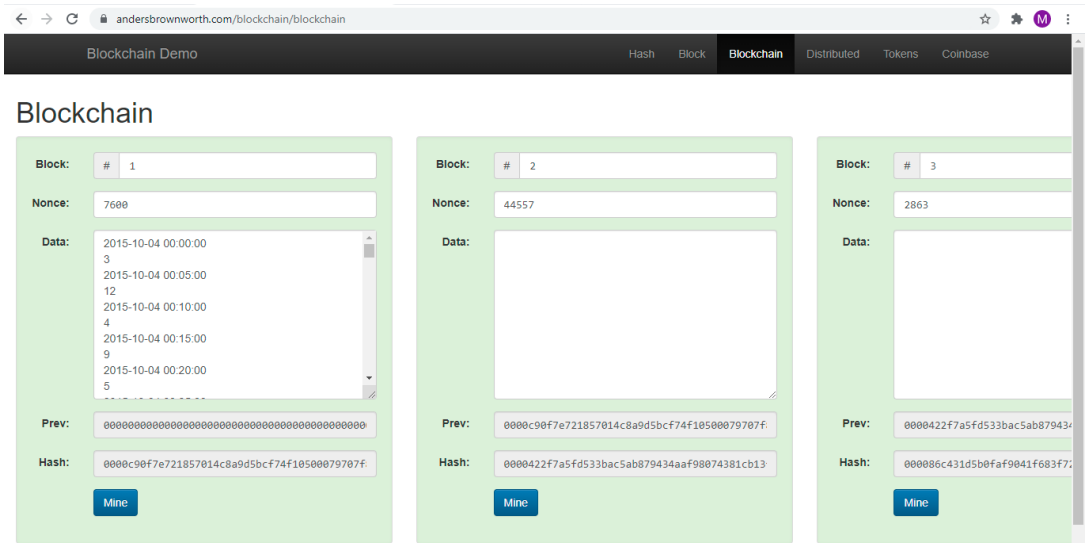

Fig. 4 Simulation of Blockchain after mining all the blocks

Solution: We used following algorithms to secure our vehicles over the road network. Which can be explained as:

- Algorithms 1: This algorithm is used to encrypt the communicated data (over the road network) by the sender side.
- Algorithms 2: This algorithm uses Ring signature and public key sharing among users/ drivers (over the road network) to encrypted and share the data.
- Algorithms 3: This algorithm is used to decrypt the communicated data (over the road network) by the receiver side.
- Algorithms 4: This algorithm is used to verify signature or shared keys or validate user to access the services (provided by vehicles).

Figure 3 and Figures 4 show the creation of Blocks, and Blockchain which are written in Java language.

6. An Open Discussion on Internet of Things (IoT) – Machine Learning based Autonomous Vehicles (AV)

Consistent supervision of data from various interconnected Avs and AIVs along with the strategy to compute suitable routes and paths based on environmental factors is what contributed towards the success and evolution of smart vehicles. Incorporating AI with such vehicles led to various patterns which are constantly evolving and they contribute towards identifying a route that smoothen the travel experience. When the AI determines that traffic patterns (using machine learning) are changing, it can even change the course of a journey if necessary. Few other comparisons are summarized here as:

a) Current Vehicles vs Future Vehicles
b) Autonomous Vehicles Vs Autonomous Intelligent Vehicles

In [13, 27], details about Intelligent Vehicles, connected vehicles, Hybrid Vehicles and Autonomous Intelligent Vehicles and raised issues in it have been explained. The majority of previous research on sensory network coverage have been theoretical. Deeper analysis might concentrate on solutions that can be implemented more quickly in the real world. The following is a list of other research issues. These distributed self-organizing networks have three major challenges: high node mobility [25, 26], system scalability constraints, and a wide variety of environmental factors. Automobiles travelling at high speeds in varied situations, such as on highways, provide a unique challenge. The bulk of iterative algorithms meant to optimise channel bandwidth or predefined paths interact with these properties. VANET security and privacy must be managed [27, 28]. The user's privacy concerns may collide with the recipient's desire to know the source of the information. Virtual area networks (VANs) face unique challenges when trying to establish reliable wireless connection

7. Related Work

As discussed in [26, 27], for a wireless network to function, several general security requirements must be taken into account. These include authenticity, scalability, privacy and anonymity; as well as cooperation, stability, and low communication delay. With respect to this may researchers/ scientist have made serious attempts to secure/

preserve privacy of vehicles/ such transportation system in the previous decades. Which can be summarized here as:

In the case of vehicular ad-hoc networks, the authors of [15] and [16] have worked on a seven-layered secure and reliable technique that utilizes blockchain based Vehicular Adhoc Network (VANETs) system. For applications that relate to gathering vehicular data, car taxes, etc. a combination of Ethereum and blockchain related smart contracts are used. The use of the technology was further enlarged to consist of peer-based interactions and intra-vehicle communication facilities. Furthermore, the author of [17] has put forth a technique using blockchain that is capable of updating the information of the vehicle wirelessly while preserving the details of the vehicle and its users. In [18], the authors have elucidated the use of blockchain via acoustic side channels along with vision empowered light so as to preserve data during intravehicular interactions. The implementation was carried out using a public key for the blockchain, a new key for cryptographic encryption, and a leverage mechanism for both the side-channels. On the other hand, the authors of [19] proposed an idea that utilizes distributed clustering to control the energy demands of IoV which is powered through blockchain facilities. The results obtained saves around 40% of energy and 82% of the transaction numbers needed. In [20], the authors have described the concept of blockchain and have focused on the architectural aspect of the selection process involved in choosing a gas filling station for an autonomous vehicle. The author has emphasized on the different security problems and concerns which prevail due to the existence of data that is transmitted between vehicles.

In [21], the proposal of a blockchain system to validate and verify consent between entities was highlighted. They've given details of using a multi-agent vehicle for communication and have elucidated how the communication can be secured in such cases. Furthermore, the authors of [22] have executed blockchain systems in unmanned aerial vehicles wherein, each vehicle is considered to be an individual node and the controlling mechanism is done by blockchain. Very recently, the authors of [23] had deployed the blockchain concept in terms of transferring data pertaining to traffic jams and scenarios which are transmitted to vehicles in a tamper proof way. The data is gathered through proof-of-event consensus and warnings are initiated through two-phase transaction strategies.

In the last, many other mechanisms like swing and swap, path confusion, l-diversity, encryption-based method, mix zone, etc., have been used in previous decades to preserve the privacy of users during accessing location-based services (LBSs).

8. Conclusion

This paper elaborates on IoT based Blockchain technique which ultimately records and keeps a track of all activities and transactions of users based on their interaction and connections with other nodes/users in the network. Smart contracts are used to help record the transactions and user activities consistently and frequent updates and upgrades of these records are augmented with IoT fragments to escalate the trade invested

on the same which is linked with Blockchain systems. User convenience and user efficiency are major issue in transportation sector/ future vehicles.

References

[1] C. Bila, F. Sivrikaya, M. A. Khan and S. Albayrak, "Vehicles of the Future: A Survey of Research on Safety Issues," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 5, pp. 1046-1065, May 2017, doi: 10.1109/TITS.2016.2600300.

[2] Chen, Keji, et al. "A hierarchical hybrid system of integrated longitudinal and lateral control for intelligent vehicles." *ISA transactions* 106 (2020): 200-212.

[3]] Piao J, McDonald M. Advanced driver assistance systems from autonomous to cooperative approach. Transp Rev 2008;28:659–84.

[4] Sebastian A, Tang M, Feng Y, Looi M. Multi-vehicles interaction graph model for cooperative collision warning system. In: Intelligent vehicles symposium. IEEE; 2009, p. 929–35.

[5] Malikopoulos, Andreas A., Christos G. Cassandras, and Yue J. Zhang. "A decentralized energy-optimal control framework for connected automated vehicles at signal-free intersections." *Automatica* 93 (2018): 244-256.

[6] Haboucha, Chana J., Robert Ishaq, and Yoram Shiftan. "User preferences regarding autonomous vehicles." *Transportation Research Part C: Emerging Technologies* 78 (2017): 37-49.

[7] Pedan, Marko, Milan Gregor, and Dariusz Plinta. "Implementation of automated guided vehicle system in healthcare facility." *Procedia engineering* 192 (2017): 665-670.

[8] M. Gregor, M. Pedan, L. Mizeráková, "SMART" zdravotnícke zariadenia - využitie moderných technológií v zdravotníctve, in: ProIN : dvojmesačník CEIT, ISSN 1339-2271, vol. 16, no. 5-6 (2015), pp. 21-24

[9] Heard, Brent R., et al. "Sustainability implications of connected and autonomous vehicles for the food supply chain." *Resources, conservation and recycling* 128 (2018): 22-24.

[10] Juan Antonio Guerrero-ibanez, Sherali Zeadally and Juan Contreras Castillo. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wireless Communications, Vol. 22, No. 6, 2015, pp.122-128.

[11] N. Sharma, N. Chauhan and N. Chand, "Security challenges in Internet of Vehicles (IoV) environment," *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 203-207, doi: 10.1109/ICSCCC.2018.8703272.

[12] Kim, S. (2018). Blockchain for a trust network among intelligent vehicles. In *Advances in Computers* (Vol. 111, pp. 43-68). Elsevier.

[13] Honnery, Damon & Moriarty, Patrick. (2004). Future vehicles: An introduction. International Journal of Vehicle Design. 35. 1-8. 10.1504/IJVD.2004.004048.

[14] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[15] Y. Yuan, F.-Y. Wang, Towards blockchain-based intelligent transportation systems, 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2016 Nov.1-4.

[16] B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16), ACM, New York, NY, USA, 2016, pp. 137–140

[17] A. Dorri, M. Steger, S.S.. Kanhere, R. Jurdak, "Blockchain: a distributed solution to automotive security and privacy," eprint arXiv:1704.00073, March 2017.

[18] S. Rowan, M. Clear, M. Huggard, C.M. Goldrick, “Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channel,” eprint arXiv:1704.02553, 2017. http://arxiv.org/abs/1704.02553.
[19] Sharma, V. An Energy-Efficient Transaction Model for the Blockchain-Enabled Internet of Vehicles (IoV). *IEEE Commun. Lett.* **2019**, *23*, 246–249.
[20] Pustišek, M.; Kos, A.; Sedlar, U. Blockchain based autonomous selection of electric vehicle charging station. In Proceedings of the 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), Beijing, China, 20–21 October 2016.
[21] Buzachis, A.; Celesti, A.; Galletta, A.; Fazio, M.; Villari, M. A secure and dependable multi-agent autonomous intersection management (MA-AIM) system leveraging blockchain facilities. In Proceedings of the 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), Zurich, Switzerland, 17–20 December 2018.
[22] Kuzmin, A.; Znak, E. Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles. In Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July–2 August 2018.
[23] Yang, H.-K.; Cha, H.-J.; Song, Y.-J. Secure Identifier Management Based on Blockchain Technology in NDN Environment. *IEEE Access* **2019**, *7*, 6262–6268.
[24] A. M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.332.
[25] Amit Kumar Tyagi, N.Sreenath “Vehicular Ad Hoc Networks: New Challenges in Carpooling and Parking Services”, in proceeding of International Conference on Computational Intelligence and Communication (CIC), Volume 14. International Journal of Computer Science and Information Security (IJCSIS), Pondicherry, India, pp. 13-24.
[26] R, Varsha et al. ‘Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles’. International Journal of Hybrid Intelligent System, Vol 16, Issue 4: 223 – 236, 1 Jan. 2020.
[27] Amit Kumar Tyagi, S U Aswathy, Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks, Volume 2, 2021, Pages 83-102, ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.
[28] Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56
[29] Shabnam Kumari, Amit Kumar Tyagi, Aswathy S U, “The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges”, in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.
[30] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.