Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2021)
Vol.03/ No.02
Pages: 93-106
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2021.2.003

Blockchain Framework for Communication between Vehicle through IoT Devices and Sensors

Jennifer S. Raj
Professor, Department of ECE, Gnanamani College of Technology, Namakkal, India
E-mail: jennifer.raj@gmail.com

Abstract

The advent of autonomous vehicles is indeed a potential field of research in today's situation. Connected Vehicles (CV) have received a lot of attention in the last decade, which has resulted in CV as a Service (CVaaS). With the advent of taxi services, there is a need for or demand for robust, seamless, and secure information transmission between the vehicles connected to a vehicular network. Thus, the concept of vehicular networking is transformed into novel concept of autonomous and connected vehicles. These autonomous vehicles will serve as a better experience by providing instant information from the vehicles via congestion reduction. The significant drawback faced by the invention of autonomous vehicles is the malicious floor of intruders, who tend to mislead the communication between the vehicles resulting in the compromised smart devices. To address these concerns, the best methodology that will protect and secure the control system of the autonomous vehicle in real time is blockchain. This research work proposes a blockchain framework in order to address the security challenges in autonomous vehicles. This research work enhances the security of smart vehicles thereby preventing intruders from accessing the vehicular network. To validate the suggested technique, money security criteria such as changing stored user ratings, probabilistic authentication scenarios, smart device compromise, and bogus user requests were employed. The observed findings have been documented and analysed, revealing an 82% success rate.

Keywords: Performance, ensemble, deep learning, sentiment analysis, machine learning

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

1. Introduction

Recently the manufacturing of vehicles has become a challenging task to mechanical engineering, and computer professionals, primarily due to the combination of communication and information technology with automobiles dynamically transforming the age-old vehicles into smart vehicles known as autonomous vehicles [1]. These self-driving cars are equipped with artificial intelligence, which allows them to interact with other vehicles, make dynamic and adaptive judgments, and cruise without a driver. Despite the numerous appealing characteristics of these vehicles, the major difficulties with deploying these autonomous vehicles rely on secure connectivity [2]. Furthermore, the increased production of automobiles has resulted in a variety of difficulties such as road safety, transportation infrastructure, fuel consumption, parking space, and so on. The event is largely composed of a collection of moving and stationary e cars that are wirelessly linked together. In the beginning, it was introduced to ensure safety and comfort to the drivers operating in vehicular environment [3]. With progress in technology, this has changed towards intelligent transportation systems, where autonomous vehicles communicate and connect with the aid of smart devices. This has led to a higher success rate in the creation of Connected and Autonomous Electric Vehicles (CAEVs) [4].

The use of internet by vehicles to share information in the form of localization, sensory and risk data is commonly called as Connected Autonomous Vehicles (CAVs) or internet of vehicles (IoV). This technology is considered to be a crucial application of VANETs, enabling them to become smarter with more control units, adapters and sensors to communicate with the other devices in the network and also to monitor the activities of a vehicle [5]. One of the biggest expansions of CAV applications is that of online cab booking services. This has significantly expanded the use of CAV for better vehicle entertainment experiences. Ride sharing and online cab facilities have dramatically revolutionized public transportation industry, making them widely popular among users [6]. Main use of online cabs also reduces the overhead of money negotiation between the customer and the driver, giving the customer the ability to tractor ride using GPS. In this paper we have proposed enhancement of security in the CAV network using blockchain technique [7]. The IoT device stores the vehicle ratings (previous and current), the vehicle number, and vehicle location when moving from one place to another. The blockchain network saves all the information stored by the IoT devices [8]. This way, in case of a breach in security, the vehicle owner can determine the information registered for that particular IoT device.

2. Related Work

The authors in [9] examined the blockchain methodologies using electric vehicle charging stations. In this paper, a number of prototype implementation using blockchain has been analysed. Due to data flow and exposure of information, between vehicle to vehicle interceptions there is a high security concern. Similarly, authors in [10] have also used blockchain framework for facilitating, negotiating and verifying with the consent entities. The authors have incorporated multi agent vehicle in order to ensure security in the vehicles. In [11], an unmanned aerial vehicle with a blockchain framework is introduced. Here every vehicle behaves as a node which uses creating and reading transactions and is also able to exchange communication through blockchain. Authors in [12-14] have utilised blockchain methodology to monitor and secure traffic flow sharing between vehicles with data correctness and tamper resistance in the agreement mechanism. Traffic data bypassing is collected using proof of event agreement [15]. Here blockchain enables two phase transaction between the vehicles. The observed simulation result indicates a positive response for the proposed work by the authors with respect to trust verification tracing events [16].

Moreover to enable vehicle security and constrain the attacks, a number of authentication methodologies where also proposed. Attacks like authentication and guessing time requirement, location spoofing and replay have been identified to analyse and improve security mechanism proposed by authors in [17]. This method is also related by drawing a comparison between the existing methodologies with respect to security and performance.

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

Similarly, a number of researchers have also focused on ensuring security in information exchange by considering external intruders, who have the ability to disrupt confidentiality [18], authenticity and integrity [19, 20]. In secure exchange of messages is introduced within a smart city using elliptic curve cryptography methodology [21]. This technique enhances security by using two level authentications. Both formal and informal analysis is made using burrows logic along with internet security protocols validating the work. Moreover the proposed methodology is compared with previously existing techniques in relation to overheads, latency and reliability [22-24]. Presence of intruders and malicious users will collapse the whole communication system leading to chaos on the streets. The biggest issues with CAV is data falsification attack where information to save from peers and other vehicles are relied upon [25]. Till date many be secure CAV mechanism have been introduced scientists and researchers. However, the number of books on CAV using blockchain is very limited. In this paper a blockchain framework is introduced to secure the IoT sensors which are attacked by expert intruders [26-27].

3. Proposed Methodology

In this proposed work, a blockchain framework of CAV is used to enable transparency and security of vehicles and users. To keep track of every activity that the IoT sensors perform [28], a secure methodology is introduced. Henceforth for ensuring and providing safety at the time of ride sharing in CAV, the transmission that takes place between the sensors through smart devices is also kept track of. Though maintaining a record or tracking everyday activities of the vehicles is an easy task, it further increases the computational complexity of the system in real time. This is primarily because many intruders tend to attack mobility [29] of vehicles using man in middle or denial of service threat. However when a complete track of record of all the activities are in place, it will be easy to identify and trace the attempts by intruders to penetrate into the security of IoT devices. Moreover, these devices belong to the upper layer of the network and the attack probability is low when compared with edge level devices [30]. In

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

order to check security of smart devices, providers who register are used so that devices and information are not tracked altered or changed by any other devices once they are casted.

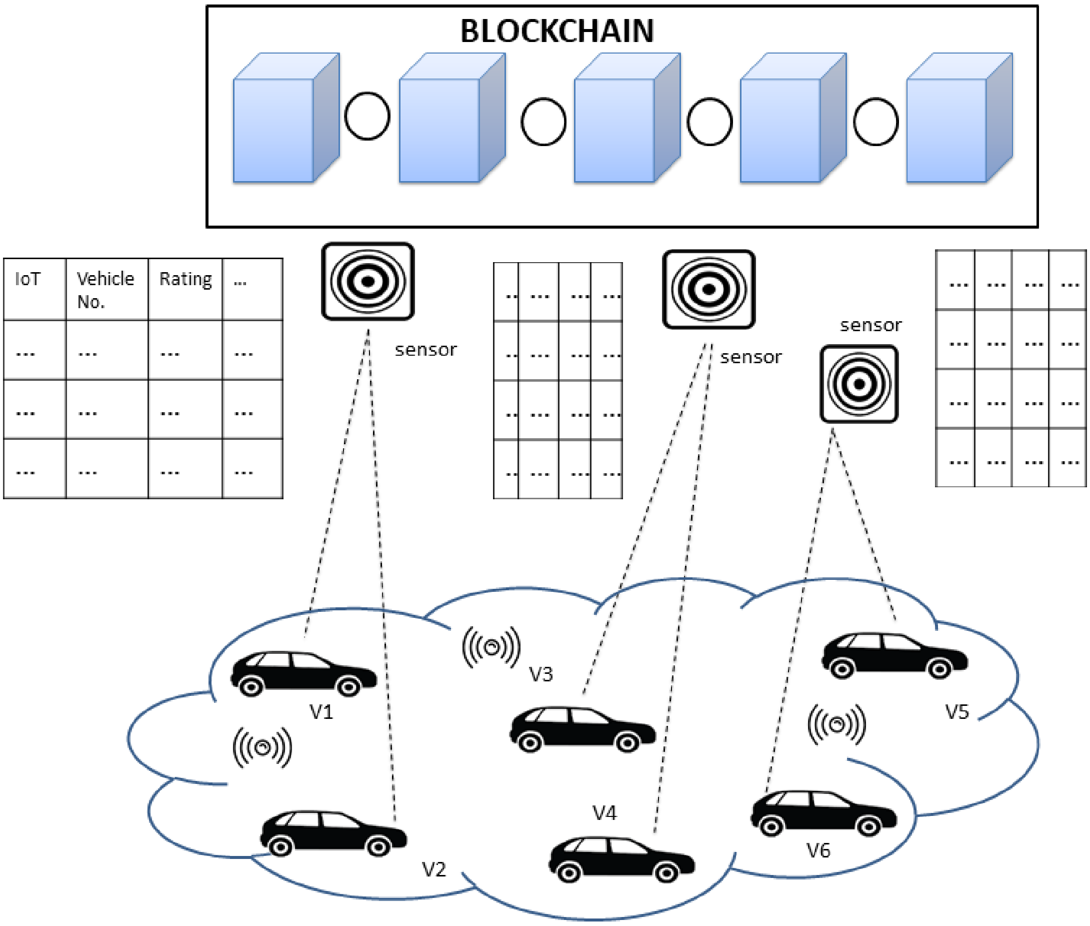

Figure 1. Blockchain- CAV architectural framework

Similarly, uniqueness in money bank vehicles is verified to guarantee that tracking information is not taken by anybody. This elaborate process can be easily resolved by using blockchain technique with smart contracts that layout as writing the code, objects, models and rules between the parties. Smart contracts indicate an agreement or a consensus between two parties. When a smart contract is established, it will not be altered or deleted from the blockchain network. Hence, a central authority is not required to validate the work performed

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

by individual entities. Every vehicular node will be able to calculate its result of contract without the need for external interference. Hence using the proposed blockchain framework, device or automated vehicle which is logged into or registered with the network prior to accessing or providing vehicular service is kept track of. The essential details of IoT devices and vehicles are saved in an ordinary database at the beginning and then moved onto the blockchain permanently where every activity is kept track of. Blockchain technique incorporated CAV architectural framework is represented in figure 1. It can be observed that smart devices for IoT sensors are connected to the vehicles such that they can be used to guide monitor and control drivers on the street. Based on the transmission range and the communication coverage of the IoT sensors and devices, the number is vehicles connected will vary.

Both blockchain network and ordinary tables will be used to keep track of vehicle numbers as well as ratings provided by users and customers. This way, a complete record or track of every illegal or legal activity carried out by the IoT devices or vehicle can be maintained. In the event of compromise in the IoT device due to intruder attack the blockchain authorities who are in-charge of that particular device will be able to identify the attack and take immediate course of action to ensure security to the vehicle. Rather than recording every activity of the IT devices it is easier to record, analyse and trace every vehicle using blockchain. However this aspect of maintaining such a large data based on vehicular data will further increase the possibility of computational time and power, especially since the vehicle is in mobility in real time scenarios. Hence in order to address this aspect of levitation in power and high storage, we save only the activities of the IoT devices instead of the entire vehicle in blockchain. In a particular device which keeps track of a specific number of vehicles, we will be able to easily track and retrieve the user's request from blockchain. It is also possible to minimise information that are saved in a block by using blockchain technology. Detection of intruders who will be able to change the previous interactions or history of the device and can also reduce the vehicles rating or block it completely is also possible.

4. Scenarios of Attacks

There are a number of attacking strategies available and it can be adopted by an intruder, who used to perform malicious activities. Traffic congestion, data falsification, driver rating alteration, and breach of IoT sensors and gadgets are some of the difficulties produced by intruders that cause mayhem in the car at work. Listed below are some of the attacking scenarios that occur between vehicles and its users in a ride service:

- Traffic Congestion: Here, for the benefit of the intruder, he might divert suggestions of path on the road.
- Data falsification attack: One of the biggest security concerns in CV is data falsification attack, since vehicles are heavily dependent on the data received from peers or other vehicles.
- Modification of ratings: Once the rating for a particular cab driver has been submitted and it is not possible to change the rating even on successful intrusion into the IoT device
- Misbehaving with the user: When a person takes a ride on the vehicle, if the service provider behaves in an inappropriate manner by changing the route taken or by halting frequently, the location of the cab will be monitored continuously by the IoT sensors and the path taken will also be traced and updated in the server in order to prevent any mishap from occurring. In such events and notification will be sent to the primary server and the cab driver will be punished or terminated accordingly.
- Add-on of compromised IoT: When compromised IoT devices are registered by the intruder to execute passive and active attacks it is instantaneously identified by the blockchain peer nodes by checking the illegal action performed such as compromising or stealing of legitimate IoT devices.

Using secure information sharing and cab riding mechanism with blockchain, it is possible to prevent such attacking strategies. Moreover, a number of simulation is also carried out with respect to several parameters, indicated the validation of the proposed work.

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

5. Results and Discussion

Experimental observation indicates that, the proposed security framework performs better than the previously existing algorithms. Fig.2 shows the user's fake request graph, where the efficiency of the proposed work tends to increase as the number of requests increase, while that of the existing methodology performs less efficiently. Moreover, as the network congestion increases, it will also lead to tremendous degradation in the network performance.

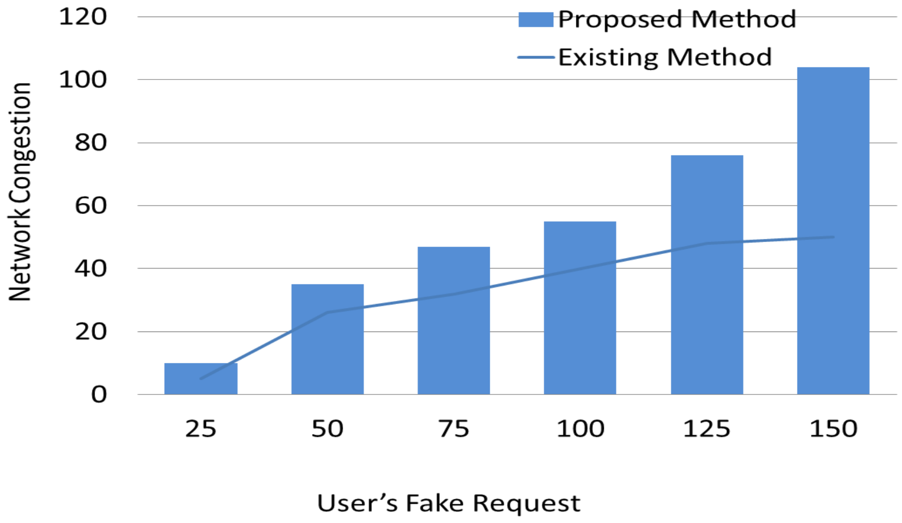

Figure 2. Network Congestion due to User's Fake Request

Fig.3 indicates the compromised devices that are controlled and monitored at a regular basis. Here, when an IoT device is compromised, it will intrude into restricted area and alter or remove confidential information and further it will be used for personal gain. This will also affect the network performance. On the other hand, Fig.4 shows the ratings stored and it may be altered by intruders and will also pave a platform for the continuation of misbehaviour with customers.

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

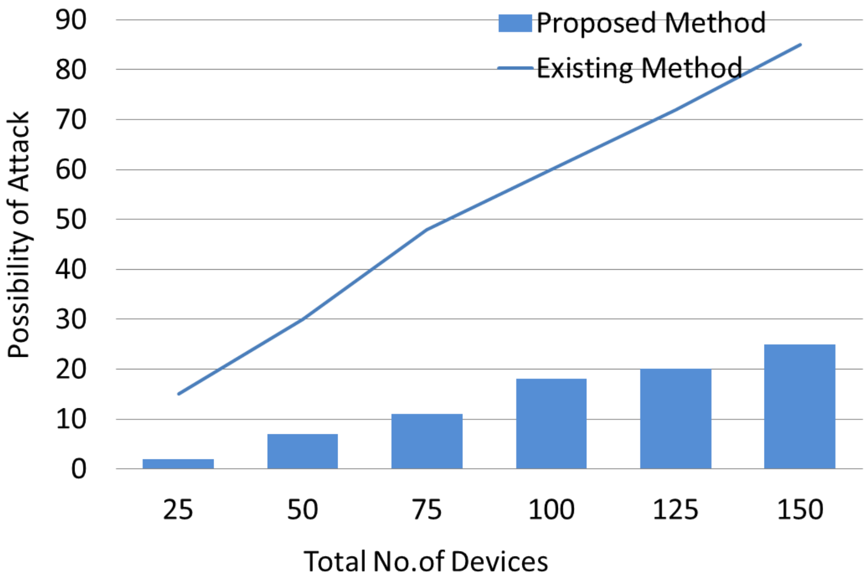

Figure 3. Compromised Devices Vs. Possibility of Attack

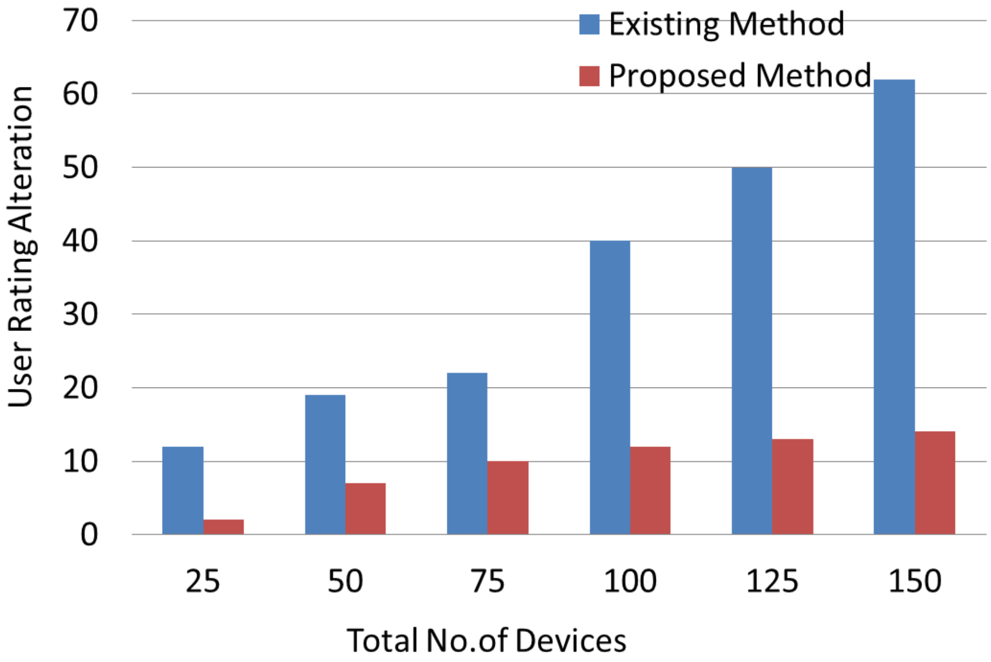

Figure 4. Possibility of User Rating Alteration by Intruders

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021

6. Conclusion

In this work, a blockchain framework is used to secure the transmission that takes place between autonomous vehicles that are connected. IoT sensors and devices are used as a medium for transmission and can be compromised by intruders. To ensure transparency and secrecy among cab drivers and customers, every activity of the entities of the IoT devices and vehicles are properly recorded and traced with blockchain. Information is extracted from the IoT devices and stored onto the blockchain, providing enhanced device security and customer safety. Using this methodology, a significant decrease in the compromise of IoT devices and users' fake requests is observed. The result attained shows a positive success rate of about 82% when compared with the other existing works. As a future scope, deep and reinforced learning can be used to improve the system intelligence.

References

[1] Sivaganesan, D. "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 59-69.

[2] Madaan, G., Bhushan, B., & Kumar, R. (2021). Blockchain-based cyberthreat mitigation systems for smart vehicles and industrial automation. In Multimedia Technologies in the Internet of Things Environment (pp. 13-32). Springer, Singapore.

[3] Haoxiang, Wang, and S. Smys. "Big Data Analysis and Perturbation using Data Mining Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 19-28.

[4] Haro-Olmo, F. J., Alvarez-Bermejo, J. A., Varela-Vaca, A. J., & López-Ramos, J. A. (2021). Blockchain-based federation of wireless sensor nodes. The Journal of Supercomputing, 77(7), 7879-7891.

[5] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[6] Banotra, A., Sharma, J. S., Gupta, S., Gupta, S. K., & Rashid, M. (2021). Use of blockchain and internet of things for securing data in healthcare systems. In Multimedia Security (pp. 255-267). Springer, Singapore.

[7] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." Journal of ISMAC 2, no. 02 (2020): 106-117.

[8] Ramaguru, R., Sindhu, M., & Sethumadhavan, M. (2019, April). Blockchain for the Internet of Vehicles. In International Conference on Advances in Computing and Data Sciences (pp. 412-423). Springer, Singapore.

[9] Shakya, Subarna. "Process mining error detection for securing the IoT system." Journal of ISMAC 2, no. 03 (2020): 147-153.

[10] Saranti, P. G., Chondrogianni, D., & Karatzas, S. (2018, May). Autonomous vehicles and blockchain technology are shaping the future of transportation. In The 4th conference on sustainable urban mobility (pp. 797-803). Springer, Cham.

[11] Sivaganesan, D. "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 59-69.

[12] Shirley, D. Ruth Anita. "Systematic diagnosis of power switches." In 2014 International Conference on Embedded Systems (ICES), pp. 32-34. IEEE, 2014.

[13] Smys, S. "A Survey on Internet of Things (IoT) based Smart Systems." Journal of ISMAC 2, no. 04 (2020): 181-189.

[14] Erdem, A., Yildirim, S. Ö., & Angin, P. (2019). Blockchain for ensuring security, privacy, and trust in IoT environments: the state of the art. Security, Privacy and Trust in the IoT Environment, 97-122.

[15] Raj, Jennifer S. "Security Enhanced Blockchain based Unmanned Aerial Vehicle Health Monitoring System." Journal of ISMAC 3, no. 02 (2021): 121-131.

[16] Reebadiya, D., Rathod, T., Gupta, R., Tanwar, S., & Kumar, N. (2021). Blockchain-based Secure and Intelligent Sensing Scheme for Autonomous Vehicles Activity Tracking Beyond 5G Networks. Peer-to-Peer Networking and Applications, 1-18.

[17] Shrestha, Sujan, and Subarna Shakya. "Technical Analysis of ZigBee Wireless Communication." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 197-203.

[18] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the Lifetime of the Nodes. In IOP Conference Series: Materials Science and Engineering (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[19] Dhaya, R., and R. Kanthavel. "Bus-Based VANET using ACO Multipath Routing Algorithm." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 40-48.

[20] Angin, P., Mert, M. B., Mete, O., Ramazanli, A., Sarica, K., & Gungoren, B. (2018, June). A blockchain-based decentralized security architecture for IoT. In International Conference on Internet of Things (pp. 3-18). Springer, Cham.

[21] Karthikeyan, M., S. Sathiamoorthy, and M. Vasudevan. "Lane Keep Assist System for an Autonomous Vehicle Using Support Vector Machine Learning Algorithm." In International Conference on Innovative Data Communication Technologies and Application, pp. 101-108. Springer, Cham, 2019.

[22] Kaiser, C., Steger, M., Dorri, A., Festl, A., Stocker, A., Fellmann, M., & Kanhere, S. (2018, September). Towards a Privacy-Preserving Way of Vehicle Data Sharing–A Case for Blockchain Technology?. In International Forum on Advanced Microsystems for Automotive Applications (pp. 111-122). Springer, Cham.

[23] Aishwariya, K. K., Sanil K. Daniel, and K. V. Sujeesh. "Zone Safe Traffic Assist System and Automated Vehicle with Real-Time Tracking and Collision Notification." In International Conference on Innovative Data Communication Technologies and Application, pp. 663-669. Springer, Cham, 2019.

[24] Shirley, D. R. A., Sundari, V. K., Sheeba, T. B., & Rani, S. S. Analysis of IoT-Enabled Intelligent Detection and Prevention System for Drunken and Juvenile Drive

Classification. Automotive Embedded Systems: Key Technologies, Innovations, and Applications, 183.

[25] Srinivas, Kethavath, and Mohit Dua. "Fog Computing and Deep CNN Based Efficient Approach to Early Forest Fire Detection with Unmanned Aerial Vehicles." In International Conference on Inventive Computation Technologies, pp. 646-652. Springer, Cham, 2019.

[26] Rakovic, V., Karamachoski, J., Atanasovski, V., & Gavrilovska, L. (2019). Blockchain paradigm and Internet of Things. Wireless Personal Communications, 106(1), 219-235.

[27] Kumar, S. Satheesh, S. Karthik, J. S. Sujin, N. Lingaraj, and M. D. Saranya. "Smart On-board Vehicle-to-Vehicle Interaction Using Visible Light Communication for Enhancing Safety Driving." In Inventive Computation and Information Technologies, pp. 247-257. Springer, Singapore, 2021.

[28] Abubaker, Z., Gurmani, M. U., Sultana, T., Rizwan, S., Azeem, M., Iftikhar, M. Z., & Javaid, N. (2019, November). Decentralized mechanism for hiring the smart autonomous vehicles using blockchain. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 733-746). Springer, Cham.

[29] Manickavasagam, L., N. Krishanth, B. Atul Shrinath, G. Subash, S. R. Mohanrajan, and R. Ranjith. "Instrument Cluster Design for an Electric Vehicle Based on CAN Communication." In Inventive Computation and Information Technologies, pp. 271-284. Springer, Singapore, 2021.

[30] Ekramifard, A., Amintoosi, H., & Seno, A. H. (2019, March). A systematic literature review on blockchain-based solutions for iot security. In The 7th International Conference on Contemporary Issues in Data Science (pp. 311-321). Springer, Cham.

Author's Biography

Jennifer S. Raj received the Ph.D degree from Anna University and Master’s Degree in communication System from SRM University, India. Currently she is working in the Department of ECE, Gnanamani College of Technology, Namakkal, India. She is a life member of ISTE, India. She has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. She is book reviewer for Tata Mc Graw hill publication and publishes more than fifty research articles in the journals and IEEE conferences. Her interests are in wireless Health care informatics and body area sensor networks.

ISSN: 2582-337X
Submitted: 10.07.2021
Revised: 13.07.2021
Accepted: 14.07.2021
Published: 17.07.2021