Study Investigation of the Internet of Vehicle (IoV) Security

Emmanuel O. Akingboye
Graduatedept. of Computer Networks and Security
University of Bolton, United Kingdom

Thaier Hamid, PhD
Lecturer Dept. of Computer Networks and Security
University of Bolton
United Kingdom

ABSTRACT

Cybersecurity is the protection of the things connected to the Internet in one way or the other with a lot of things and millions of connections involved, the Internet connection becomes the target for hackers to compromise the Confidentiality, Integrity, Availability of the networks involved, and even compromise the connected devices. The Internet of vehicle security becomes even more fragile.This paper is to discuss the IoV in general, the security challenges facing theInternet of vehicles users', create more awareness of the Internet of vehicle security, and lastly provide a security mitigation recommendation for the Internet of vehicle users. Furthermore, the academic research analysis to be generated from this research paper will further help other researchers to establish or add their research analysis to the result findings of the above research topic for the general safety of the Internet of vehicle users, also to reduce the gap between cybersecurity and the Internet of vehicle (IoV) technology.

Keywords

IoV, Security

1. INTRODUCTION

The invention of vehicles in the early years has enhanced transportation, making transportation an accessible network. However, statistics referenced show that close to 90% of traffic accidents are caused by human driving parallax errors [3], [4], therefore calling for the need for efficiency, intelligent features, and safety features in IoV. Furthermore, the estimated numbers of vehicles are expected to soar up to two (2) billion by the end of 2035, and research also suggested that the IoV devices are expected to reach over fifty-one (51) billion by 2023,[5], [15]. The tremendous increase in the number of IoV devices and vehicles directly shows the need for safety features needed in vehicles.Furthermore, the Internet on its own since invention has enhanced various aspect of life. The Internet invention has gathered devices of things to form the Internet of Things (IoT) under its umbrella, the word Internet of things (IoT) first came out in 1999 via a presentation from Kevin Ashton of MIT [20], [21]. The rapid development in technology has since then seen the Internet of Vehicles (IoV) emerge from the Internet of Things (IoT), also VANETs.IoV has since composed the grid structure of the Internet of mobility. Thesecurity issues with the need for safety in vehicles and other vulnerabilities is the birth of the term **INTERNET OF VEHICLE SECURITY**.

2. IoV ARCHITECTURE

The Internet of vehicle architecture comprises of heterogeneous networks that can adapt to evolving technologies to provide the Internet of vehicle users safety use with highly spiced technology features that enhance the Internet of things in general, also to equip technology on the road [18].The Internet of vehicles architecture identifies functionalities in vehicles, check for similarities in the functionality to help group them according to their functionalities, and further prioritize the segmented layers of the heterogeneous functionalities with the help of the architectural structure [13]. There are numbers of network features enabled by the Internet of vehicles for the users include reliability, scalability, interoperability, flexibility, modularity, among many others, this is to create a flexible integration and technology adaptation simply with the Internet. Studies show that the Service Oriented Architecture (SOA), coupled with the plug-and-play technology design, plays an essential part of the IoV architecture in most of its stages [13].IoV requires high-performance accuracy, real-time data analysis of sensors, intelligent decisions, network modularity, network reliability, and stability in data transmissions [4]. The IoV architecture further simplifies its functions and implementations by segmenting the architecture into different layers.

2.1 Application layer

The application layer is the known layer that manages the smart applications such as infotainment applications, traffic safety applications, efficiency applications, radio, and media applications that exist in the IoV [13]. This level of the IoV architecture is connected to the intelligence level, studies show that the application layer responds to process data communicated from the artificial learning and intelligence layer to promote IoV efficiency [4]. Furtherly called the IoV resources powerhouse [15], this layer also stores and compute data in addition to intelligent decision making.

2.2 The Network/co-ordination layer

This level can be called the communication layer[19], this networkcommunication layer of the Internet of vehicles consists of the likes of 3/4/5Gs, GSM, DSRC, IEEE 802.11p WAVE, LTE, WiMax, Wi-Fi, WLAN, Bluetooth which are useful in supporting various forms of smart communications of the IoV. The network communication includes the Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P),Vehicle-to-Vehicle (V2V), Vehicle-to-Sensor (V2S) [19], also edge cloud, to optimize the real-time information interaction, and the artificial intelligence self-organizing network among vehicle-to-vehicles, vehicles-to- Internet, or Vehicle-to-Human services in the IoV communication layer [7].Communications experienced in IoV network/ communication layer can be refer to as the Vehicles-to-everything communication (V2X) [7].The vehicles communications include:

- **Vehicle-to-Internet (V2I);** This provides connections between vehicles and the Internet via the technologies of 3/4/5Gs, Bluetooth, Wi-Fi access points on the roadside, satellite network [7].

- **Vehicle-to-Sensor (V2S);** With this, vehicles intend to generate connections between themselves and the embedded sensors that circulate the generated data around the vehicle. The generated data here will then forwarded to the Electric Control Unit for processing [7].
- **Vehicle-to-road Infrastructure (V2I):** Road signals and many other road infrastructures like the traffic monitoring sensor use the V2I connection, it is based on the IEEE 802.11p WAVE standard [2].
- **Vehicle-to-human (V2H);** research shows the V2H connect vehicles with the pedestrians, drivers, passenger, and more uses the plug and play technologies, smart devices, the Near field communication (NFC), Android system of the OAA, and this sort of connection is generally based on the 3/4/5Gs technologies [4], [7], [15], [18], [20], [21].
- **Vehicle-to-Vehicle (V2V) communication:** this connection provide interaction, and communication between vehicles with the proximity services of devices similarity [7].

2.3 The perception Layer

This layer gathers the sensor phases that stimulate all data on the Internet of vehicles according to [19], data collected here could be vehicles attached situations, environmental conditions, safety drive data, radio frequency identification for the vehicle position, geographical location, and other factors.Also called the sensing layer of the IoV, it accumulates different sources of the massive heterogeneous data required in the IoV [4]. The likes of the facial expression data, driving route related data, vehicle temperature data, climatic information, destination analysis, speed control, traffic congestions data, road map, fuel level, mechanical fault detection data, and many more data that function to enhance the data processing efficiency, and the communication of the Internet of vehicles applications [7]. This stage the IoV communicates with various technologies around the Internet of the vehicles to specifically detect events useful for the efficiency of the functionality of the vehicles, VANETs, Internet applications, and the Internet of things [5].

2.4 Artificial intelligence / Cognition layer

This layer from academic journals shows the virtual cloud representation in the IoV, helping to process data communicated from other layers to make a smart decision. Furthermore, this layer manages the Big Data Analysis and Vehicular cloud computing (VCC) in the IoV architecture layer [13]. The heterogeneous data compilation, flow, data fetching, pattern analysis, and intensive learning of sensor behavior take place at this layer ensuring the enhancement of the intelligence of the IoV. The processes here include the likes of the road conditions check, driving pattern of vehicle users, the difference in vehicle model analysis, real-time driving analysis, storage of collected data, and vehicle security analysis [4].

2.5 Control Layer

The control layer is also referred to as the management layer in IoV, this layer deal with the management of various active network service provision inside the Internet of vehicles system to help generate policies for better management like the vehicle packet flow, traffic information management amongst others [5].Research further proves that the control layer with its functions maintains the position of the principal determining system of the IoV with the control management ability [4].

3. IoV NETWORK MODEL

The IoV network model is often known as the Lego construction bricks that make up the main network element of the IoV [13], this explains and simplifies the functionalities of the IoV heterogeneous network comprehensiveness as a package. The IoV network model creates efficient integration for the IoV infotainment applications use [18], and safety drive function. These include voice-over internet protocol, video services, audio services, vehicle software updates, route planning system, live weather updates, vehicle navigation system, speed control, vehicle emergency alert system.The IoV network model further explains the collaboration between technologies to achieve reliable and efficient internet use in vehicles, technologies like Wi-Fi, IEEE 802.11p, 5G [6], [18].The IoV network model has three frames that can be fracture and discussed in three-phase as seen from research [20], [21].

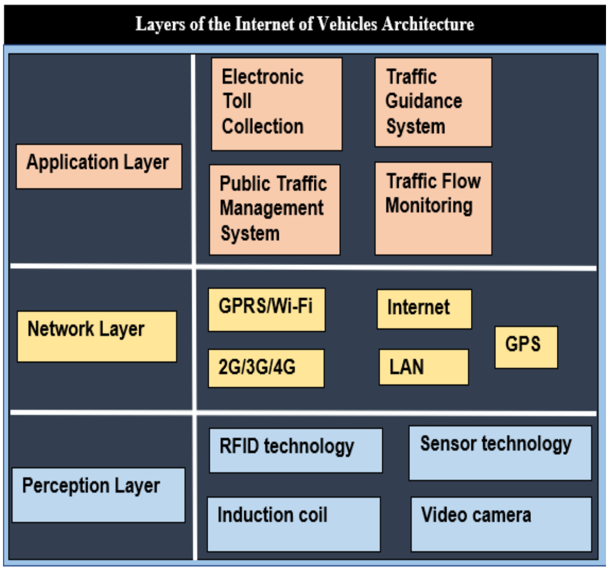

Figure 1: Most discussed IoV architecture

3.1 Cloud

Considering the storage space needed for information in vehicles, how vehicles work, and the amount of data to be collected, processed, and transmitted, the cloud infrastructure architecture is the best solution in handling the level of IoV data magnitude. The cloud computing plays essential role in the IoV framework to enhance its applications [13]. Examples are uploading of the traffic information on the cloud for vehicle usage, processing, storing, and analyzing data. The cloud has emerged as the leading infrastructure in the IoV framework because of the heterogeneous nature [18], noting that smartphones, Access points, RSUs, and BSUs all uses the cloud infrastructure for their data processing medium and communication medium. Cloud computing importantly works as infrastructure, services, and storage in IoV, making it the brain of the IoV network model [20], [21].

3.2 Connection/Network

Impressively, the connection layer function as the bridge between the cloud system and the vehicle in other to access the smart IoV applications based on the cloud service [13]. Furthermore, the interconnection that occurs among many networks needed for the vehicles like the 3/4/5Gs, LTE, Wi-Fi, VANETs also stresses the need and function of the connection layer as it prioritizes needed connection after integration. The connection level produces mainly connection between the third-party Network Inter Operator(TPNIO), the Gateway of Internetworking (GIN), and the Technology Handling system. GIN represents all accessible networks, while the TPNIO usually manages the connection involved in IoV networks. The establishment of data routing in the IoV is a necessary process that happens at the connection level because of the difference in cloud services and networks.This layer also shows the IoV communications like the Vehicle-to-Infrastructure (V2I), Vehicle-to-Personal Devices (V2T), Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Units (V2R), and they use technologies to promote internet connection in vehicles [20], [21].

3.3 User Layer

The User layer of the IoV network model shares updates about the endpoint users, customers, and consumers of theIoV products [20], [21].The IoV users can be furtherly identified as the passengers of a vehicle connected to the IoV applications using smartphone devices, auxiliary cables, Bluetooth, Wi-Fi, and other connection media, user can as well be the driver who is in charge of the control of a vehicle directly using the IoV applications like the navigation system while driving, radio, music streaming, real-time weather updates, speed control and many tracking system that monitors the connection between uber drivers and their potential passenger to give updates on the driver's location before pickup [20], [21]. The applications used in this layer could either be used for safety services, or commercial and entertainment services such as the Speed control, connected drive system, petrol pump, and another location calculator, weather report, emergency brake system, music streaming, vehicle self-diagnostic system, vehicle monitor and surveillance, traffic information. All these applications are enabled using 3/4/5Gs Ethernet and Wi-Fi connections [18], [20], [21]. more, or user could be a pedestrian outside the vehicle sharing some applications with the vehicle and other users at a certain time like the real-time tracking system that monitors the connection between uber drivers and their potential passenger to give updates on the driver's location before pickup. The applications used in this layer could either be used for safety services, or commercial and entertainment services such as the Speed control, connected drive system, petrol pump, and another location calculator, weather report, emergency brake system, music streaming, vehicle self-diagnostic system, vehicle monitor and surveillance, traffic information. All these applications are enabled using 3/4/5Gs Ethernet and Wi-Fi connections [18], [20], [21].

3.4 Benefits, Features, and applications of IOV

Research papers show that the Internet of vehicles has many distinguishing characteristics that support the goal of the IoV science in enhancing vehicle usage. Impressively, these features turned out to be valuable advantages for the IoV product users [19], [20], [21]. The applications are compatible with VANETs the same as the IoV to enable the vehicle to act in a mobile device transformed way [5]. The IoV applications can be further subdivided into different categories according to their performance [20], [21]. The IoV applications can be divided into the following categories:

- ❖ **Traffic efficiency applications:**These are applications that manage the elementary float to urban blockage, also deal with the transportation logistics system like Road congestion management [19].
- ❖ **Safety-related applications:**The safety-related features and applications used in vehicles to manage safeties of vehicles, and the users with the data received from the sensors of the IoV science processed with the Internet. This provides warnings to reduce road accidents in vehicles reducing user'spotential accidents, providing safety applications that act proactively in sending users safety warning to avoid anyform of mishap [20], [21]. The safety-related application aims at reducing latency, parallax safety errors and increase vehicles level of reliability with its features [12]. These safety features include:

- Collision avoidance with automatic brake sensor application.
- Traffic signals violation warning system used to send drivers information about the traffic situation of vehicle location, roadwork information, nearest bridge information, curve bend cautions.
- Speed control warning system used for sharing and displaying road speed limits in real-time, warning drivers as they go above them to limit the potential risk of accidents.
- Blind merge warning sending messages to vehicle drivers to avoid any anticipated crash at junctions using the RSUs, also providing an all-clear signal for drivers in tricky road bends.
- SOS service application that usually sends emergency messages to save a driver or vehicles users in case of breakdowns or accidents which will contain the current location of the vehicle, picture of the emergency location, voice recording short message to ask for help using the vehicle-to-vehicle, and vehicle-to-infrastructure services [20], [21].

- ❖ **Crashing warning system:**This calculates the distance between cars with the vehicle-to-vehicle communication and sends a caution message if there is not enough distance for brake application.
- ❖ **In-vehicle diagnostic signage:**Checks the health of vehicles to give the information needed to drive like low oil, due vehicle services, faulty lights, etc.
- ❖ **Comfort and Convenienceapplication:** These are applications in vehicles aimed to maintain a high-performance level in vehicles with ease like remote door lock, real-time vehicle tracking system, dash camera, weather information, parking help, and more [19].

- **Infotainment applications:** These are the applications that provide vehicle users with cheerful and enjoyable activities while using vehicles like peer-to-peer Bluetooth and Wi-fi enabled devices, Internet provision, parking system, online music streaming, hands-free calls, and messages on the dashboard [19].

4. IoV SECURITY

The IoV efficiency is measured with processes that encapsulate its features like data collection, data processing, and data transmission [20], [21]. These fundamental processes of the IoV features also make the IoV system vulnerable to different types of cyber-attacks and threats. Let's review the security challenges facing the Internet of vehicles based on previous academic facts, also recommend appropriate mitigations and preventions that can be provided for a more secured IoVworld.

4.1 IoV COMMON THREATS AND VULNERABILITIES

Numerous threats and vulnerabilities have accumulated over the years to become serious contending challenges for the Internet of vehicles; literature reviews of previous academic papers often show long lists of IoV security issues regarding threats and vulnerabilities. Below is the category of threats and vulnerabilities associated with the IoV security system.

- Masquerading attack.
- Data availability attacks.
- Wormhole attack.
- Data Authenticity attacks.
- Privacy bridge.
- A denial-of-Service attack.
- Ultrasonic sensors attack.
- Spoofing attack.
- Signal level attack.
- Sensor hardware attack.
- Digital level attacks.
- Availability attacks.
- Secrecy Attacks.
- Routing attacks.
- Dissimulation of GPS attack.
- Eavesdropping attack.
- Impersonation attack.
- Data falsification attack.
- Malware attack.
- Fuzzy attack.
- Channel hindrance attack.

The above-listed threats and vulnerabilities are the common vulnerabilities in vehicles according to peer-reviewed journals on the Internet of vehicle security, they are frequently mentioned threats and vulnerabilities in all IoV products, and this prove how common they exist within the Internet of vehicles to cause potential damages and harm to the IoV devices network[1], [2], [4], [6], [7], [13], [15], [17], [20],[22].

4.2 IoV SECURITY MITIGATIONS

The mitigation process will help increases the security level in the vehicles, and secure future design [8]. Cybersecurity technics of both software and hardware devices are needed to increase its proposed security. The IoV security countermeasure requirements should include the following:

- **Intrusion detection systems:** Anomaly-based detection, and signature-based detection have proved to be efficient against IoV intrusion penetration which will be a useful defenseagainst threats and attacks.[8].
- **Pseudonym security technic for IoV:**This security measure is made up of the anonymous batch vehicle (ABV) authentication and Anonymous Batch Message Authentication (ABM) to help convey all safety Location-Based Information in IoV products [8], [24].
- **Authentication security:** This security measure is made up of the anonymous batch vehicle (ABV) authentication and Anonymous Batch Message Authentication (ABM) to help convey all safety Location-Based Information in IoV products[8], [24].
- **Honeypot Control:** The honeypot will provide an intended replicated field for hackers to operate, which will give users opportunities to know how hackers intend to operate on their vehicles and help avoid real-time damages. The honeypot security mitigation works perfectly with the Intrusion system in vehicles [8].
- **Key Management:** This countermeasure provides more security for the IoV keys to validate, authenticate, and manage the usage [24]. This security system uses the Key distribution Centre (KDC) policy to generate, transmit, and securely distribute keys.
- **Threat Model:** The threat model ensures that the weaknesses of the IoV are exposed to the users making it easy to detect the vulnerabilities and threat, therefore giving a clear hint of the needed mitigation. This method can be visible with the use of a graph technic, or mathematical-based technic to provide the relationship between various parts of the IoV to display a clear interpretation of vehicle vulnerabilities to users [8].
- **Private routing protocol technic:**Discussing the advantages of using private routing protocol in the IoV by research journals, this privatizes all the routing node data making it all secure over the Internet and when transmitting in vehicles [24].Encryption of transmitted data is a possible provision with the routing protocol solution.

- Users and drivers of vehicles must park in secure locations to prevent physical access that targets to compromise the sensors [11].
- Networks monitoring alarm systems with the intrusion protection systems configuration to trigger warnings and enforce changes in vehicles that will reduce physical access to vehicles also disallow unusual behaviors in the vehicle dashboards [11], [12].

5. EXTRA LAYER SECURITY IMPLEMENTATION

The extra layer mitigation control recommended is the snort configuration as the IDS (Intrusion detection system) and UFW (uncomplicated firewall) as the combined designed security for IoV better networks.

5.1 IoV IPDS, Firewall features, and deployment review

The proposed extra security layer for the Internet of vehicles security can be best designed as a software package containing the IPDS and Firewall configuration settings available to be installed in different unit parts of the vehicle CAN BUS system to gain more reliable security [14]. The features of the IPDS firewall software would include the following.

1. **Intrusion Prevention:** The intrusion prevention configuration will be the part of the software configured to send the usual log alert, then move to close open ports on the CAN-BUS unit when thevehicle is not in use. These will prevent zero-day attacks.
2. **Packet filter (firewall):** The firewall configuration added to the software will enhance security monitoring all communication of the CAN-BUS unit, checking on the packets sent and received to drop bad packets and allow the good ones.
3. **Intrusion Detection:** This will mainly function more by detecting all abnormal activities and changes in vehicles during use and even when the vehicle is not in use [14].
4. **Log analysis:** The log analysis will highlight important alert messages and send them to the log file for vehicle users. Furthermore, the log analysis will show users the overall level of extra security of their IoV products.

5.2 IDS Recommendation

Intrusion detection system configuration of various types like the Snort or Suricata plus the firewall would strengthen the vehicles CAN BUS system and protect them against zero-day attacks by noticing unusual behaviour in the network.

5.3 Firewall Recommendation

The recommended firewall for the IoV better security is the uncomplicated firewall (ufw) simply designed to filter the network packet with a rule to monitor incoming and outgoing packets on the network.

5.4 RESULT

The result from the snort configuration and the firewall configuration will enhance failure in connection from any external network, also will displace a threat log from attackers. With this extra layer of security in place plus the physical security measures, this research project has practically proven that the implementation tested can increase the level of the Internet of vehicle security.

6. CONCLUSION

The discussion in this paper generally combined the introduction to IoV, the architecture, benefits, application of IoV, vulnerabilities of IoV, and the mitigation required for safer Iov in general. The Intrusion detection system plus firewall implementation demonstrated in this paper was the best available choice for the CAN-BUS network in vehicles. IDS and Firewall is additional security for IoV in general, also providing information about upcoming potential errors or cyber-attacks in vehicles CAN-BUS network. Lastly, this paper discussed the various important sides of IoV and the security mitigation to promote a simplified IoV security solutionand awareness to the readers.

7. REFERENCES

[1] Abu Talib, M., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2018). Systematic literature review on Internet-of-Vehicles communication security. International Journal of Distributed Sensor Networks, 14(12). https://doi.org/10.1177/1550147718815054

[2] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. IEEE Access, 8, 54314–54344. https://doi.org/10.1109/ACCESS.2020.2981397

[3] Chen, C. M., Xiang, B., Liu, Y., & Wang, K. H. (2019). A secure authentication protocol for internet of vehicles. IEEE Access, 7, 12047–12057. https://doi.org/10.1109/ACCESS.2019.2891105

[4] Chen, M., Tian, Y., Fortino, G., Zhang, J., & Humar, I. (2018). Cognitive Internet of Vehicles. Computer Communications, 120(February), 58–70. https://doi.org/10.1016/j.comcom.2018.02.006

[5] Contreras-Castillo, J., Zeadally, S., & Guerrero-Ibanez, J. A. (2018). Internet of Vehicles: Architecture, Protocols, and Security. IEEE Internet of Things Journal, 5(5), 3701–3709. https://doi.org/10.1109/JIOT.2017.2690902

[6] Duan, W., Gu, J., Wen, M., Zhang, G., Ji, Y., & Mumtaz, S. (2020). Emerging Technologies for 5G-IoV Networks: Applications, Trends and Opportunities. IEEE Network, 34(5), 283–289. https://doi.org/10.1109/MNET.001.1900659

[7] Fraiji, Y., Ben Azzouz, L., Trojet, W., & Saidane, L. A. (2018). Cyber security issues of Internet of electric vehicles. IEEE Wireless Communications and Networking Conference, WCNC, 2018-April, 1–6. https://doi.org/10.1109/WCNC.2018.8377181

[8] Gafencu, L., & Scripcariu, L. (2018). Security Issues in the Internet of Vehicles. 2018 12th International Conference on Communications, COMM 2018 - Proceedings, 441–446. https://doi.org/10.1109/ICComm.2018.8430112

[9] G, A.E. (2018). How to hack any car with this tool. [online] Information Security Newspaper | Hacking News. Available at: https://www.securitynewspaper.com/2018/05/03/hack-car-tool/ [Accessed 05 March. 2021].

[10] gen_too (n.d.). Install and Configure Snort 3 NIDS on Ubuntu 20.04 - kifarunix.com. [online] Available at: https://kifarunix.com/install-and-configure-snort-3-nids-on-ubuntu-20-04/.

[11] Hodge, C., Hauck, K., Gupta, S., Bennett, J., Hodge, C., Hauck, K., Gupta, S., & Bennett, J. (2019). Vehicle Cybersecurity Threats and Mitigation Approaches. NREL/TP-5400-74247, 1–41. https://www.nrel.gov/docs/fy19osti/74247.pdf

[12] Joy, J., Rabsatt, V., & Gerla, M. (2018). Internet of Vehicles: Enabling safe, secure, and private vehicular crowdsourcing. Internet Technology Letters, 1(1), e16. https://doi.org/10.1002/itl2.16

[13] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. IEEE Access, 4, 5356–5373. https://doi.org/10.1109/ACCESS.2016.2603219

[14] Lokman, S.-F., Othman, A.T. and Abu-Bakar, M.-H. (2019). Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking, 2019(1).

[15] Nanda, A., Puthal, D., Rodrigues, J. J. P. C., & Kozlov, S. A. (2019). Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. IEEE Wireless Communications, 26(4), 60–65. https://doi.org/10.1109/MWC.2019.1800503

[16] Payne, B. R. (2019). Car Hacking: Accessing and Exploiting the CAN Bus Protocol Car Hacking: Accessing and Exploiting the CAN Bus Protocol. Journal of Cybersecurity Education, Research and Practice, 2019(1), 5.

[17] Prakash, A. (n.d.). Exploiting CAN-Bus using Instrument Cluster Simulator.

[18] Qureshi, K. N., Din, S., Jeon, G., & Piccialli, F. (2020). Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects. IEEE Transactions on Intelligent Transportation Systems, 1–10. https://doi.org/10.1109/tits.2020.2994972

[19] Sadiku, M. N. O., Tembely, M., & Musa, S. M. (2018). Internet of Vehicles: an Introduction. International Journal of Advanced Research in Computer Science and Software Engineering, 8(1), 11. https://doi.org/10.23956/ijarcsse.v8i1.512

[20] Sharma, N., Chauhan, N., & Chand, N. (2018). Security challenges in Internet of Vehicles (IoV) environment. ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications, 203–207. https://doi.org/10.1109/ICSCCC.2018.8703272

[21] Sharma, Sachin, Ghanshala, K. K., & Mohan, S. (2018). A Security System Using Deep Learning Approach for Internet of Vehicles (IoV). 2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2018, 1–5. https://doi.org/10.1109/UEMCON.2018.8796664

[22] Shukla, S., & Holle, J. (2019). Real life experience from implementation of Firewall, Router and IDS Ethernet switch and uC functions Selling mobility instead of cars Autonomous driving Big data.

[23] Smith, C., Starch, N., & Isbn, P. (2016). The Car Hacker 's Handbook (Issue April).

[24] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., Xu, J., & Xiong, Y. (2016). Security and Privacy in the Internet of Vehicles. Proceedings - 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things, IIKI 2015, 116–121.