IMPROVING THE CYBER SECURITY OF NETWORKED CARS USING ARTIFICIAL INTELLIGENCE

Muhamed Ćosić[1], Rudolf Petrušić[1], Vehbi Ramaj[2]
[1]Internacionalni univerzitet Travnik u Travniku
[2]Univerzitet Haxhi Zeka, Kosovo

Review article
https://doi.org/10.58952/nit20231101069

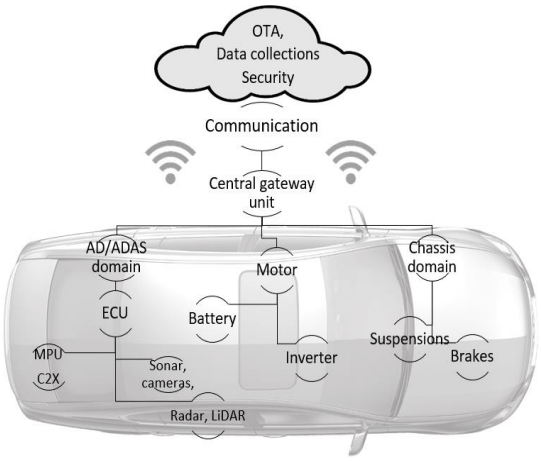
Summary

The automotive industry represents an important segment of the overall industrial development in the world. In order to respond to the ever-increasing demands of customers, the automotive industry tries to keep up with the most modern technologies, and in recent times this primarily refers to information and communication technologies. Software-implemented functions in new vehicles are constantly increasing and are absolutely at the top of all innovations implemented in new vehicles. Thanks to artificial intelligence technologies, new concepts such as self-driving cars are being developed, as well as various driver monitoring systems, road condition monitoring systems, etc. There is an increasing number of artificial intelligence-based systems that enable new vehicles with different functions. The mentioned systems imply the use of a large number of networked IoT devices that exchange large amounts of data. By increasing the degree of networking and information exchange, the number of cyberattacks on vehicles also increases, which affects vehicle safety. Also, proportionally with the increase in the number of such systems, the need for designing security methods, mechanisms, architectures and protocols for detecting and mitigating attacks on car communication grows. This paper presents the challenges of cyber security in the application of artificial intelligence in the automotive industry.

Keywords: *artificial intelligence, automotive industry, cyber attacks.*

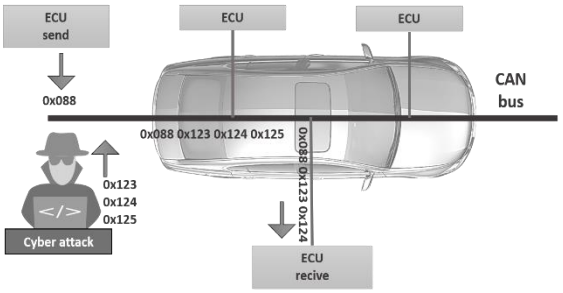
1 INTRODUCTION

The automotive industry is extremely dynamic in terms of the development of new technologies and represents an industry that is always focused on incorporating the latest scientific achievements. More recently, that focus includes computer science, computer networks and information communication technology in general. Today's modern cars are highly dependent on information and communication technology, especially due to the desire to be as connected as possible. Advances in the degree of car connectivity imply new aspects of consumer interest in data security. Consumers want cars that are as safe as possible, not only in terms of the physical safety of passengers, but also the safety of consumer data, which is becoming more and more important every day to maintain trust in car manufacturers. Any lapse in physical or data protection undermines consumer confidence in the car manufacturer. This is why the automotive industry is facing a big challenge because the drive to apply new technologies and more connected cars creates an environment in which the degree of threats and the probability of cyberattacks increase almost on a daily basis. On the one hand, network connectivity enables cars to gain new functionalities, and on the other, it puts the security of data and communications at risk. Modern cars contain a network of electronic control units (ECUs) through which various engine functions are controlled, driving characteristics regulated and monitored in various systems such as e.g. positioning and navigation system. Work is already underway on the implementation of high-performance computing platforms (HCP) in order to be able to integrate greater computing power into the aforementioned ECU modules..



Sheme 1: Example of ECU architecture

ECU modules are interconnected with the CAN bus. CAN Bus is the most well-known and widely used protocol in the automotive industry and is considered the de facto standard for vehicle networks (Avatefipour, et.all. (2019). CAN bus allows ECUs to share information along a common bus leading to improvements in performance fuel and emissions, but also introduced vulnerabilities by giving access on the same network to cyber-physical systems (Abbott-McCune, Shay, 2016).



Scheme 2: Fuzzing attack scenario on the CAN bus

The mass installation and application of ECUs in cars presents a demanding challenge for electrical and electronic architecture, especially for data processing and optimization of network security. Modern cars are also becoming mobile laboratories of the Internet of Things (IoT) as an increasing number of IoT devices are embedded in them. The emergence of IoT has been made possible by the emergence of low-cost computer chips that, due to their

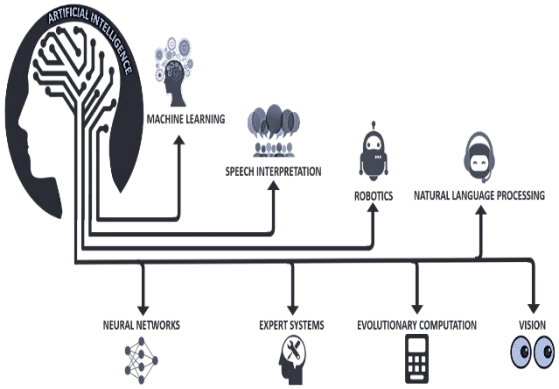
affordability, are embedded in many things, from from simple measuring instruments to complicated medical devices, cars, ships and airplanes (Ćosić, Krnjić, Petrušić, 2022). IoT devices in cars function as complex systems for car connectivity, predictive maintenance, etc. ECU modules as well as IoT devices require programming or appropriate software in order to function correctly. Software is taking more and more control over the various functionalities of modern cars. How sophisticated modern cars are in terms of computer technology is shown by the fact that the number of lines of code in some of them reaches one hundred million. For the sake of comparison, the software in the Boeing 787 aircraft has a total of "only" seventeen million lines of code. The further development of cars implies increasing autonomous driving, which will additionally affect their dependence on computer and information communication technology. Increased connectivity provides new opportunities for malicious actors, as the attack surface increases at the same time, and thus the probability of a cyber attack increases. Cyber attacks are dynamic in nature and are constantly adapting to digital innovations. Any type of cyber attacks can cause serious security issues (Li, Y., et.all. 2018). Due to all of the above, it can be seen that one of the fundamental challenges of the modern automotive industry is the identification of security risks and protection against cyber attacks.

2. ARTIFICIAL INTELLIGENCE AND INTELLIGENT VEHICLES

The term artificial intelligence (AI) describes the ability of a machine to perform operations that typically require human intellect, such as speech recognition, natural language understanding, and decision making (Soori, Arezoo, Dastres, 2023). Artificial intelligence, like no technology before it, is revolutionizing the automotive industry. The development of fourth and fifth level autonomous cars would be unthinkable without the application of artificial intelligence technologies. Also, the functionality provided by modern cars is enabled, among others, by the use of artificial intelligence technologies. Although it has been present since half of the last century, artificial intelligence is only now receiving a lot of publicity in the automotive industry, and the reason for this is the amount of data we have at our disposal today. In modern cars, data is produced from a multitude of sensors, IoT devices, ECU modules, etc. One of the conditions for the application of artificial intelligence is the existence of a large amount of data. The increasingly extensive incorporation of artificial intelligence technologies in the automotive industry consequently leads to structural changes and conditions an increase in investment in applications that are in line with the mentioned technologies. Today, there are a large number of definitions of artificial intelligence, however, the precise definition and meaning of the word intelligence, and even more artificial intelligence, is the subject of many discussions and has caused much confusion. In the literature, it is possible to find definitions that mainly rely on the following four views:

- A field of study in the field of computer science that focuses on the development of computers that would be able to imitate humans in terms of thought processes;
- The concept of increasing the performance of machines to have capabilities similar to human intelligence;
- Enhancing human intelligence through the use of computers, where computers are used as a tool to increase human capabilities;
- In a limited sense, the study of techniques that will enable more efficient use of computer technology.

Sheme 3: Elements of artificial intelligence



The key elements of artificial intelligence are machine learning, artificial neural networks, natural language processing, expert systems, vision, evolutionary computing, robotics and speech interpretation (Scheme 3).

The use of artificial intelligence in the automotive industry is constantly increasing and it is predicted that the level of incorporated systems based on artificial intelligence in new vehicles will increase by 109% in the middle of this century, for comparison it should be noted that in 2015 it was only 8%. Almost all systems in the car have the possibility of improvement using artificial intelligence techniques, especially infotainment man-machine interface systems (speech and gesture recognition, driver monitoring, virtual assistance, etc.) and advanced driver assistance systems (ADAS) as well as autonomous vehicles (computer vision , ECU modules, radar-based detection modules, etc.)

Deep learning technology, which is a technique for implementing machine learning (an approach to achieve AI), is expected to be the largest and fastest growing technology in the automotive AI market. It is currently used in voice recognition, voice search, recommendation engines, sentiment analysis, image recognition, and motion detection in autonomous vehicles. This is precisely why efforts are being made to improve the performance of cameras and various sensors to generate the necessary amount of data to enable deep learning computer vision algorithms for parallel computations.

Autonomous cars are vehicles that are capable of performing the same tasks as those driven by experienced people, but without their intervention. Artificial intelligence techniques enable such vehicles to independently interpret traffic signs, identify obstacles and process all necessary data so that, based on complex algorithms, they can make correct decisions that will result in participating in traffic in a safe manner. Algorithms used in autonomous vehicles use real-life datasets for training and development to develop the necessary decision-making capabilities for the car's behavior in traffic. There are three essential conditions that every car must fulfill in order to be fully autonomous:

1. must have a visibility camera,
2. must have a communication system and
3. it must have sensors.

Fulfillment of the mentioned conditions enables the car to generate the necessary amount of data that will be processed by artificial intelligence techniques, and based on that processing, the functioning of the car in autonomous driving mode is also enabled. Simply put, the role of artificial intelligence in creating the infrastructure for autonomous vehicles is that, based on processed data from the components installed in the car, the autonomous vehicle can ""see, hear, think" and make decisions independently, i.e. show the characteristics of a human driver. Each new ride generates new experiences that are registered and recorded and stored in the database so that in the future these data can be used to make better decisions and to shorten the time needed to make them. In order to enable autonomous vehicles to function properly and safely, artificial intelligence, primarily neural networks and deep learning, is becoming an absolute necessity. Artificial

intelligence systems must be incorporated into autonomous vehicles in order to provide users with the necessary user experience and ensure their safety in traffic.

3. CHALLENGES OF CYBERNETIC SECURITY

Cyber security in the automotive industry is a topic that receives a lot of attention, since cyber attacks not only threaten data, but also human lives. It is precisely for this reason that it is not advisable to rely on the traditional industrial approach to software development activities. Therefore, it is too big a risk to ensure the quality and safety of the product first, while cyber security is secondary. Another evident problem is that competent regulatory bodies often do not have an adequate response when it comes to setting appropriate standards for emerging technologies. The aforementioned regulatory bodies must also face the risky testing of autonomous vehicles on public roads. The mere existence of the threat of cyberattacks, as well as their perception, is enough to weaken confidence in the functioning of new technologies and create an unfavorable social and economic climate for their adoption. Car manufacturers, aware of the fact that connected and autonomous vehicles will become the main target of cyberattacks, are increasingly emphasizing security research that will offer adequate protection against such attacks.

Cybersecurity should be considered an investment for companies, not a cost, especially considering additional factors of personal security such as damage to reputation or trust when a data breach occurs (Sanguino, Domínguez, Baptista, 2020). Attack surface and attack feasibility are significant for networked vehicles due to their additional functions (Jeong, S., et. all., 2021). The effectiveness of defense mechanisms depends on the correct identification of cyber attacks. Thorough and accurate identification of cyberattacks enables quality analysis and definition of security goals, and provides a foundation for designing risk mitigation models. Mitigation techniques generally require setting up authentication systems and misbehavior detection systems (Petit, Shladover, 2015).

Cyber attacks can be classified into three main categories:

1. attacks on the autonomous management system,
2. attacks on autonomous driving components and
3. attacks on vehicle-to-vehicle (V2V)[13] and vehicle-to-everything (V2X)[14] communications.

Based on the aforementioned categorization of attacks, defense models can also be classified into three categories:

1. defense of the security architecture,
2. attack detection and
3. anomaly detection.

In order to function properly, various computer systems, sensors and electronic components are embedded in connected and autonomous cars, and all of them require a high level of cyber security to mitigate security risks. In order to ensure a comprehensive cyber security framework, it is necessary to adopt the best security practices that should be combined with already existing security models and mechanisms. It is very important to focus security mechanisms on possible entry points (ECU modules, wired and wireless networking connections, etc.) that could be primary targets of cyber attacks. Table one shows potential cyberattacks on networked cars with their key features.

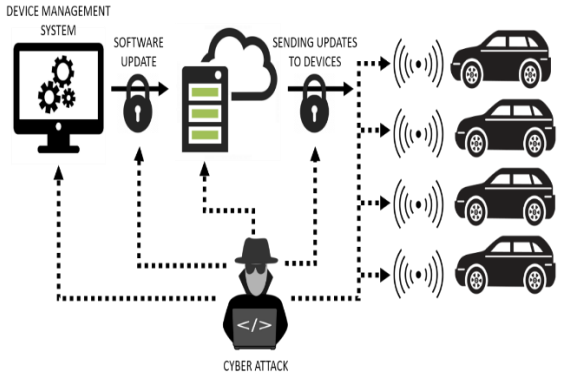
[13] Vehicle-to-vehicle (V2V) communication enables vehicles to wirelessly exchange information about their speed, location, and heading.

[14] Vehicle-to-everything (V2X) is communication between a vehicle and any entity that may interact with the vehicle.

Table 1: Potential cyberattacks on networked cars

FORM OF CYBER ATTACK						
Attack on IoT devices	**OTA updates**	**Attacks on ECU modules**	**DDoS Attacks**	**Attacks on cloud services**	**Car theft and remote kidnapping**	**Ransomware attacks**
GPS jamming and spoofing	Update attacks	External attacks via OBD ports	Termination of service for legitimate users	Exploiting live migration	Wireless car theft	Attack on a vehicle (attacks on car owners)
Attacks on camera sensors, radar, LiDAR, web interface, etc.	A direct attack on the telematic control unit	Attacks on devices connecting to the Internet	Botnets on wheels	The possibility of attacking multiple vehicles at the same time	Cloning keys	Attacks on the supply chain

There is great potential arising from the integration of devices with vehicles, but there are also new threats and vulnerabilities that hackers are trying to use to carry out cyber attacks. So, in addition to traditional attacks such as stealing information and disrupting the operation of cars, as can be seen from Table 1, we also have new forms of attacks such as attacks on IoT, DDoS or remote car theft. Also, due to the need for vehicle networking, there are security risks for the networks to which they are connected. On section xx, a possible scenario of a DDoS attack is shown.



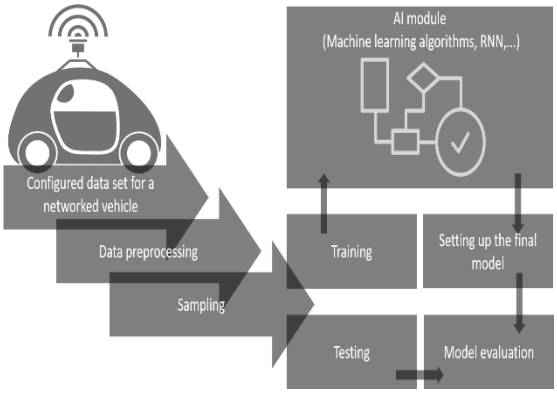
Scheme 4: Possible DDoS attack scenario

One of the possible new threats arises from a new paradigm developed by car manufacturers, which implies mutual communication between vehicles in traffic. This type of communication stems from the need to exchange data and information about various situations that may occur during traffic such as traffic jams, accidents or weather conditions. The Internet of Vehicles enables intelligent cars to exchange messages with other cars, traffic management departments, and companies to analyze vehicle identification data, accident detection, and hazard warnings (Xiao, Wu, Li, 2019). Hackers seek to attack precisely these communication channels in order to compromise data security and use them to inject malicious software. It is precisely because of the existence of the network that hackers' work is made easier because they do not have to have physical access to the vehicles or their individual components. In order to detect these or similar security breaches and reduce the possibilities for carrying out cyber attacks, the so-called layered approach in cyber security. Such a security model implies the identification of priority processes for the protection of critical systems and a quick response to possible incidents that will enable cyber resistance and facilitate the recovery of systems that have been attacked.

4. THE ROLE OF ARTIFICIAL INTELLIGENCE IN CAR CYBERNETIC SECURITY

The automotive industry, faced with an increase in cyberattacks, seeks to provide defensive methods that will prevent or mitigate the possible consequences of such attacks. In order to ensure effective protection measures, there is continuous research in the fields of authentication protocol security and network security, and attack detection methods are also being researched. The application of artificial intelligence techniques has great potential in all the mentioned fields, from attack research to defense mechanisms themselves. Traditional protection models cannot cope with increasingly sophisticated cyber attacks. Security models that combine

traditional protection models, machine and deep learning, artificial neural networks as well as other artificial intelligence techniques can ensure effective protection of vehicles against cyber attacks. The implementation of artificial intelligence techniques in the protection of cars from cyber attacks first of all implies the collection and storage of appropriate data both in terms of quality and quantity. Modern cars are continuously synchronized and updated, and they themselves produce huge amounts of data (connected cars can produce up to 25 GB of data per hour), which is a good assumption for successful analysis using artificial intelligence techniques. Traditional methods without the help of artificial intelligence techniques are not able to sort through all this explosion of data obtained from various sensors, OTA servers, various IoT devices and other components installed in cars. Technologies such as machine and deep learning are necessary for the understanding and quality analysis of such data, through which it is possible to identify the patterns of normal behavior of the system in the car, as well as the timely detection of incident situations. The listed, as well as other artificial intelligence techniques, are capable of timely detecting cyber attacks and activating protection systems that will prevent or reduce possible damage (Scheme 5).



Scheme 5: Cyber attack detection mechanism based on artificial intelligence techniques

Figure 5 shows a possible scenario of cyberattack detection using machine learning and artificial neural networks. The model implies pre-configuration of a set of data for a networked vehicle in terms of settings for methods of collecting and saving user records. Machine learning algorithms are used for the purpose of timely detection of possible incident situations, i.e. anomalies in the collection and storage of data. Due to its nature, the car network is more predictable than a regular computer network, which means that an attack is easier to detect. With machine learning techniques such as unsupervised learning, it is possible to "teach" algorithms to be able to distinguish between normal situations and incident situations, that is, it is possible to train them to detect a cyber attack in a timely manner. The car protection module against cyberattacks must be configured in such a way that it "knows" each individual subsystem in the car in detail in order to be able to perform a separate analysis of each of those systems. In this way, using machine learning algorithms, it is possible to learn normal patterns of data manipulation whether it is data sent from or to the car. Any pattern that deviates from previously learned patterns is detected as an incident situation, that is, it indicates a possible cybernetic attack. A car protection module based on artificial intelligence techniques can have a hybrid architecture consisting of classification models for detecting common variants of malicious software and models for detecting all activities that cannot be qualified as regular. The artificial intelligence module shown in Scheme 5 can use different techniques to detect a cyber attack, and some of these techniques are e.g.:

- k-nearest neighbor,
- modified Bat algorithm
- decision tree,
- long-term short-term memory,
- deep autoencoder methods, etc.

In the event that an anomaly is detected that may indicate a cyber attack, the model implies the execution of two possible steps. The first step is to warn the driver of a possible cyber attack (sound signal, message on the display, etc.) and on the basis of which the driver is given the opportunity to perform the necessary actions to prevent the attack. The second step involves blocking all messages sent by the attacker and isolating the entire system from "harmful" signals and data that the attacker wants to insert into the system. It would also be valuable if complex incidents were broken down into individual steps so that all the necessary attack steps could be reproduced (Sommer et.all. 2019).

CONCLUSION

Artificial intelligence, as one of the most advanced technologies in computer science, finds increasing application every day in all industries, including the automotive industry. The automotive industry is extremely dynamic in terms of the development of new technologies and represents an industry that is always focused on incorporating the latest scientific achievements. Automakers face major intellectual challenges in developing and revising technology. One of the key technologies that can provide an answer to these challenges is artificial intelligence, so the automotive industry is one of the main industries that uses this technology to increase performance in all its segments. The continuous growth of the automotive artificial intelligence market is evident, which is closely related to the growth in demand for autonomous cars and the demand for improved user experience and new functionalities. The automotive industry, faced with an increase in cyberattacks, seeks to provide defensive methods that will prevent or mitigate the possible consequences of such attacks. Artificial intelligence has great potential in ensuring effective protection measures to protect modern car manufacturers from cyberattacks. Many artificial intelligence technologies such as machine learning, artificial neural networks, etc. are becoming an important tool for car manufacturers who want to ensure the safety of their products. With machine learning techniques such as unsupervised learning, it is possible to "teach" algorithms to be able to distinguish between normal situations and incident situations, that is, it is possible to train them to detect a cyber attack in a timely manner. In the end, it can be concluded that one of the most important contributions of the use of artificial intelligence techniques in modern networked cars is that through them it is possible to identify priority processes for the protection of critical systems and a quick response to possible incidents that will enable cyber resilience and facilitate the recovery of systems that have been attacked.

LITERATURE

1. Sommer, F., Duerrwang, J., Kristen, R. (2019), Survey and classification of automotive security attacks, Institute of Energy Efficient Mobility (IEEM), University of Applied Sciences, Karlsruhe, Germany, MDPI Open Access J. 10 (4) (2019) 1–29
2. Li, Y., et all. (2018), Influence of cyber-attacks on longitudinal safety of connected and automated vehicles in ScienceDirecrt, Accident Analysis and Prevention 121 (2018) 148–156.
3. Abbott-McCune, S., Shay, L.(2016), Techniques in hacking and simulating a modem automotive controller area network, 2016 IEEE International Carnahan Conference on Security Technology (ICCST), pp. 1–7
4. Avatefipour, et.all. (2019), An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning, IEEE Access 7
5. Jeong, S., et. all. (2021), Convolutional neural network-based intrusion

detection system for avtp streams in automotive ethernet-based networks, Veh. Communications, Vol. 29, June 2021
6. Martinelli, F., et.all. (2017), Car hacking identification through fuzzy logic algorithms, 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2017, pp. 1–7.
7. Markovitz, M., Wool, A. (2017), "Field classification, modeling and anomaly detection in unknown CAN bus networks," Vehicular Communications, vol. 9, pp. 43–52
8. Alheeti, K. M., Gruebler, A., McDonald-Maier, K. (2017), Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," Digital Communications and Networks, vol. 3, No. 3, pp. 180–187
9. K array, K., et.all. (2018), Attack tree construction and its application to the connected vehicle. In: Koc¸, C¸ .K. (Ed.), Cyber-Physical System Security. Springer, Cham, Switzerland, pp. 175–190
10. Schmittner, C., et. all. (2016), Using SAE J3061 for automotive security requirement engineering. In: International Conference on Computer Safety, Reliability, and Security, pp. 157–170
11. Sanguino TDJM, Domínguez JML, Baptista PDC (2020) Cybersecurity certification and auditing of automotive industry. In: Milakis D, Thomopoulos N, van Wee B (eds) Policy implications of autonomous vehicles, vol 5. Cambridge, Elsevier, pp 95–124
12. Petit, J., Shladover, S. (2015), Potential cyberattacks on automated vehicles, Computer Science, IEEE Transactions on Intelligent Transportation Systems, Volume 16, Issue, 2, p. 546 – 556
13. Pham, M., Xiong K. (2021), A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles, Computer Science, Computer and Security 109
14. Cao Y., et.all. (2019), Adversarial sensor attack on LiDAR-based perception in autonomous driving. In: ACM SIGSAC Conference on Computer and Communications Security. ACM; 2019. p. 2267–81
15. Narain S, Ranganathan A, Noubir G. (2019), Security of GPS/INS based on-road location tracking systems. In: IEEE Symposium on Security and Privacy (SP). IEEE; 2019. p. 587–601
16. Karnouskos, S., Kerschbaum, F. (2018), Privacy and integrity considerations in hyperconnected autonomous vehicles, Proc. IEEE, vol. 106, no. 1, pp. 160–170
17. Xiao, J., Wu, H., Li, X. (2019), Internet of Things Meets Vehicles: Sheltering In-Vehicle Network through Lightweight Machine Learning, Journals Symmetry, Volume 11, Issue 11, p. Xx
18. Soori, M., Arezoo B., Dastres, R. (2023), Artificial intelligence, machine learning and deep learning in advanced robotics, a review, Cognitive Robotics, Vol. 3, 2023, p. 54-70