Complex Engineering Systems as an enabler for security in Internet of Vehicles: The nIoVe approach

Angeliki Zacharaki  
Information Technologies Institute  
Centre for Research and Technology  
Hellas  
Thessaloniki, Greece  
angezach@iti.gr

Ioannis Paliokas  
Information Technologies Institute  
Centre for Research and Technology  
Hellas  
Thessaloniki, Greece  
ipaliokas@iti.gr

Konstantinos Votis  
Information Technologies Institute  
Centre for Research and Technology  
Hellas  
Thessaloniki, Greece  
kvotis@iti.gr

Christos Alexakos  
Industrial Systems Institute  
ATHENA Research Center  
Patras, Greece  
alexakos@isi.gr

Dimitrios Serpanos  
Industrial Systems Institute  
ATHENA Research Center  
Patras, Greece  
serpanos@isi.gr

Dimitrios Tzovaras  
Information Technologies Institute  
Centre for Research and Technology  
Hellas  
Thessaloniki, Greece  
dimitrios.tzovaras@iti.gr

Abstract—Today’s vehicles are increasingly “connected”; there is wireless data exchange with servers, infrastructure and other vehicles. Tomorrow’s vehicles will be automated and autonomous, capable of sensing their environment and navigating through cities without human interference. Therefore, connected and autonomous vehicles come with the cost of a new set of threats pertaining to higher risks of cyber-attacks. A cyber-attack in a Connected Vehicle (CV) can yield high recall costs, loss of property and even jeopardise human safety. Therefore, the need for cyber protection of CVs is becoming paramount. nIoVe introduces a holistic and multi-layered cybersecurity solution for the Internet-of-Vehicles (IoV) by addressing secure-by-design aspects of CVs, along with cyber protection, threat response and attack recovery at vehicle, infrastructure and service/application layer of the whole IoV ecosystem at complex use cases.

Keywords— Security, IoV, Internet of Vehicles, Connected Vehicles

I. INTRODUCTION

Connected Vehicles (CV) are equipped with networking devices and can exchange information flows with other local devices (inside vehicle) or distant servers (e.g. smart city infrastructure). It is expected that in the not too distant future vehicles will be fully automated and will be operated autonomously, meaning that they will be able to sense the nearby physical environment and to navigate through cities without human interference. Connected, as well as autonomous vehicles come with a new set of cyber-security vulnerabilities and higher risks of cyber-attacks. Thus, the need to protect the CVs against cyberattacks is becoming a priority [1].

Modern vehicles are gradually transformed into complex digital platforms that shape the Internet of Vehicles (IoV) [2,3], and interact (on real-time basis) with the transport infrastructure, transport authorities, service providers/third parties, personal devices and other modern ICT components (e.g. IoT devices) that operate in their proximity. In addition, Connected Autonomous Vehicle (CAV) technologies are getting closer to maturity with several demonstrations worldwide; CAVs are capable to sense their environment and navigate with limited or even no human control. Such advances promise enormous potential benefits for the citizens and societies like increased comfort and convenience for passengers, improved road safety, reduced costs, reduction of traffic and parking-related problems, etc. However, the abovementioned benefits and opportunities bring in new cyber-risks and opportunities for cyber-threat actors. New and unexplored attack surfaces are created through these complex & interconnected ICT infrastructures that are exposed to a continuously and fast evolving cyber-threat environment. Specifically, a shared communications network and control infrastructure, relying on internal and/or external vehicle systems, increases the exposure of potential vulnerabilities and the likelihood of cyber-attacks. Specifically, the heterogeneous network architecture of IoV ecosystem includes many types of vehicular communications, for instance includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) of mobile networks, Vehicle-to-Network (V2N) and Vehicle-to-Pedestrian (V2P) communication. The architecture not only includes vehicles and Road Side Units (RSUs), but also other communication devices such as smartphones, IoT sensors, cameras, etc.

Currently, there is not a dedicated scientific field studying the protection of CVs and CAVs against cyber-attacks and thus, the respective research endeavours are limited. For data protection on the other hand, the governmental rules on the protection of personal data, both in EU and USA, apply to any processing of personal data, including those collected from vehicles [4]. Attacks on automobile systems are expected to increase rapidly in the following years due to the rapid increase in connected automobile hardware & software without foundational cybersecurity principles [5]. In 2015 Chrysler recalled more than one million cars after a couple of hackers demonstrated to the magazine WIRED that they could control a Jeep’s system remotely over the internet [6]. The hackers were able to turn the air conditioning and stereo on and off, disable the brakes, and interfere with steering, while the car was being driven. In 2016 and 2017 Tesla vehicles were subject to attack when one of the hackers hacked into the control system for the power supply of a Tesla Model S P85 and modified it, installing autopilot and other software from dual motor Tesla vehicles on its hardware. However, the second threat is to personal data of passengers. In November 2017 Uber reported the theft of data belonging to 57 million of their users. The hackers also gained access to the personal

978-1-7281-3345-4/19/$31.00 ©2019 IEEE

This work has been supported by the EU Horizon 2020 funded project “nIoVe: A novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles”, under grant agreement no: 833742 2020
information of seven million drivers, including approximately 600,000 US driver’s license numbers; anything could be the target of an attack [7].

The nIoVe cybersecurity reference framework for CVs, CAVs and Internet-of-Vehicles (IoV) network provides an enhanced Cybersecurity platform for passengers and Original Equipment Manufacturers (OEMs). This framework is based on a complex system that is able to: a) identify the risks associated with CVs and IoV networks, b) recognise and evaluate suspicious threat patterns with the use of advanced Machine Learning (ML) algorithms, and c) to enable appropriate coordinated mitigation actions in order to address vehicle safety/security and ensure proper performance and data management. Additionally, nIoVe can offer (near) real time detection of anomalies, as well as response against evolving complex cyber-attack and successfully recovery. Furthermore, nIoVe will increase the OEMs readiness level and the effectiveness of the automation of existing cybersecurity services and will open up the cybersecurity ‘blackbox’ to connected and autonomous vehicles. In this context, it will build trust through coordinated assessment but also drive forward security-by-design and privacy mechanisms that are needed to guarantee the smooth and reliable operation of CVs and CAVs.

The paper is structured as follows: Section II presents the major challenges on the security for IoV systems along with the current solutions. Section III describes the proposed system architecture. Finally, conclusions are presented in Section IV.

II. SECURITY CHALLENGES IN IOV SYSTEMS

A. Cybersecurity in CVs, CAVs and Internet-of-Vehicles

The cybersecurity for CAVs can be logically approached on several layers: Vehicle, Connection Infrastructure and Human Factors. The Vehicle layer concerns vulnerabilities applicable to low level sensors essential for correct functioning of vehicle core components such as positioning, inertial measurements, engine control, tyre pressure monitoring, light detection and ranging, infrared vision systems, etc. All these elements are presenting potential attack vectors with vulnerabilities already exposed to security community. For example, GPS spoofing [8], GPS jamming [9], DDoS on Engine Control Unit (ECU) [10], packet injections to TPMS [11], jamming and spoofing of LiDAR sensors’ data [12], etc. On the Connection Infrastructure layer the traditional cyberattacks such as DDoS [13], Phishing and Ransomware [14] are merging with CAVs specific Network protocol attacks [15], Rogue updates [16] and Password & key attacks [17]. Furthermore, connectivity specific attacks such as physical access attacks on OBD port [18] or media systems [19], close proximity attacks on keyless entry and ignition systems [20] or signal jamming [21], and finally remote access attacks through radio [22] or cellular channels [23] are of significant importance to be included in the cybersecurity solution. The last layer, Human Factors, is nevertheless of most crucial importance and is concerning the privacy [24] and behavioural aspects.

In order to face such challenges, nIoVe adapts a multi-layered tooling approach which targets to cover a wide spectrum of threat handling at the above identified layers and further expands it into a two dimensional space in which detection, assessment, response and recovery are addressed in parallel. Each component of the nIoVE platform incorporates layer specific characteristics (Vehicle, Connection Infrastructure and Human Factors) and propagates the analysis to the dedicated tools at the corresponding action stage (detection, assessment, response and recovery).

B. Attacks types in IoV ecosystem

In information security, attacks and threats can be classified into six main categories, including i) spoofing identity, ii) tampering with data, iii) repudiation, iv) information disclosure, v) denial of service, and vi) elevation of privilege.

Specially, IoV environments may get attacked from various of aspects by different methods like jamming, interference, eavesdropping, and so on. Such attacks can have negative effects on the stability, robustness, real-time, security, and privacy of IoV and make it lose the ability to provide effective services, and even cause serious accidents. IoV is characterised of dynamic topology, bandwidth limitations, transmission power limitations, abundant resources, mobile limitation, non-uniform distribution of nodes, perception of data depending on the vehicle trajectory, and other challenges dealing with large-scale networks, making its security defence a very complex task.

The nIoVe framework introduces a Risk Assessment Engine (RAE) allowing the timely and valid detection of most possible threats to the IoV ecosystem. Those engines work together with a knowledge base for recording all types of attacks that have occurred in CVs, CAVs and the IoV ecosystem in order to assess the possible harmful events to the integrated IoV ecosystem.

C. Dynamic and automated Cybersecurity Risk Assessment

The recent survey on the risk analysis, vulnerability and mitigation techniques identification provides risk overview for smart cities [25]. There are five main vulnerability categories also applicable to the IoV environment needed to take into account for threat modelling in order to develop an appropriate and precise risk-modelling framework:

1. Weak software security and data encryption;
2. Use of insecure legacy systems and poor ongoing maintenance;
3. Many inter-dependencies and large and complex attack surfaces;
4. Cascade effects;
5. Human error and deliberate malfeasance of disgruntled (ex) employees.

Several solutions have been proposed in the domain of the risk assessment where only partial automation is achieved. For instance, risk assessment framework [26] in IOT systems had been developed only with periodic risk assessment. The main reasoning for such approach is the limitation on the system knowledge and dynamic adaptation due to the lack of understanding of risk propagation and dependencies between different assets. Another set of manual approaches [27] describing MS STRIDE and DREAD application for risk modelling is also lacking automation characteristic. CAIRIS method [28] is based on the evaluation of the context, goals, boundaries, stakeholders, scope and risk criteria.
In contrast, nIoVe is incorporating a dynamic real-time risk assessment in link with anomaly detection where deep understanding of risk propagation and interdependencies within the network are at its core. In particular, a wider set of multi-faceted anomaly detection analysers and risk receptors are integrated.

D. Cyber-attacks prediction and attribution

Recently, the extensive and rapid growth of intrusion attacks has gained the focus of research community at very large scale where they are trying to defend against attackers [29]. However, without getting insight knowledge of attacks, it is hard to effectively develop mitigation strategies. Several Machine Learning techniques have been widely used for intrusion detection and predictions modelling such as Bayesian Network learning [30], Genetic Algorithm [31], Snort [32], Fuzzy theory [33] and Information Theory [34].

The nIoVe framework combines and attributes the attack propagation by leveraging existing mitigation advisory strategies. Automated risk assessment and decision making upon allowed estimated risk tolerances will enable the nIoVe platform to handle complex situations on attack prediction in IoV environments.

E. Forensic Readiness

Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. Pre-requisite of a forensic operation is the detection of an attack. The proposed solutions of identifying the presence of various attacks are using statistical anomaly detection, on the Arithmetic Mean (AM), Geometric Mean (GM) and Harmonic Mean (HM) [35]. Based on the simultaneous changes between the various means, a security forensics criterion is provided to unravel the existence of an attack. For Internal Intrusion Detection and Protection System (IDDPS), current solutions propose Data Mining and Forensic Techniques to identify the representative SC-patterns for a user. By identifying a user’s SC-patterns as his/her computer usage habits from the user’s current input SCs, the IDDPS resists suspected attackers [36]. A novel approach which consists of two main modules, the Timestamping Tool and the Listening Tool, is used to ensure that the collected log files have not been changed by unauthorized users so can be used as evidence in digital forensics [37].

The nIoVe approach intends to bring forensic readiness in the IoV ecosystem. Our first priority will be to ensure that necessary forensic information can be collected and used as knowledge-base about the cyber attacks in CVs, CAVs and the IoV ecosystem.

F. Vulnerability Information Sharing

Having the timely access to the security information, accident or attack propagation reporting is a key for a successful cyber-defense. The analysis performed on available tools for efficient threat information sharing [38] suggests that we derive from traditional computer security incident response teams (CSIRTs) reporting to a more modern approaches such as TAXII [39], SCAP [40], CWE, CWSS and CEE, all coordinated by MITRE [41]. On the European level, several efforts exist, such as Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) [42], developed by NATO and Collective Intelligence Framework (CIF) created by the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) [43]. Still, according to ENISA report on cybersecurity for smart-cities [44], Europe is still lacking transverse information sharing on threats and incidents between cities and countries specifically regarding the connected infrastructure and CAVs. In addition, there are a lot of initiations and start-ups related to cybersecurity data repositories. A few examples are: 1. the ‘Data Repository for Cybersecurity Research and Education’ [45], which continually adds new data that is responsive to cyber-risk management (e.g., threats, vulnerabilities, consequences), and 2. the ‘RISI Online Incident Database’ [46] for industrial security which includes incidents of a cybersecurity nature that directly affect industrial Supervisory Control and Data Acquisition (SCADA) and process control systems, accidental cyber-related incidents, as well deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations.

The proposed approach utilizes a repository which consists of components to support core functional requirements for data sharing, like metadata indexing, policies & procedures to connect researchers and stakeholders, a centralized interface for request and sharing of datasets, feedback exchanging and participating in collective knowledge activities. Beyond the state-of-the-art, the proposed repository will host knowledge generated by the Co-simulation Tool in the form of simulation testing reports. Those shared results will make possible to provide proactive services related to vulnerabilities assessment and expected penetration testing results based on hypothetical settings. Additionally, to fulfill ENISA recommendations, Shared Threat Intelligence Services will be provided in nIoVe, allowing not only efficient and secure information sharing for cyber security incidents reporting, but also permitting cross-border attack propagation identification and tracking.

G. Threat Predictive Analytics, Monitoring and Detection Intelligence

The most dangerous threats are the ones that are most difficult to discover [47]. Traditionally, the most common methods on successfully detecting malicious content involved signature-based systems, their main functionality being the identification of the digital fingerprint from known threats and its comparison against traffic of corporate networks, in order to find potentially harmful data. This approach may have been sufficient in the past, however nowadays attacks can be sophisticated, targeting specific assets and containing malware that mutates daily, or even hourly [48]. Answering those challenges, anomaly detection-based techniques [49] are capable for complex, little knowledge-based attack identification, but usually fall short in successfully identifying false positives [50]. As such methods can be classified in statistical, rule-based, distance-based, profiling and model-based [51, 52], researchers try to develop better models per category in order to tackle such shortcomings. In this perspective, Artificial Intelligence and Machine Learning can pose very promising results on accurate, real-time anomaly-based threat detection, analysis and prediction, with tech giants such as Google and IBM already integrating AI technologies into their commercial malware detection offerings [53]. Time-to-Detect (TTD) is also a very crucial parameter, with recent research [54] revealing that European companies take 3 times longer to detect cyber-intrusions.
In the proposed framework, the utilization of AI-based classification and incident detection techniques aims at the successful identification of both known and yet-to-be seen strains of malware. Big data analysis includes clustering of known threats on IoV networks, data feature extraction to improve classification (e.g., based on Deep Neural Networks) of newly found anomalies into malicious scripts, memory-based attacks, zero-day malware and potentially unwanted programs. Optimal balance between accuracy of detection (extremely low false-positives) and TTD (early, before-execution-detection in a malware’s cyber kill chain [55]) will be achieved, by combining data from large cyber-attack databases and training ‘normal’ behavior of data exchange through correlation of network traffic, endpoint-device status and contextual data (such as authorization credentials and time-of-access). Also, an intuitive and customizable dashboard offers unique linked data exploration, perception and knowledge extraction for effective cyber-threat assessment. Employing state-of-the-art advances on visual analytics, it will enable the dynamic connection of different datasets with several types of visualization, linked together, so that user selection in one visualization has a direct impact on the others.

H. Incident Response and Recovery Mechanisms

In spite of any adopted intrusion avoidance strategy, it is still possible that intrusions happen. Thus, it is of paramount importance to complete a security protection strategy by including response capabilities able to stop an ongoing attack as soon as possible and limit its impact. Such actions can include a number of response and mitigation techniques, including file removal, process termination, periodic backups, network filtering, and device quarantining [56]. Mitigation action policies are highly dependent on the strictness of their rules. Stringent policies can increase the detection rate and decrease the False Negative Rate (FNR). However, they may also result in an increased false alarm rate, i.e., False Positive Rate (FPR). Too many false alarms may annoy the user into giving up on the product. Thus, security policy design should seek a balance between security and user comfort [57]. Viewing the response activity from an organizations’ point of view, improvements of response capabilities, include more automated reporting and analysis through integration of Security Information and Event Management (SIEM), improved utilization of current enterprise security tools already in place, and better response time [58].

In nIoVe architecture a Response Toolkit will be developed, defining the sets of rules for an adaptable mitigation action prioritization. The toolkit functionalities will be based on: (i) user-oriented balance between security and comfort, by translating passenger’s requirements into information on warning intervals, latency and jamming signals, and (ii) device-level criticality, imposing strictest policies for more vulnerable devices, while forbidding measures that could risk of users. The developed response toolkit will take appropriate response actions, ranging from passive (e.g., notifications) to active (i.e., data packets jamming), while also issuing silent visual cues to the end-users based on evaluated incident meta-data and associated risks (via the risk assessment engine).

I. Trusted Identity and Data Access Management

As CVs and CAVs continue to evolve, increasing the lines of software code needed to control the vehicle and increasing the number of connected devices in the ecosystem, the number of potential security vulnerabilities have also been increasing. Experts at CSIRO, University of New South Wales and Virtual Vehicle Research Center addressed car security using blockchain technology with research suggesting that smart car connectivity should adopt a decentralized model to avoid issues associated with a single point of failure [59]. They propose a system where data can be securely exchanged between vehicles, smart homes, software vendors and others, as well as provide car owner privacy with blockchain technology ensuring proper access control, identity management and data integrity. Moreover, Cube is also developing an autonomous car security platform based on blockchain technologies, deep learning and quantum hash cryptography [60].

The nIoVe framework improves the identity and access management systems by using the distributed ledger technology, named Open Distributed Ledger (ODL) and implement it through blockchain technology. In nIoVe, blockchain will be applied for the secured IoV information system and CV/CAV permission handling but also the timely update of firmwares, patches, etc. Also, through the incorporation of Blockchain-as-a-Service, nIoVe will enable a horizontal secured authentication and authorization mechanisms throughout its various components.

J. Multi-level Interoperability

In IoV ecosystems, interoperability is the ability of different systems and software applications to communicate, exchange data, and use the information that has been exchanged, that can be distinguished in three levels for IoV ecosystem information:

- **Foundational** interoperability allows data exchange between CVs/CAVs, IoT devices without implying anything on the interpretation of the data.
- **Structural** interoperability is a type of interoperability which implies that CV/CAV manufacturers and IoT devices providers exchange a common format for data exchange (i.e., the message format standards) and protocols for communication. This type of interoperability ensures proper interpretation of the data exchanged.
- **Semantic** interoperability is interoperability at the highest possible level, ensuring the ability of two providers to exchange information and to use the information that has been exchanged.
In addition, a fourth level of interoperability which is not technical, but is equally important is the process interoperability, i.e., the set of actions needed for different processes to put in contact two different systems in order to exchange data. Several standards have been defined for IoV (HTTP/HTML, O-MI, O-DF etc.) [61] and yet interoperability remains an issue. This is due to three main factors: 1. the presence of too many standards, which makes it hard for vendors to choose one which will ensure an easy integration with all the other vendors’ software; 2. the fact that many standards are too generic, which can lead to multiple interpretations; and 3. incompatible terminologies, meaning that even if two systems adopt the same standard, they might attribute different meaning to the same words or use different words for the same meaning.

In order to overcome interoperability problems, nIoVe approach provides protected data interconnection links between all needed actors (passengers, citizens, CV/CAV manufactures, IoT devices providers, smart cities, etc.) via secure communication links as well as thrust and identification mechanisms, able to decrease time of process and reaction while drastically increase the efficiency of the relevant actors.

III. NIOVE ARCHITECTURE AND FUNCTIONAL COMPONENTS

The overall technical architecture of the nIoVe approach as well as its major technical elements and their interconnections are illustrated in Fig. 1.
This is a realistic and decentralized solution to be applied in the IoV ecosystem of the CV/CAVs market, in which vehicle manufacturers, IoV ecosystem and beneficiaries may get involved with their own priorities and limitations. To be noted that the nIoVe is multi-layered meaning that its major functionalities are (semi-)automatically adapted to the existing CVs/CAVs specifications & various IoV contexts. The bottom layer of the architecture consists of the IoV Infrastructure, namely the CVs/CAVs and their networks, as well as possible virtualized honeypots operated on vehicles. In the second layer (Secure Communication Layer), the Vehicle Data Collectors (VDC) are dedicated to sensing components build-in the vehicles, while all other data collectors (Intelligent Transport Data & Network Traffic Collectors) coming from the smart-city infrastructure (cameras, meters for traffic, etc.) are used to formulate a secured data transfer channel to serve the higher layers of the architecture. Last but not least, the Blockchain component (Blockchain-enabled Trust Management & Identification Platform) provides a semi-private (consortium-based) Blockchain based on Ethereum in order to provide trust management services like device authentication, user authorization (mainly for admins), data exchange verification, secure software updates and maintenance. This concept has been successfully proposed in other market sectors like consumer electronics for example [62, 63].

The middle part of the diagram illustrates the Security Information and Event Management (SIEM) Platform for IoV, which includes the three core elements of the solution. The first is the ML-Driven Threat Analysis & Situational Awareness which pre-processes all collected data, detects anomalies, perform risk assessment and provide visual analytics services to platform users. The second is the Multi-layer Response Toolkit which takes action whenever an attack is on progress or in regular maintenance processes and finally the third component is the Recovery Toolkit, used to estimate the damage made and to recover data, device and the overall system. More information on the components of the SIEM Platform for IoV are presented in the following sections. Finally, the topmost part of the Fig.1 shows the users, who are the CVs/CAVs and their manufacturers, Industry Cooperation Teams (ICT) and Computer Security Incident Response Teams (CSIRTs), IT administrators, and citizens (passengers & pedestrians).

The ML-Driven Threat Analysis & Situational Awareness is divided into four sub components, the Risk Assessment Engine, the Visual Analytics Suite of IoV, the Anomaly Detector Toolkit an also the pre-processing tool, named Data Cleansing, Fusion and Reduction Toolkit.

IV. CONCLUSION

The proposed cybersecurity multi-layered approach to vehicle cybersecurity reduces the possibility of a successful CV/CAV cyber-attack, and mitigates the potential consequences of a successful intrusion through coordinated response strategies. By putting together, the network information, system architecture, used operating systems and patches, identification of components and configurations of service applications, data and data-storage, a common IoV wide knowledge network will be established. This will enable efficient and precise attack attribution and propagation identification and intelligence sharing among CV/CAV stakeholders including cyber-response teams, vehicle manufacturers, transport operators and authorities at local, national and world-wide level. The advanced nIoVe cybersecurity framework aims to provide a concrete security and privacy solutions in connected-autonomous vehicles and IoV ecosystems. This framework, will consist of: a) the core nIoVe toolkit (i.e. a Threat Intelligence Monitoring Platform driven by Machine Learning technologies, a multi-layered and coordinated response toolkit, a recovery toolkit, a trust management and accountability reinforcement platform, a threat intelligence repository); and b) a reference architecture along with a set of secure-by-design guidelines and methodologies for OEMs.

The next step after implementation of nIoVe is the validation of the proposed technology and the cybersecurity framework through demonstrations. Those demonstrations will be targeted to CAVs infrastructure and IoV network pilot sites with the participation of technical partners, OEMs manufacturers, experts, etc. Pilots will be supported by existing cybersecurity architectures and methods, which will be classified according to the preferable operation mode.

REFERENCES

[1] J. Contreras-Castilo, S. Zeadally, and J. A. Guerrero-Ibanez “Internet of vehicles: Architecture, protocols, and security”. IEEE Internet of Things Journal, vol. 5(5), 2017, pp. 3701-3709, doi: 10.1109/JIOT.2017.2690902.

[2] F. Yan, W. Shangguang, L. Jinglin et al. “An overview of internet of vehicles”. China communications, vol. 11(10), 2014, pp. 1-15.

[3] M. Gerla, L. Eun-Kyu, P. Giovanni, and L. Uichin “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds”. In Internet of Things (WF-IoT), IEEE World Forum on, 2014, pp. 241-246.

[4] Regulation (EU) 2016/679 of the European Parliament an of the Council, “on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, Official Journal of the European Union, 2016, Available at: https://tinyurl.com/yyppyvdku.

[5] McAfee Labs Threats Reports, December 2018, Available at: www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2016.pdf

[6] V. Baum “How to avoid cyber-attacks to connected vehicles?”, Medium, 2018, Available at: https://medium.com/driving-to-the-future/how-to-avoid-cyber-attacks-to-connected-vehicles-16a8011ba7eb3

[7] A. Balakrishnan, and B. Deirde “Uber hid a hack that exposed data of 57 million users and drivers for more than a year”, CNBC on-line, 2017, Available at: https://www.cnbc.com/2017/11/21/uber-hack-exposes-data-of-57-million-users-and-drivers-report-says.html

[8] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful GPS spoofing attacks”, 18th ACM conference on Computer and Communications Security (CCS’11), 2011, pp. 75-86.

[9] G. P. Hancke “Security of embedded location systems”, Secure Smart Embedded Devices, Platforms and Applications, 2014, pp. 267–286.

[10] Koscher K., A. Czeskis, F. Roesner et al., “Experimental security analysis of a modern automobile,” in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 447–462.

[11] A. Wright, “Hacking cars,” Communications of the ACM, vol. 54(11), 2011, pp. 18–19, doi: 10.1145/2018396.2018403.

[12] B. G. Stottelaar “Practical Cyber-Attacks on Autonomous Vehicles”, 2015, Master Thesis, University of Twente, Available at: http://essay.utwente.nl/66766/

[13] A. Pathre, “Identification of malicious vehicle in VANET environment from DDOS attack,” J. Global Res. Comput. Sci., vol. 4(6), 2013, pp. 30–34.

[14] FireEye, “Connected Cards: the Open Road for Hackers”, 2016, Available at: https://tinyurl.com/p3rzeln

[15] U. E. Larson, D. K. Nilsson and E. Jonsson, “An approach to specification-based attack detection for in-vehicle networks,” in Proc. IEEE Intelligent Vehicles Symposium, 2008, pp. 220-225.
[61] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris, “Smarter cities and their innovation challenges,” Computer, vol. 44(6), 2011, pp. 32–39.

[62] I. Paliokas, N. Tsoniotis, K. Votis, and D. Tzovaras « Trustworthy Blockchain Technology Platform in Connected Consumer Oriented Medical Devices Environments”. IEEE Consumer Electronics Magazine, col. 8(4), 2019, pp. 50-55, doi: 10.1109/MCE.2019.2905516.

[63] D. Pathal, N. Malik, and S. P. Mohanty, “The blockchain as a decentralized security framework,” IEEE Consum. Electron. Mag., vol. 7(2), 2018, pp. 18–21.