Secure Multi-access Edge Computing Assisted Maneuver Control for Autonomous Vehicles

Andrea Tesei*†, Marco Luise*, Paolo Pagano† and Joaquim Ferreira‡
*Department of Information Engineering
University of Pisa
Via G. Caruso 16, 56122 Pisa, Italy
Email: andrea.tesei@phd.unipi.it, marco.luise@unipi.it
† National Inter-university Consortium for Telecommunication (CNIT)
Via Moruzzi 1, 56124 Pisa, Italy
Email: andrea.tesei@cnit.it, paolo.pagano@cnit.it
‡Institute of Telecommunications
University of Aveiro
Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
Email: jjcf@ua.pt

***Abstract*—The sensing capabilities of smart vehicles are growing and enabling unprecedented functionalities that drive the future commercial adoption of autonomous vehicles. However, the real-time requirements of mission-critical vehicular applications are revealing the current limitation of Vehicular Ad-hoc Networks (VANETs). In this scenario, computing paradigms like Vehicular Edge Computing (VEC) are promising solutions to match low-latency requirements. However, there still exist security challenges that need to be addressed to assure safe and secure autonomous driving deployment. We propose in this paper a secure architecture based on the VEC cloud paradigm that enables the deployment of real-time and mission-critical autonomous driving applications at the edge of the network. We leverage the IOTA-VPKI vehicular security scheme to support the security lifecycle of vehicular applications. Furthermore, we describe a Cooperative Autonomous Driving Maneuver Control application to discuss the effectiveness of the proposed architecture in the cooperative lane change use case. We plan to extensively test this architecture in real environments located in Italy and Portugal and to contribute to the future successful deployment of autonomous vehicles.**

***Index Terms*—Autonomous Driving, Vehicular Edge Computing, Vehicular Ad-hoc Networks, Vehicular Public Key Infrastructure, Security**

I. Introduction

The evolution of the automotive industry in the last century gave birth to a new generation of vehicles capable of unprecedented functionalities. Such advanced features definitely transformed the traditional vehicle from an old-fashioned mechanical system into a full-scale, smart, connected, and computational equipped machine on the move [1]. Indeed, the incorporation of information and communication technology within vehicles and transportation infrastructure contribute to enhancing road safety, vehicle ease of use and convenience, and drivers' Quality of Experience (QoE). These smart cars have powerful on-board computing capabilities which are located in cameras, embedded systems, sensors, and Advanced Driver-Assistance Systems (ADAS) to name a few. Thanks to this computing power those cars support features such as sensing the surrounding environment, making quick and timely decisions, navigating without human intervention, and performing maneuvers autonomously. Such cars are referred to as autonomous cars: an autonomous car is in fact a computer-controlled car that can guide itself, interact with surroundings, make decisions, and fully operate without any human input [1]. The emergence of autonomous cars is firstly related to the increase in the number of vehicles: according to World Health Organization (WHO), there are more than 2 billion registered vehicles around the world, and a total of 1.35 million people dying each year on the world' roads [8]. If we consider also the human population grows, the impact on transportation infrastructure, traffic congestion, accidents, and pollution become unmanageable without the deployment of cutting-edge technologies. Among the efforts to improve this situation, Vehicular Ad Hoc Networks (VANETs) used in Intelligent Transportation Systems (ITS) provide essential connectivity to support connected and autonomous cars [2]. The sketch in Figure 1 depicts the complete environment. The ITS infrastructure is mainly composed by *On-Board Units* (OBUs) installed in vehicles, and *Roadside Units* (RSUs) deployed on the road. Those computational entities provide connectivity to vehicles through vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. Considering also the urban scenario, pedestrians enter the game with pedestrian-to-vehicle (P2V) and vehicle-to-pedestrian (V2P) communications. Finally, registration and management authorities are needed to enroll and authenticate vehicles in the system, as well as authorize them to use applications developed by service providers.

The presence on-board of such computational and sensing capabilities enable the typical set of application and services provided by the VANET technology, such as accident warning, real-time alerts of collisions, overtaking, ambulance approaching, road works, traffic information, cooperative cruise control,

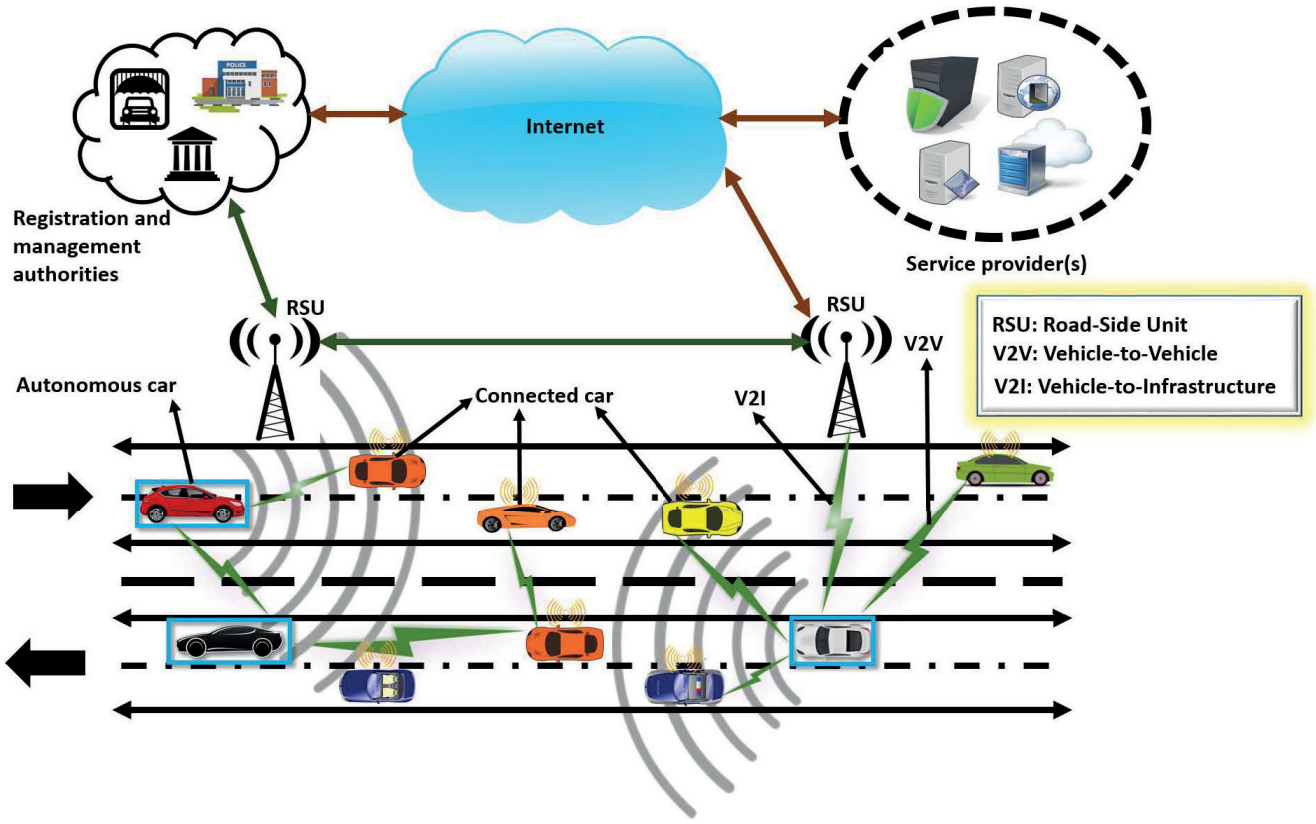

Fig. 1. Autonomous and connected car communication environment. [1]

and maneuver control. Other new and popular applications that are emerging are the ones based on artificial intelligence, augmented reality (AR), image-aided navigation, and intelligent vehicle control, to name a few. However, such applications demand massive computation resources, and still have critical deployment issues and latency requirements [3], [4]. Furthermore, the number of sensors installed in these smart cars is growing: this will generate an enormous amount of data in the future. Consequently, the computational power needed to analyze data from future vehicles will contribute to the exhaustion of the vehicle' on-board resources [2]. The deployment of powerful processors such as Graphics Processing Units (GPUs) can match this demand, but the negative impact on vehicle' energy consumption (e.g. fuel efficiency and driving range) classify this solution as infeasible with the current GPU technologies.

Computing paradigms such as Cloud Computing are promising solutions to match the future computational resource needs of connected and autonomous vehicles. Besides, Cloud-based architectures introduce other issues related to long latency and massive data transmission. In the VANET environment, this latency depends on the condition of the wireless channel, network bandwidth, and traffic congestion [2]. In this scenario, the applications with real-time processing and reliability requirements cannot be deployed safely. Consequently, the deployment of such Cloud-based approaches is thus limited to not real-time and heavy processing tasks. To overcome these issues, a promising approach is to deploy computing resources at the edge of the wireless network. This approach enables the delivery of cloud resources at the edge of the network, thus supporting delay-sensitive applications with low-latency requirements. The solution to delegate tasks to Cloud resources available at the different network levels is called *computation offloading*. This technique consists of dividing an application into different tasks to be sent and executed on other devices that may be idle or underutilized [5]. Computation offloading can be classified as *static* when the task delegation is defined before execution, or as *dynamic* when the delegation decision is made at run-time based on several aspects also related to the current network condition, mobile devices, and remote servers.

As discussed by De Souza *et al.* in [2], there exist different types of clouds based on the level of the network where the remote execution environment is deployed. Vehicular Cloud (VC) corresponds to a pool of vehicular computing resources that can be dynamically coordinated through V2V connections. The EDGE refers to the set of edge servers attached to RSUs or base stations, thus in the vicinity of streets, avenues and roads. Finally, Traditional Cloud (TC) refers to a set of large-scale centralized data centers that are available in the facilities of a cloud provider. Based on the conjunction of these cloud types, different cloud paradigms were recognized: Vehicular Cloud

Computing (VCC) refers to the usage of VC and TC together; Vehicular Edge Computing (VEC) concerns to the usage of VC and EDGE together; finally, Vehicular Fog Computing (VGC) uses all three types of cloud described above, i.e. VC, Edge, TC. Based on the available cloud paradigms, computation offloading can be done in the different cloud layers available, thus supporting real-time and mission-critical vehicular applications like the ones related to autonomous driving discussed earlier.

Despite the significant advantages of computation offloading in the autonomous driving scenario, there are still important challenges and open issues. Among them, two of the major factors impeding the deployment of the autonomous car are security and privacy [1], [11]. Data sharing among vehicles and with the infrastructure is the cornerstone of connected and autonomous car deployment. In this scenario, different aspects are fundamental including, but not limited to, quality of data shared, the integrity of the data, prevention of unauthorized data access, mitigation of external signal spoofing or jamming during communication, promptly revocation of misbehaving vehicles. With the computation offloading technique in place, the scenario is even worst because sensitive data can be sent to untrusted servers for execution, thus augmenting the whole attack surface.

A. Contribution of this paper

This paper proposes a secure architecture compatible with the Vehicular Edge Computing (VEC) cloud paradigm that enables the deployment at the edge of the network of real-time and mission-critical applications. The proposed architecture guarantees the security of each application-specific communication exploiting IOTA-VPKI architecture [6], [7], which deploy at the edge different Trusted Authorities (TAs) that are entitled to authenticate, enroll, authorize, and eventually revoke vehicles. To this end, each component of IOTA-VPKI architecture is deployed as Multi-access Edge Computing (MEC) App thus minimizing issuing certificate and revocation checking latency. This secured architecture mitigates security issues and threats described above and guarantees a lower time vulnerability window compared to the latest US and EU standards, as demonstrated in [7]. For the sake of completeness, a Maneuver Control application for autonomous vehicles is considered as a sample mission-critical vehicular application deployed at the edge to better discuss the proposed architecture and the different secured messages that can be exchanged.

The rest of the paper is organized as follows: Section II addresses relevant related work, while Section III provides a detailed description of the proposed scheme, and outlines Maneuver Control use cases relevant for the discussion; finally, Section IV concludes the paper with a brief description of future works.

II. Related Work

As discussed in previous Section I, the number of vehicles registered worldwide is growing, and the evolution of autonomous driving is gathering a lot of attention both from industrial and research point of view. There are several works available in research that address the decision-making process that is essential for the real deployment of such autonomous vehicles. For example, anomaly detection for Cooperative Adaptive Cruise Control (CACC) is presented in [16]. The authors focused their analysis on the presence of a compromised platoon leader which can expose the system to serious security threats. AutonoVi is presented in [17] as a novel algorithm for autonomous vehicle navigation supporting dynamic maneuvers with traffic constraints and norms. This work focused on the analysis of optimization technique and data-driven vehicle dynamics modeling, without mentioning any communication security-specific mechanism.

Considering the exploitation of Edge Computing in vehicular applications, computation offloading is gaining momentum within the research community. A Fog computing based framework to assist autonomous driving is proposed in [12]. The authors described a new concept of distributed digital twins, called edge twin, that is created using overhead views from cameras and data streams from vehicle sensors. The fault-tolerant property of the system is also discussed in the case of fog and camera failures. Another interesting approach is discussed in [14], where a distributed LiDAR sensors network is installed on roadside lamp posts for sharing data among passing vehicles. This approach avoids installing expensive sensors on each vehicle and leverages Edge servers to process sensor data into environment maps used by autonomous vehicles. In [15], the authors presented ECASS, an auxiliary sensing system that leverages edge computing to locate nearby vehicles for self-driving vehicles. Despite the interesting approach, this work focused the analysis on the nearby vehicle detection and localization when autonomous vehicles are partial or even completely blocked by trucks or buses. An interesting work that focuses the analysis on the VEC security is presented in [13]. The authors described a secure communication scheme for VEC applications based on decentralized attribute-based encryption (ABE). However, the proposed scheme does not cover any revocation mechanism and is focused on key management, ABE-based secure data collection, and processing result dissemination.

The aforementioned research works provided advanced techniques for the decision-making process in autonomous driving but lack security schemes that consider the different attacks and threats to which the autonomous driving systems are exposed. Our VEC-based security architecture provides a comprehensive approach that covers the full security lifecycle of vehicular applications (i.e. authentication, authorization, misbehavior detection, and revocation). Furthermore, it is compatible with the latest EU and US standards thus applicable in real vehicular environments.

III. Proposed Scheme

The emergence of real-time applications that enable and support the deployment of autonomous vehicles motivates the design of new vehicular secure infrastructures that support low latency communications. The security challenges described

in Section I need to be addressed with secure architecture that guarantees the minimum vulnerability window, thus maximizing the security level. In the subsequent subsections, the Multi-access Edge Computing (MEC) based architecture is presented, and the details of MEC-enabled IOTA-VPKI security mechanism enforcement is described. Furthermore, different autonomous driving Maneuver Control use cases are outlined to discuss how to deploy on the edge of the network a secured mission-critical vehicular application.

A. Secured Vehicular Communications: IOTA-VPKI

Firstly presented in [6], IOTA-VPKI is a Vehicular Public Key Infrastructure (VPKI) fully compatible with EU and US standards that leverages Distributed Ledger Technology (DLT) to transparently store issued certificates, VPKI management events, and revocation information. Besides the compatibility of IOTA-VPKI with every DLT implementation that supports immutable data storage, IOTA was used to test the effectiveness of the proposed scheme [7]. IOTA DLT leverages a Direct Acyclic Graph (DAG) ledger fashion, which enables devices with small resource capacity to issue new transactions and thus participating in the system. In the IOTA-VPKI scheme, each vehicle accesses the IOTA network with a secured connection with the nearest neighbor IOTA Reference Implementation (IRI) node.

Generally speaking, the latest version of IOTA-VPKI architecture described in [7] is composed of different Trusted Authorities (TAs) that are entitled to authenticate, enroll, authorize, and eventually revoke vehicles. As the trust anchor of the whole VPKI, the Root Certificate Authority (RootCA) authorizes both Long Term Certificate Authority (LTCA) and Short Term Certificate Authority (STCA) for issuing certificates to vehicles. The LTCA is thus entitled to enroll vehicles in the system issuing Long Term Certificates (LTCs). The STCA is in turn responsible for issuing Short Term Certificates (STCs) which authorize the vehicles to access system applications. Finally, beyond the current EU and US standards, the Misbehavior Authority (MA) performs misbehavior detection and reports for vehicles to be revoked from the system to Revocation Authority (RA) which resolve vehicle identity and exclude it from the system. Hence, the IOTA-VPKI architecture implements new functionalities in MA and RA which enable a general-purpose, transparent, and privacy-aware active revocation mechanism. This novel revocation technique leverages DLT to store and distribute revocation information in a short time, thus supporting also applications with low-latency requirements.

However, the V2I communications between vehicles and IOTA-VPKI components exploit wireless communication, thus the corresponding delay is dependent on several aspects related to wireless channel condition, network available bandwidth, and traffic congestion. To mitigate this dependability, we redesign each IOTA-VPKI component instance in such a way that it can be independently deployed at the edge of the network, exploiting Multi-access Edge Computing standards. In this way the delay introduced by wireless media become negligible, and the IOTA-VPKI architecture enhances support to mission-critical application with real-time requirements.

The result of IOTA-VPKI deployment at the edge is depicted in Figure 2. The complete details of the proposed MEC-based architecture will be discussed later in Section III-B. Each TA is deployed as a single MEC Application via the Mp1 reference point. This particular standard interface connects the MEC platform with the MEC applications and provides service registration, service discovery, and communication support for services [9]. In turn, the inter-TAs communication that are defined by the US and EU standards are enabled by MEC Platform Service via logical network connection between different MEC Apps.

As discussed in Section II, the related works available in research lack security schemes that cover secure communications between autonomous vehicles and infrastructure. Thus, we can assume that they exploit a standard security scheme, namely a signcryption scheme that employs certificate revocation *by expiry*. This means that when the system recognizes a malicious vehicle it will remain trusted in the system for a long time. In fact, considering the latest EU security policy the maximum certificate validity period can be greater than 1 month with certificate pre-loading [7]. The resulting vulnerability window is not compatible with real-time autonomous driving applications. IOTA-VPKI implements *active* revocation mechanism, thus supports promptly malicious vehicle exclusion from the system thus matching real-time requirements.

All in all, the new architecture remains compatible with standard vehicle OBU software/hardware. Similarly, the new delivery model of IOTA-VPKI components continues to be compatible with the current US and EU standards. Furthermore, this new deployment strategy maximizes the applicability of the proposed scheme to the majority of the vehicular applications available in the market.

B. Mission-critical Vehicular MEC Apps Architecture

The proposed secure architecture that enables the mission-critical vehicular applications deployment on the edge of the network is depicted in Figure 2. The Edge Controller, also known as MEC Platform Manager [9], handles the management of MEC specific functionality and the applications running on available EDGE nodes. In turn, the EDGE Node, also known as MEC Host, contains the MEC Platform Services which serves essential functionality required to run MEC Applications. The communication between EDGE Controller and MEC Platform Services is enabled via the Mm5 standard reference point. This interface is used to configure the MEC Platform with specific application rules and requirements, as well as to perform application relocation when needed. In turn, when multiple EDGE Node is available, the Mp3 standard reference point enables the connection between different MEC Platform Service instances for control communication.

Thanks to the proposed architecture, every mission-critical vehicular application can be deployed at the edge of the network exploiting a common containerization technique [10],

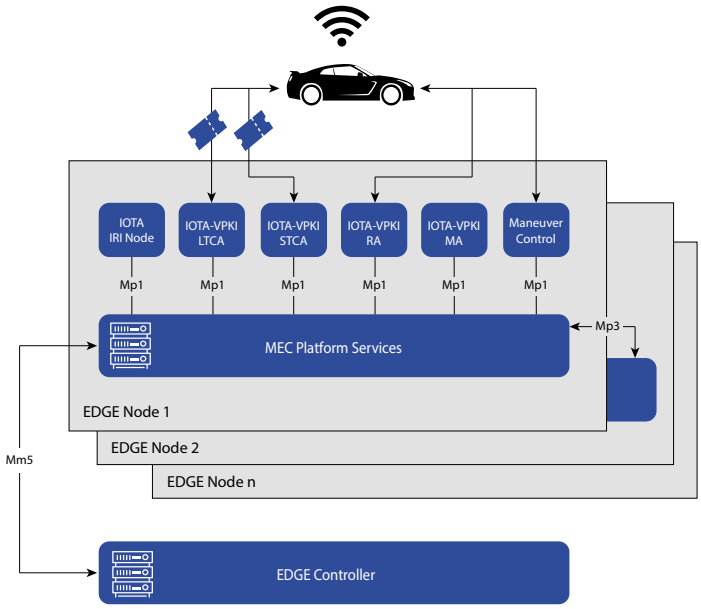

Fig. 2. Secured Architecture for Vehicular MEC Applications.

and uploading the application package to the EDGE Controller. In turn, the EDGE Controller will verify the application requirements to deploy the MEC Application to the most suited EDGE node among the ones available. Furthermore, the vehicular MEC application needs to enforce any client to provide a valid credential issued by IOTA-VPKI for each communication. The implementation of this security mechanism in each mission-critical vehicular application mitigates and lowers the exposure of the system to security issues and threats introduced in Section I. Furthermore, the Revocation Authority (RA) component can immediately exclude from the system any vehicle that is recognized to be misbehaving. This enables mission-critical vehicular applications to run in a system with very short vulnerability window compared with latest US and EU standards, as discussed and demonstrated in [7].

C. Cooperative Autonomous Driving Maneuver Control

A successful deployment of autonomous driving depends on the evolution and reliability of decision-making techniques. Decision making in increasingly complex and uncertain environments is the cornerstone of autonomous cars [1]. The advanced car' sensing capabilities prioritized decision-making approaches that focus on cars' local environment, also referred to as "ego-vehicles" approaches. With the progress of vehicular networks, the fusion of local sensing environment with the information about the surroundings coming from vehicular infrastructure has gathered much attention from the research perspective. In this sense, connected car technology will play an essential role in the deployment of autonomous car in the future. An ideal autonomous car will be able to mimic human behavior and this is possible only with the consideration of the surroundings together with the local car environment.

Cooperative Autonomous Driving is a promising approach that considers both local and surrounding environments. Shahzadi *et al.* in [11] divided Cooperative Autonomous Driving into two categories: cooperative sensing and cooperative decision. Cooperative sensing leverage V2V and V2I communications to share sensing information. Cooperative decisions create a collaborative group of autonomous vehicles that make decisions according to the different environments local to the autonomous cars participating in the group. The Cooperative Autonomous Driving approach enables different use cases including, but not limited to, convoy driving, cooperative lane change, cooperative intersection management, and cooperative sensing. However, the security of information and attack protection are essential aspects to be addressed for safe and reliable deployment of such use cases [1].

We focus our study on the cooperative lane change use case. We describe the issues and challenges of this cooperative autonomous driving maneuver, with particular reference to the security of communications. Considering the current US and EU Intelligent Transportation Systems (ITS) standards, connected vehicles periodically broadcast beacon messages that contain position, direction, speed, and other data about the sender vehicle. This message is known as Cooperative Awareness Message (CAM) in the ETSI EU standards. When a particular warning situation arises in the field, a specific environmental notification message is broadcasted to the cars approaching the dangerous position. This message is known as the Decentralized Environmental Notification Message (DENM) in the ETSI EU standards. When a connected vehicle receives such messages, its actuators are triggered to take a specific action that mitigates environmental risks. Our Maneuver Control MEC App implements cooperative lane change use case analyzing the information in the CAM messages, and eventual notifications of lane blocks carried by DENMs. Furthermore, the Maneuver controller automatically generates the sequence of actions to be taken to perform a lane change minimizing the risks of accidents. This is done for each vehicle registered in the Maneuver Control application. The vehicle registration is done exploiting IOTA-VPKI security architecture. Each V2V and V2I communication between vehicles and Maneuver Control application will be signed and eventually encrypted using public-key cryptography. In this way, our scheme guarantees the privacy and security of communication and can perform revocation in real-time in the case of misbehaving or malicious connected vehicles. Any connected or autonomous vehicle that broadcasts false or malicious messages can degrade the decision-making process made by the Maneuver Control app. In such cases, it is essential to have the lowest vulnerability time window to enhance the safety and security level of the whole system.

IV. Future Work and Conclusions

In this paper we propose a novel secure architecture that leverages the Vehicular Edge Computing (VEC) cloud paradigm to enable the deployment at the edge of the network of real-time and mission-critical autonomous driving applications. Starting from our previous work on IOTA-VPKI [7] we decomposed its architecture in different MEC-deployable

applications to deploy IOTA-VPKI' Trusted Authorities (TAs) at the edge of the network. To complement our proposal, we described the Cooperative Autonomous Driving Maneuver Control use case related to cooperative change lane. We described the details of such use case with particular reference to the secured messages exchanged. We exploited the IOTA-VPKI signcryption scheme compatible with US and EU standards to protect the communication between Maneuver Control application and vehicles. IOTA-VPKI Revocation Authority (RA) guarantees promptly exclusion of recognized misbehaving and malicious vehicles from the system. This assures a lower vulnerability time window and the minimum impact on the decision-making process made by the Maneuver Control application.

As future works, we plan to deploy and test this scheme in a protected environment to demonstrate the effectiveness of the architecture and to measure the time vulnerability window. The test sessions will be executed in two real testbeds: the first available in Livorno (Italy) seaport, with the possibility to execute test sessions also on the highway; the second in Smart City context at Aveiro (Portugal). Leveraging real test sessions and these pilot sites we will demonstrate the effectiveness of the proposed architecture, contributing with a step forward towards the successful deployment and adoption of autonomous driving.

REFERENCES

[1] R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges" in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1275-1313, Second quarter 2019.

[2] A. B. De Souza et al., "Computation Offloading for Vehicular Environments: A Survey" in IEEE Access, vol. 8, pp. 198214-198243, 2020.

[3] Boukerche, Azzedine, and Victor Soto. "Computation Offloading and Retrieval for Vehicular Edge Computing: Algorithms, Models, and Classification." ACM Computing Surveys (CSUR) 53.4 (2020): 1-35.

[4] Liu, Yujiong, et al. "Dependency-aware task scheduling in vehicular edge computing." IEEE Internet of Things Journal (2020).

[5] Rego, P. A., Costa, P. B., Coutinho, E. F., Rocha, L. S., Trinta, F. A., and de Souza, J. N "Performing computation offloading on multiple platforms." Computer Communications 105 (2017): 1-13.

[6] A. Tesei, L. Di Mauro, M. Falcitelli, S. Noto and P. Pagano, "IOTA-VPKI: A DLT-Based and Resource Efficient Vehicular Public Key Infrastructure," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-6.

[7] A. Tesei, D. Lattuca, P. Pagano, M. Luise, J. Ferreira, & P. C. Bartolomeu. "A Transparent Distributed Ledger-based Certificate Revocation Scheme for VANETs." arXiv preprint arXiv:2010.13555 (2020).

[8] "World Health Organization. (2021). Road Safety.". [Online]. Available: https://www.who.int/data/gho/data/themes/road-safety

[9] ETSI, GS. "MEC 003 v2.2.1-Multi-access Edge Computing (MEC); Framework and Reference Architecture." Group specification, European Telecommunications Standards Institute (2020).

[10] M. Alam, J. Rufino, J. Ferreira, S. H. Ahmed, N. Shah and Y. Chen, "Orchestration of Microservices for IoT Using Docker and Edge Computing," in IEEE Communications Magazine, vol. 56, no. 9, pp. 118-123, (2018)

[11] Shahzadi, S., Iqbal, M., Dagiuklas, T. et al. "Multi-access edge computing: open issues, challenges and future perspectives." Journal of Cloud Computing 6.1, 30 (2017).

[12] M. Maheswaran, Y. Tianzi, and M. Salman. "A fog computing framework for autonomous driving assist: architecture, experiments, and challenges." Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering. 2019.

[13] Cheng, Cheng-Yu, et al. "Attribute-Based Access Control for Vehicular Edge Cloud Computing." 2020 IEEE Cloud Summit. IEEE, 2020.

[14] P. -Y. Kong, "Computation and Sensor Offloading for Cloud-Based Infrastructure-Assisted Autonomous Vehicles" in IEEE Systems Journal, vol. 14, no. 3, pp. 3360-3370, 2020.

[15] Wang, Xiong, et al. "ECASS: Edge computing based auxiliary sensing system for self-driving vehicles." Journal of Systems Architecture 97 (2019): 258-268.

[16] Alotibi, Faris, and Mai Abdelhakim. "Anomaly Detection for Cooperative Adaptive Cruise Control in Autonomous Vehicles Using Statistical Learning and Kinematic Model." IEEE Transactions on Intelligent Transportation Systems (2020).

[17] Best, Andrew, et al. "Autonovi: Autonomous vehicle planning with dynamic maneuvers and traffic constraints." 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). IEEE, 2017.