Vehicular Cloud: Overview and Security Issues

Lucian Gafencu
Department of Telecommunications and Information Technologies
Technical University "Gheorghe Asachi"
Iaşi, Romania
lucian.gafencu@etti.tuiasi.ro

Luminița Scripcariu
Department of Telecommunications and Information Technologies
Technical University "Gheorghe Asachi"
Iaşi, Romania
lscripca@etti.tuiasi.to

***Abstract* — Vehicular communications, from inter and intra-vehicle communications, up to the newer paradigms of Vehicular Cloud, have been a research topic which was closer to reality than many other topics. The weak implementation of Vehicular Ad-Hoc Networks (VANETs) due to the lack of standardization and commercial interest have consisted a basis for future research and implementations. Vehicular Cloud applications are now a reality (Apple CarPlay, BMW Connected Drive) and are expanding at an exponential rate. Also, the power of the many sensors and components in cars nowadays, are giving the opportunity to send important data about the driving experience, road safety issues and facilitate the use of applications for the people in cars. Of course, with the more information being sent, the more the opportunities for hackers to retrieve sensitive data. Security is one of the most important features, because not only data can be lost, but human lives are at stake, because of the autonomous facilities implemented. This paper, presents a brief overview of the concepts in Vehicular Cloud, with an accent placed on security aspects. Vulnerabilities and threats are presented, as well as solutions presented in technical studies, like the usage of cryptographic principles.**

Keywords—Vehicular; Cloud Computing; Security;

I. INTRODUCTION

In a world full of changes and advances in technology, in networking to be more precise, everything is essentially connected and communicating, thus the paradigm of Internet of Things. Among the "things", vehicles, with all their sensors, assisted driving facilities, in-car entertainment systems are also connected. Besides the desire to improve road safety, the development of mobile communications also helps to improve transportation efficiency and humans comfort while driving.

For the last years, vehicular communications were made up of intra-vehicle communications, meaning the methods and standards with which sensors on a car communicate one to each other, or, the communication between vehicles and other types of infrastructure. In the last decade VANET was the research theme for scientists and automotive industry, but, the lack of commercialization and the rapid development of mobile networks and cellular communications (3G, 4G, LTE-A, 5G) saw VANET remaining behind. It could not meet the requirements for future autonomous driving scenarios.

The emergence of the Internet of Vehicles, as a part of IoT brought vehicular communications to new horizons. Cloud computing, which is the concept of migrating computing, storage, data processing and other functions from traditional desktop and portable computer devices, by virtualizing these functions in the cloud platform, can be used, and simultaneously use the vehicular environment and the devices' processing capabilities to sustain the growth of Mobile Cloud Computing. Thus, the Vehicular Cloud, can be seen as an extension to Mobile Cloud Computing [1], vehicles being able to share their resources in terms of information and data processing in order to bring significant benefits to drivers and other users.

The objectives of this paper are:

- An introduction on the concepts involved in Vehicular Clouds and Vehicular Cloud Computing, in order to understand the role in current research in a multi-domain area: Automotive, Communications, and Information Technology;
- A presentation of security risks, threats and vulnerabilities in Vehicular Clouds, and the way they derive from classical Vehicular Ad-Hoc Networks (VANETs) and from Cloud Computing and Cloud Technologies.
- A conceptual discussion of security mechanisms involved in managing the vulnerabilities and threats, and how could advances in cryptography can apply in this area of interest.

II. VEHICULAR CLOUD

A. Overview

In literature, [2], vehicular cloud computing can be divided into two categories, which can limit one of the misunderstanding of how the vehicular cloud works. A brief explanation of the concepts is to follow, and can also be seen in figures 1, 2 and 3:

978-1-5386-1495-2/18/$31.00 ©2018 IEEE

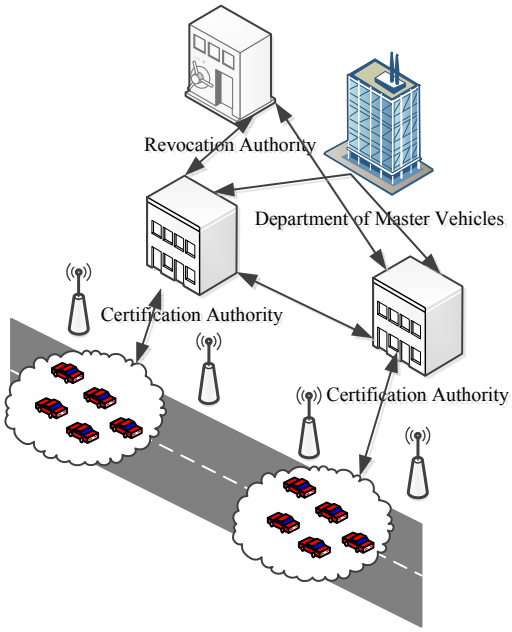

Fig. 1: Vehicular Computing

Vehicular Computing (VC) is the concept that permits the usage of computing capabilities of the vehicles, which can be used in order to provide public services. For example, vehicles parked in a big parking lot can be used as temporary datacenters, or vehicles which travel in zones where there isn't any mobile coverage, can use the other vehicles that travel behind or in front of them as access points. Many of the Vehicular Computing aspects can be seen as vehicles playing the role of IaaS (Infrastructure as a Service) or PaaS (Platform as a Service).

Vehicular using Cloud (VuC) is a more classical approach, in which vehicles use cloud services and resources instead of using their own.

Other authors, [3], define a third category of vehicular clouds, naming it a Vehicular Hybrid Cloud, where vehicles act both as service providers (Vehicular Computing) and as

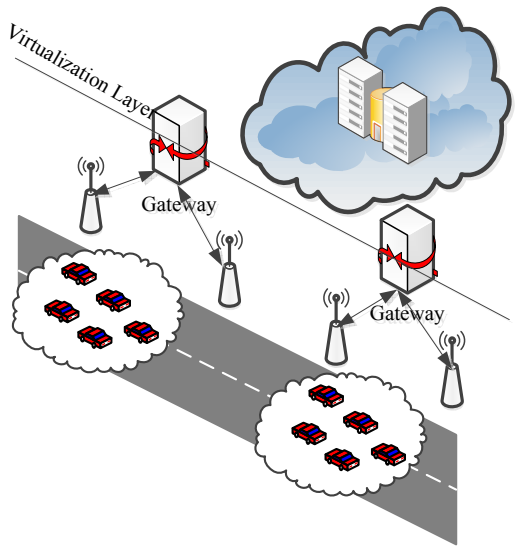

Fig. 2: Vehicular using Cloud

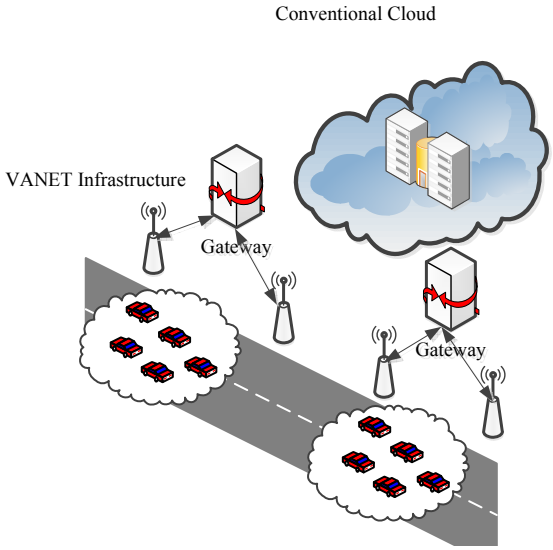

Fig. 3: Hybrid Architecture

users(Vehicular Using Cloud) Figure 3 presents a hybrid architecture.

B. *Requirements*

Many of the issues raised by VANET researches in terms of security and privacy still stand and are at the basis of research for the Vehicular Cloud. A high level of security is needed to be reached with minimum cost in terms of latency induced and atop of that, as vehicles become "smarter", more components are communicating and sending data intro the network, opening new communication channels that hackers can challenge. Table 1, [4], summarizes what we stated.

Requirements in terms of security and privacy and concepts that come to fulfill them are grouped and stated in what follows:

- Data verification, in terms of the authenticity of the sender, is achieved by the use of digital certificates, in which information about the identity of the vehicle and its wright to send messages in the network, are being stored;
- Data integrity means all the measures taken that the information sent is not being altered while it is being routed to the network;

TABLE 1: Vehicular application requirements [4]

Application Type	Latency Limit	Bandwidth	Security Requirements	Examples
Infotainment	500	+++	+	Video Streaming
Traffic Efficiency	200	+	++	e-Toll Collection
Safety	100	+	+	Collision Warning
Reliable M2M	20	+	++	Auto-cruise
Real-time Virtual Reality	5	++	++	Augmented reality navigation
Control	1	++	+++	Co-operative electronic stability control

- Network availability is the capacity of the network to ensure that whenever an entity wants to send data it can. Denial of Service attacks need to be countered in order to reduce the risk associated with the availability of the network;
- Privacy and anonymity are concepts that state that the identity of e vehicle must not be revealed to third party entities that do not have credentials to enter the vehicular network or are not allowed to access this kind of information;
- Confidentiality must ensure that messages even if they are, willingly or not, intercepted by other entities, they cannot be deciphered or understood. Of course, there are sorts of messages like CAM (Cooperative Awareness Message) or DENM (Decentralized Environment Notification Message) which are broadcasted in the network and do not have confidentiality requirements.

III. SECURITY ASPECTS

A. *Cloud Computing Security overview*

Traditional Cloud Computing, as it was first defined by the National Institute of Standards and Technology (NIST) is "a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management e□ort or service provider interaction" [5] attracts users with its scalability, high resource elasticity and, last but not least, bypassing the need for own investments in network infrastructure.

In terms of security, it is for certainly that there are still great advances to be made in order to overcome the security challenges of this concept. But when we add on top the security requirements for vehicular networks, the amount of research to be done grows exponentially. Data security, cloud network infrastructure security and cloud applications security, are all domains of interest, so that organizations that offer cloud services, like computation outsourcing, resource sharing and external data warehousing , need to take in mind, according to [6], security aspects from the design phase, matching the appropriate solution targeted for the appropriate deployed technology and finishing up with testing in order to validate the security monitoring and alerting capabilities. It is important that in the phase of testing, any vulnerability be logged and deeply investigated.

B. *Attackers and threats*

Because of the nature of the Vehicular Cloud, attackers and threats do not necessarily have the same characteristic as attackers in simple, point-to-point or multipoint networks. The high number of users that share the same physical, and in some scenarios, ad-hoc infrastructure, challenges the security plane of the cloud, attackers having thus more advantages then in traditional systems.

But as the authors in [7] state, the high mobility of the vehicles is like a double-edged sword. Vehicles being on a permanent movement, are not easy targets. Because of the temporary access to the network, and the heterogeneous characteristic, network access being offered though different standards of communication, like Wi-Fi, DRSC, WiMAX, 4G or the future 5G, vehicles are performing a large number of handovers. During every handover, vehicles once they detect the presence of another access network, based on the RSSI (received Signal Strength Indicator) vehicles start the process of translating or acquiring their network addresses. During this process a new set of security mechanisms are implied, reauthenticating practically the vehicle in the network, making it more difficult for an attacker to maintain the link between him and the cloud.

Additionally, because of the nature of the cloud, it being composed of numerous virtual machines that are usually not on the same physical machine, or even belonging to different service providers, attackers need to locate if their target is on the same physical machine or virtual machine, and overcoming different security precautions, that can vary from one virtual machine to another. Authors in [7] state that the attacker and the target must coexist, physically or logical, in the same region of the network or on the same potion of the cloud. Even though this requirement can be achieved it is difficult to obtain a permanent coexistence. Of course, if an attacker is impersonating a vehicle or is physically present in the network, not wanting to attack another vehicle, but to induce false data into the network, the above-mentioned considerations are not applicable.

Threats in Vehicular Cloud Computing are also subject to research, and according to [2], there are six groups, each of them having different approaches in literature, and slightly different repercussions, as show in the following classification:

- Denial of Service attempt to purely make the resources provided by the vehicular cloud for end users unavailable. The most common approach is to overload the communication channel (known in computer networks as "spamming" or flooding) and it affects the availability of the system;
- Identity spoofing is the mechanism in which a malicious node or an unauthorized user or application to take someone else's identity and credentials. Besides bypassing the authentication schemes, this threat has a significant impact on confidentiality and availability;
- Data modification or tampering is best exemplified by the Man-in-the-Middle attack, who either alters the information or uses it, by intercepting it before the destination;
- Repudiation is the attacker's ability to manipulate the data in order to not be taken responsible for actions or messages. It takes advantage of confidentiality and data integrity weak points;
- The Sybil attack is probably the most damaging attack on vehicular networks, because of the bypassing of all

security principles (authentication, confidentiality, integrity and availability).

C. Authentication and privacy

According to [8] and extended to the scope of this paper, security authentication in the Vehicular Clouds must meet a set of metrics that quantify a user's wright to enter the network:

- ownership, meaning that the node owns a unique identity;
- knowledge, meaning that the node knows unique things, like a password, a key, basically the ability of a node to sign and encrypt and decrypt data using secret keys;
- biometrics, meaning that the node has the ability to use unique human characteristics, like signature, face, or voice recognition or fingerprints in order to access the network;

Authentication techniques in classical VANETs are applicable to Vehicular Clouds, using techniques like Public Key Infrastructure. In order for the vehicle to authenticate in the cloud, it must be first authenticated by the infrastructure. The main problem is that with the vehicles traveling at high speeds, the location is rapidly changing, thus needing authentication schemes to be extended during handover schemes. An advantage of Vehicular Clouds is that the network being virtualized and not having a centralized architecture, thanks to the advances of the communication methods inside the clouds, the authentication phase is easier to manage inside the cloud.

According to [9], third-party entities being more involved in cloud management, the problem of preserving the identity and privacy protection is an even greater challenge than in VANETs. A third-party, that must be more that a basic Certification Authority entity, must have access to identities and must be equipped with capabilities that ensure that nobody can alter with the information stored there. Literature proposes a numerous set of solutions, based on Elliptic Curve Cryptography as a stepping-stone foundation. In reference [10] authors propose an Efficient Conditional Privacy Preservation Protocol (ECPP) which is based on the use of bilinear maps. Users, identified though pseudonyms, have multiple anonymous keys and use them to access the network. But the problem of a large pool of pseudonyms, and how to manage them, in terms of revocation, denial, approval and updating, remains an issue.

D. Trust

A trust model or scale is used so that a node can evaluate the trustworthiness of another entity, either being a node or an infrastructure component in order to identify malicious nodes that induce false data in the network. According to [11] there are two kinds of trust models in VANETS, that are either entity-centric, which evaluate vehicles and try to ensure reliable data delivery, or data-centric models which evaluate the trustworthiness of the data sent into the network. These two collaborate with each other.

Entity-centric trust models calculate reputation scores based on the historical interactions [12], called direct-trust, or based on the recommendations issued by neighbor nodes [13], called recommendation trust. In order to have an objective view, authors in [14] introduce a balance coefficient in order to leverage the proportion of direct and recommended trust.

Data-centric model has more to suffer because of the real time requirements of the communications. Of course, it is practically impossible to verify the information sent in real time, and revoke instantly the malicious node's ability to send data.

A concept extracted from the Internet of Things, is to establish trust chains inside groups of entities that share the same purpose, such as similar vehicles in terms of hardware, road behavior, destination or application accessed, forming thus a kind of group interaction scheme. According to [15], chains of confidence can allow the establishment of groups or communities and unique identities (for the communities) for the access to services as well as for the spreading of group information. Therefore, security is established when the nodes access the network through the use of the trust chain generated by nodes. Concretely, in [17] authors describe a trust-based authentication technique for cluster based VANET, a scheme which can be easily implemented to Vehicular Clouds. Based on the trust degree, a Cluster Head is selected, which is the vehicle with the biggest trust degree of all. The Cluster header is the one through all vehicles from within the cluster are communicating. Some Cluster headers can be in more cluster, thus acting as a gateway for vehicle-to-vehicle communication.

E. Secure information dissemination

One of the main characteristics of a vehicular environment is that it is a multi-user environment which has a high rate of topology alterations and high variation of nodes. Public key infrastructure-based access control is not one of the best choices, according to [3] because it will not ensure access control in a fine-grained manner. Basically, the authors propose that in a practical scenario, information that is sent through the network can be characterized by attributes that are extracted from the scope of the information. Furthermore, for each attribute a public key component is defined and used for encryption of data. On the user side, user secret keys are also sorted and generated based on the type of data that is likely to send across the network. An advantage of this approach is that is shows an improved reduction in computational overhead.

Other studies propose either a GPS-based location encryption scheme [17], where coordinates are used to generate keys, but because of the ease-of-access to GPS coordinates, this approach is accessible to attacks.

ID-based signatures schemes, like the one proposed in [18], in which pseudonyms are used to ensure additional privacy, and batch verification are also a topic of interest, but, as most studies, they are limited to classical VANETs, where the exchange of public and private key pairs causes a heavy computational overhead. In Vehicular Cloud Computing, identity-based signature schemes are fast based on batch verification [19]. For example, in [20], the continuous beaconing of messages, in vehicular cloud environment is not

treated like in classical VANETs, because in order to process a huge amount of vehicular traffic information, resources are allocated from the cloud to calculate and operate with this kind of information. The data flow ca be vice-versa, the cloud infrastructure itself being able to issue beaconing message, for the extended vehicular traffic information, thus saving the still limited computational capabilities of vehicles [20].

IV. CONCLUSSIONS

In this paper we have addressed the security challenges involved in the design of Vehicular Cloud Computing architecture.

After a brief introduction intro this domain, we have taken security aspects from Cloud Computing and stated how they apply and extend to the Vehicular environment. The threats, vulnerabilities and attackers have been the presented, most of them being the same that jeopardize the VANET infrastructure. Reference [21] is a research in which we have studied security aspects of VANETs more deeply and is a good starting point for future research. But the new and heterogeneous aspect of the vehicular environment implies that additional measures must be taken into account, during the handover mechanism.

Moving on to the end of the paper, trust and secure information dissemination are discussed, because after the authentication mechanisms take place, vehicles start transmitting data into the network, thus being necessary to discuss about mechanisms that securely quantify one's wright to send data, and to be taken in consideration. Of course, without a secure authentication mechanism, chaos could be induced into the network, but also, malicious vehicles could authenticate in order to induce false data. Privacy must be ensured, at the thin limit between not using private data for spoofing and other evil purposes, and securely overviewing the network users.

Future personal research will go deeper into the security aspects of vehicular communications, up until the point where cryptography and secure algorithms and aspects implied in the protocols can be used optimally in a secure vehicular environment.

REFERENCES

[1] M. Abuelela and S. Olariu, "Taking VANET to the clouds", Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, MoMM '10, ACM, New York, 2010, pp. 6–13.

[2] M. Whaiduzzaman, M. Sookhak, A. Gani and R. Buyya, "A survey on vehicular cloud computing". Journal of Network and Computer Applications, volume 40, 2014, pp. 325–344.

[3] M.R. Jabbarpour, A. Marefat, A. Jalooli, and H. Zarrabi, "Could-based vehicular networks: a taxonomy, survey, and conceptual hybrid architecture" , Wireless Networks, 2017

[4] S. Yu , C. Wang , K. Ren and W. Lou "Achieving secure, scalable, and fine-grained data access control in cloud computing", IEEE INFOCOM, pp. 1–9. 2010.

[5] P. Mell, "The NIST Definition of Cloud", Reports on Computer Systems Technology , 2011.

[6] Cloud Standards Customer Council 2015 "Security for cloud computation: Ten steps to ensure success", version 2, 2015.

[7] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing", IEEE Transactions on Intelligent Transportation Systems, vol. 14/1, pp. 284-294, 2013.

[8] Federal Financial Institutions Examination Council "Authentication in an Internet banking environment" 2009

[9] Y. Park, C. Sur and K.H. Rhee, "Pseudonymous authentication for secure V2I services in cloud-based vehicular networks", Journal of Ambient Intelligence and Human Computing, vol. 7, pp 661-671, 2016.

[10] R. Lu, X. Lin, X. Liang and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANET". IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 127–139 2012.

[11] S.A. Soleymani, A.H. Abdullah, W.H. Hassan, M.H. Anisi , S. Goudarzi, M.A.R. Baee and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review", EURASIP Journal on Wireless Communications and Networking, pp. 146, 2015.

[12] Z. Huang, S. Ruj , M.A. Cavenaghi, M. Stojmenovic and A. Nayak, "A social network approach to trust management in VANETs", Peer-to-Peer Networking and Applications, vol. 7, pp. 229–242, 2014.

[13] F.G. Mármol, G.M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks", Journal of Network and Computer Applications, vol. 35, pp. 934–941, 2012.

[14] X. Yao, X. Zhang, H. Ning, P. Li, "Using trust model to ensure reiable data acquisition in VANETs", Ad Hoc Networks, vol. 55, pp.107-118, 2017.

[15] S. Sicari, A. Rizzardi L.A. Grieco, A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, vol. 76, pp. 146–164, 2015.

[16] R. Sugumar, A. Rengarajan and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)", Wireless Networks, vol. 24, pp. 373-382, 2018.

[17] R. Hussain, Z. Rezaeifar, Y.H. Lee and H. Oh, "Secure and privacy-aware tra□c information as a service in VANET-based clouds", Pervasive and Mobile Computing vol. 24, pp. 194-209, 2015.

[18] L. Nkenyereye, B.A. Tama, Y. Park and K.H. Rhee, "A fine-grained privacy-preserving protocol over attribute-based access control for VANETs". Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Appllications, vol. 6, no. 2, pp. 98–112, 2015

[19] Z. Wan, J. Liu and R.H. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing", IEEE Transactions on Information Forensics and Security, vol. 7, pp.743–754, 2012.

[20] S. Luo, L.Pan, Q.G. Safi, C. Wei and G. Yan, "Cloud-based security and privacy-aware information dissemination over ubiquitous VANETs". Computer Standards & Interfaces, vol. 56, pp.107-115, 2012.

[21] L. Gafencu, L. Scripcariu and I. Bogdan, "An overview of security aspects and solutions in VANETs", International Symposium on Signals, Circuits and Systems (ISSCS), pp.1-4, 2017