International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 4154~4162
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp4154-4162

Securing vehicular cloud networks

Djilali Moussaoui[1], Mohamed Feham[2], Boucif Amar Bensaber[3], Benamar Kadri[4]
[1,2,4]STIC Lab., Department of Telecommunications, University of Tlemcen, Algeria
[3]Laboratoire de Mathématiques et Informatique Appliquées LAMIA, Université du Québec à Trois-Rivières, Canada

Article Info

Article history:

Received Jan 24, 2019
Revised Apr 15, 2019
Accepted Apr 22, 2019

Keywords:

Cloud computing
Vanet
VCN privacy
VCN security
Vehicular cloud networks (VCN)

ABSTRACT

Vehicular Cloud Networks (VCN) is the network that ensures mobility and availability of resources allowing new services and applications like Network as a Service (NaaS), STorage as a Service (STaaS), Computation as a Service (CompaaS) and Cooperation as a Service (CaaS). In this paper, we propose a solution to secure the Vehicular Cloud Network (VCN). Our challenge in this work is to adapt the PKI architecture, which is mainly used in wired networks to be used in VCN. To propose a security solution for Vehicular Cloud Networks (VCN), our work is based on three steps; the first one is to make network architecture study, where we tried to highlight the main network components. The second step is to propose the security solution architecture. Finally, the last step is to program a test and validate the solution using a simulation.

Corresponding Author:

Djilali Moussaoui,
STIC Lab., Department of Telecommunications,
University of Tlemcen,
Tlemcen, Algeria.
Email: dj_moussaoui@yahoo.fr

1. INTRODUCTION

Modern networks are developed along two axes. The first one is mobility, this is to ensure the network availability to the connected entities in motion. Under this axis, we can find different types of networks such as MANET (Mobile Ad hoc NETwork), VANET (Vehicular Ad hoc NETwork) and WSN (Wireless Sensor Network). The second axis is the resources availability in types (computing, storage, software) and volume. The most used networks are parallel computing, grid computing and cloud computing.

Vehicular Cloud Network (VCN) is the network that ensures the mobility and availability of resources allowing new services and applications, like Network as a Service (NaaS), STorage as a Service (STaaS), Computation as a Service (CompaaS) and Cooperation as a Service (CaaS). The VCN are the result of merging of two main networks, the VANET and Cloud networks. So, its architecture contains both the cloud computing and VANET entities.

Security in VCN is a big challenge, where security requirements must be guaranteed. The most important security requirements are authentication, integrity, privacy, confidentiality and traceability. In literature, the solution that satisfies these requirements for wired networks is the PKI (Public Key Infrastructure) enhanced with security mechanisms to ensure privacy. For this reason, our solution called VCPKI (Vehicular Cloud Public Key Infrastructure) is based on PKI, and as it is proven in section 7 our solution secures the network with a negligible impact on network performance. The rest of this paper is organized as fallows. We present networks architecture in section 2, followed by the security requirement for the VCN in Section 3. We describe the architecture of security solution in Section 4. The Section 5 presents how the solution works under VCPKI protocol. The solution analysis (security and performance analysis) is presented in Sections 6 and VII. Finally, a conclusion is given in Section 8.

2. NETWORKS ARCHITECTURE

In the following we present the architecture of VANET, Cloud Computing, also the VCN taxonomy and architecture. After studying the VANET [1] and Cloud Computing networks [2, 3], the Figure 1 defines the Vehicular Cloud Network architecture.

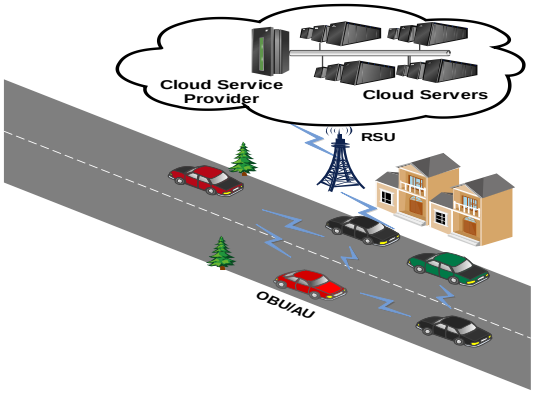
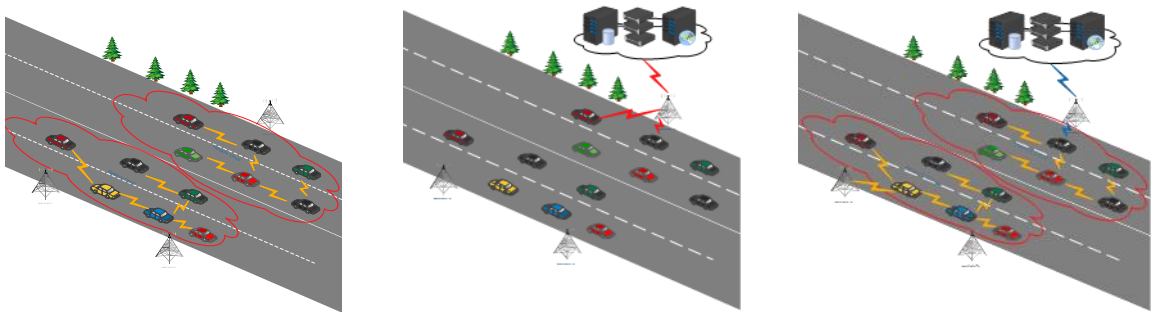


Figure 1. VCN Architecture

The end user is the vehicle, the RSU is the gateway to achieve the cloud part. In the cloud we find the Cloud Provider and Cloud Servers. Vehicular cloud is divided into three major architectures namely Vehicular Clouds (VC), Vehicles using Clouds (VuC), and Hybrid Clouds (HC). The Vehicular Clouds (VC) is a network formed only by vehicles and regarding the vehicle as shown in Figure 2(a).



(a) (b) (c)

Figure 2. Vehicular Cloud Network (VCN)

Also, the VCN can be formed Vehicles and these vehicles are connected to the traditional clouds where cloud services are available as shown in Figure 2(b). The third case is called Hybrid Cloud as shown in Figure 2(c), where vehicular clouds will interact with the traditional cloud for services exchange. The vehicles and RSUs will serve as gateways on the VANET part thereby communicating with the gateways of traditional clouds.

3. SECURITY REQUIREMENTS

The most important security requirements in the Vehicular Cloud Network are authentication, integrity, privacy, confidentiality and traceability.

- The authentication ensures that the message is generated by the legitimate user. It protects the elements of communication (messages and entities) [4, 5].
- In our context (Vehicular Cloud Network), the authentication is very important security requirement, because it is frequently solicited, to use cloud services [6]. So, our solution provides privacy-preserving authentication.

- The integrity ensures that the data is protected from deletion, modification, and production without permission [7]. The proposed solution should guarantee the integrity.
- The Privacy is necessary to protect the profile and driver's information and the vehicle localization against unauthorized access [8]. The privacy protection mechanisms are embedded in our security solution.
- The aim of confidentiality is to protect the communication of a set of vehicles from an external intruder. The encryption is the main tool to ensure this security requirement and the encryption mechanisms are defined to be sure that the encrypted information is decrypted only by the group of members (vehicles) [6] ECC.
- The traceability identifies vehicles and their communications and preserves their privacy and information confidentiality [9]. To protect user information, the identity must be hidden and also it is important to use a system component (trace manager) to obtain the real identity where it is needed [10].

4. PROPOSED ARCHITECTURE FOR SECURING VEHICULAR CLOUD WITH PKI (VCPKI)

4.1. Proposed model for VCPKI

The VCN is composed of three layers

- The network layer (VANET)
- Mobile infrastructure layer
- Cloud computing layer

The Figure 3 shows our proposed model for Secured VCN and its components. The goal of the VCN security architecture is to be in harmony with three main architectures (VANET, Cloud, PKI).

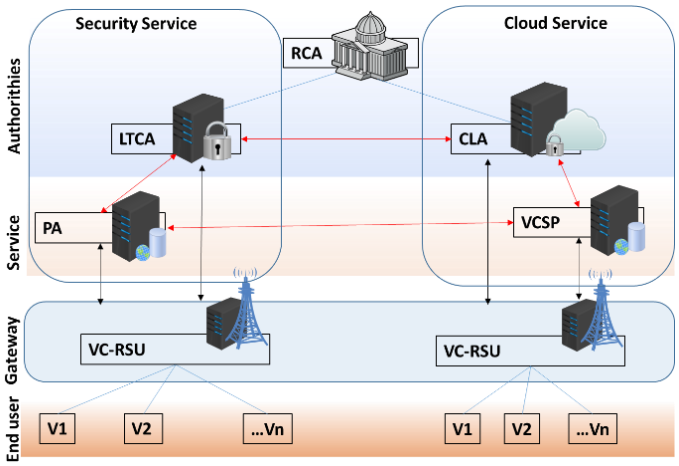


Figure 3. Proposed Model for Secured VCN

4.2. Components

4.2.1. RCA (Root Certificate Authority)

The RCA is the trust anchor in the system where the trust is assumed and not derived, its certificate is self-signed. Its main role is to issue and sign certificate only for subordinate authorities of the VCPKI security system (LTCA, VCSP).

4.2.2. LTCA (Long-Term Certificate Authority)

LTCA issue and sign long-term certificate for the system end users (Vehicles). Each entity must send its request directly to LTCA to obtain a long-term certificate. Also, the LTCA is responsible to issue tokens for vehicles (or other entities), these tokens are used to request pseudonyms (short-term certificate) from the PCA.

4.2.3. CLA (Cloud Authority)

The CLA is responsible of managing users cloud accounts, and to issue tokens for vehicles (or other entities), these tokens are used to request cloud service from the VCSP.

4.2.4. VCSP (Vehicular Cloud Service Provider)

It makes the cloud service available to the connected vehicles. For this, it acquires and manages the computing infrastructure's information. In Vehicular Cloud, there are two types of resources, the Vehicles resources (OBU), and computers resources (Datacenter).

4.2.5. PCA (Pseudonym Certificate Authority)

The use of pseudonyms is important to protect the privacy of users in the network. This authority has two main roles:

- *Issuing pseudonyms (short-term certificate):* Each vehicle sends a request to the closest PCA to achieve a set of pseudonymous certificates. Using pseudonyms, each vehicle can communicate in the network anonymously.
- *Pseudonym resolution:* The PCA is endowed with the function of resolving pseudonyms identity. This operation is used when it is necessary, it consists of finding out the related token to a specific pseudonym, after that it queries the LTCA to identify and reveal the real identity for that token. If the pseudonym is identified as malicious, the PCA can revoke all related pseudonyms.

4.2.6. VC-RSU (Local Vehicular Cloud Service Provider)

It is an RSU as used in VANET equipped with the computational unit used to offer more functionalities and services for vehicles. So the VC-RSU ensure two main functions, the first is the RSU managing the VANET, the second is cloud management function. As the first function is known and already used in VANET, the second one consists of offering local cloud services for vehicles, without requesting the service from VCSP.

4.3. Proposed Model Architecture

The proposed architecture can be divided into four Layers.

4.3.1. The end users Layer

This layer contains the vehicles connected to the closest VC-RSU.

4.3.2. Gateway layer

This layer can be compounded by a set of VC-RSU and another network component (ex: routers) that allows the direct access to the other system components.

4.3.3. Service Layer

In this layer, we find the components that allow the services: privacy (PCA) and the Cloud Service (VCSP).

4.3.4. Authorities

Three elements are the essential components in this layer: The RCA (issue the certificate for this layer components), the LTCA and CLA.

4.4. Functional View

In this section, we present functions or services, this architecture allows two main services: security and cloud.

4.4.1. Security service:

This service regroups all security operations in the network with security entities (LTCA, PCA). These operations concern LTCs and pseudonyms.

4.4.2. Cloud Service

This service concerns the cloud authorities (CLA, VCSP) and the performed operations to obtain a cloud service. This service is directly relied with the security service because we want to offer a cloud service in a secured context.

5. VCPKI DESIGN

5.1. Security Service

5.1.1. Request Long-Term Certificate:

1: The vehicle request from RSU's authority's certificate.

2: The RSU sends the certificate to the vehicles.
3: The vehicle generates Elliptic Curve Public Key Pair.
4: The vehicle creates a Certificate Signing Request (CSR), encrypted by the public key of the LTCA.
5: The vehicle sends it online to LTCA.
6: LTCA issues new LTC.
7: LTCA load its private key, signs LTC, and create a certificate.
8: LTCA sends it back to the subscriber.

5.1.2. Request a Pseudonym Certificate:

To enforce the privacy in this protocol, we divide the operation of requesting pseudonym into two steps. The first one is token request where the user can use his real identity (Long Term Certificate) from LTCA. Using this token, the user can request a pseudonym from the PCA (step 2). The Figure 4 show us an Overview on message exchange.

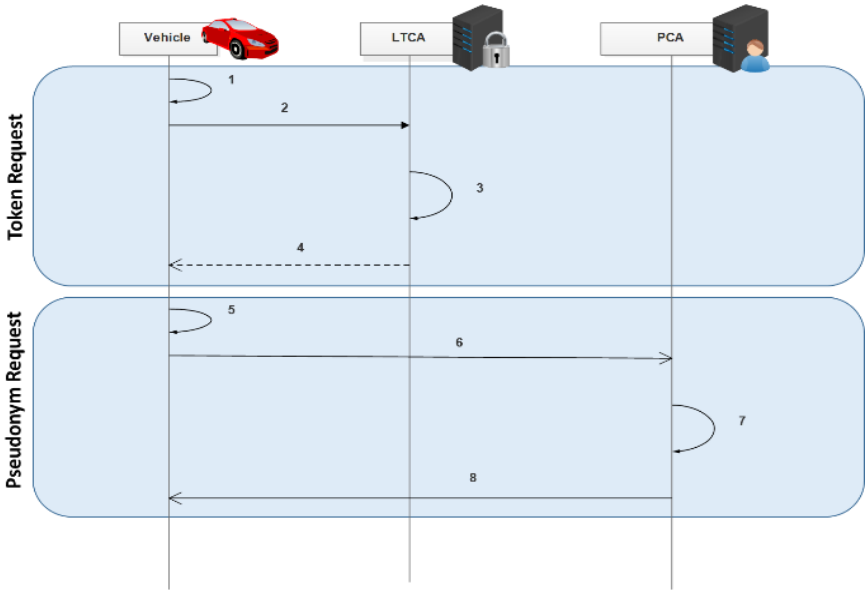


Figure 4. Request Pseudonym Certificate

a. Obtain Security Token
1: Prepare Token Request
2: Send the token request to the LTCA
3: Token generation
4: Token replay
5: Store the token in HSM to be used in the next phase.
b. Obtain Pseudonym Certificate

The pseudonym certificate request is between the PCA (Pseudonym Authority) and the vehicle where this later use the token obtained from the step before.

1: The Vehicle prepares the Pseudonym Request.
2: The vehicle sends the Pseudonym Request to the PCA, in this request the security token is sent as a parameter.
3: The PCA verifies the request and the token, and generates a set of pseudonyms.
4: The PCA sends the generated pseudonyms to the Vehicle.

5.1.3. Pseudonym Resolution

Pseudonym resolution is a process used to identify the real identity of a pseudonym. This process is requested by the police, and it is done in two phases Token Resolution, identity resolution as shown in Figure 5.

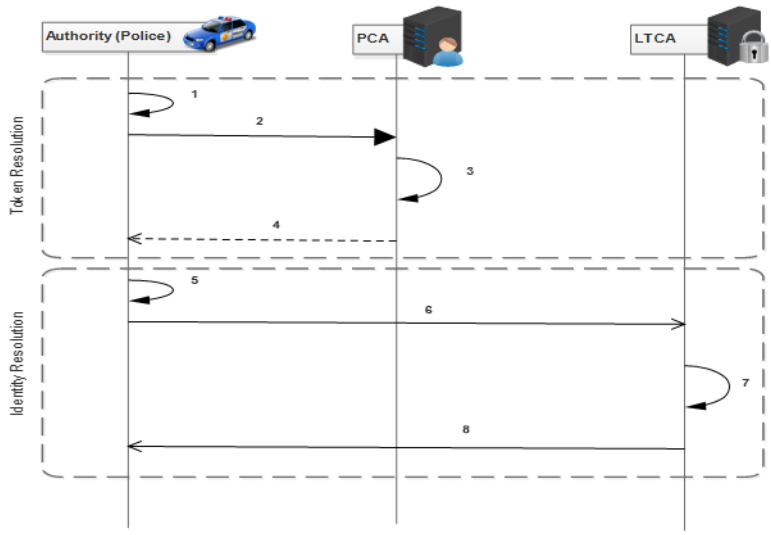


Figure 5. Pseudonym Resolution

a. Step 1: Token Resolution
1. The authority gets the malicious node's pseudonym from the network and prepares the *TokenResolutionRequest.*
2. The authority sends *TokenResolutionRequest* to the PCA, where the pseudonym of the malicious node is sent as a parameter.
3. The PCA finds the corresponding token for the pseudonym.
4. The PCA send the token to the authority by the *TokenResolutionReplay*.

b. Step 2: Identity Resolution
1. The authority prepares the IdentityResolutionRequest.
2. The authority sends IdentityResolutionRequest to the LTCA.
3. The LTCA finds the corresponding identity to the token prepare the reply message.
4. The LTCA sends the IdentityResolutionReplay where the operation result is sent.

6. SECURED CLOUD SERVICE

The cloud service allows the user to access to the cloud, our proposition ensures more security and privacy. Figure 6 gives an overview of the message exchange.

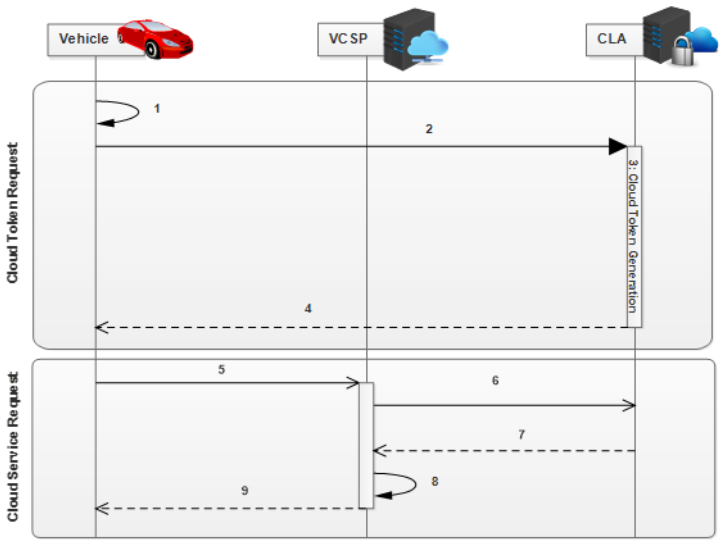


Figure 6. Secured Cloud Service

6.1. Request the cloud service

6.1.1. Step 1: Cloud Token Request

a. The vehicle prepares Cloud Token (request a pseudonym if it didn't before)
b. The vehicle sends the CloudTokenRequest to the CLA where the cloud account ID and the pseudonym are sent as parameters (the communication is performed in a secured channel)
c. The Cloud Authority (CLA) verify the cloud account ID and prepare a token for the user cloud account.
d. The Cloud Authority (CLA) send back the CloudTokenRepley that contain the Cloud Token.

6.1.2. Step 2: Cloud Service Request

a. The vehicle sends a CloudServiceRequest to the VCSP using the cloud token.
b. The VCSP sends a CloudAccountStatusReq to the CLA that includes the token.
c. The CLA replies with CloudAccountStatusRep containing the cloud account information.
d. The VCSP stores the cloud account status with the corresponding pseudonym to offer the appropriate cloud service.
e. The VCSP sends the CloudServiceReplay, if the service is grant, the vehicle can use his pseudonym to use its cloud service.

6.2. Renewing the cloud service request

As it is presented above, the vehicle requests a Cloud Service using its pseudonym, where the pseudonyms are valid for a period and the vehicle can use another the pseudonym, for that the validity of the cloud service is related to the validity of the pseudonym. So, for each pseudonym changing, the vehicle must update the cloud service request. The updating request contains the old pseudonym, the new pseudonym, and the cloud service token.

7. SECURITY ANALYSIS

The security analysis is based on how the solution ensures the VCN security requirements (Integrity, Privacy and Non-repudiation).

7.1. Integrity

Our system is a PKI based solution, so the exchanged messages must contain a valid sender signature, which is easily verifiable through the certificate authorities (LTCA, PCA). Therefore, the integrity in our system is a guarantee.

7.2. Privacy

The pseudonym is a temporary certificate, characterized by the anonymity and a short period of validity. This pseudonym is used instead of the digital certificate to provide the privacy. Pseudonyms guarantee the privacy in using the network, in VCN, the challenge is to guarantee the privacy in using network and cloud service. For this our proposition based on the authority's separation to enforce the privacy in the network and between authorities when using cloud service.

7.3. Non-Repudiation

In VCN and during emergency situations as accidents, actions or changes must be associated with a unique vehicle (driver). Also, the cloud services are offered for multiple tenants; non-repudiation is important to identify the tenant participation in any argued transaction. In VCPKI protocol, pseudonyms are used to exchange messages. The message originator only knows this pseudonym and therefore, the sender cannot repudiate.

8. PERFORMANCE ANALYSIS

To evaluate the impact of our solution on the network performance, we have implemented our system VCPKI (Vehicular Cloud PKI) on OMNET ++ 5.0 simulator [11] with veins 4.4 [12] and SUMO-0.25.0 simulator [13]. In Table 1, we present the simulation parameters In this simulation, we have measured the delay in two situations, the first one without using VCPKI protocol, the second one the network use VCPKI as a security protocol. As seen in Figure 7, the difference is negligible, it is between $2{,}1.10^{-5}$s and $7{,}73.10^{-5}$s. Also, we have measured the packet delivery ratio (PDR), as shown in Figure 8, and it is the same for the two situations (with, without VCPKI). So, the protocol VCPKI have no impact on PDR in the network.

Table 1. Simulation parameters

Item	Value
Map of Tlemcen (Algeria)	2,5km*2,5km
Simulation time	1000s
Speed max	14m/s
Packet size	1024 bytes
Bit rate	6 Mps
Number of RSU	4
Communication Rage of vehicle	800m
Communication Rage of RSU	800m

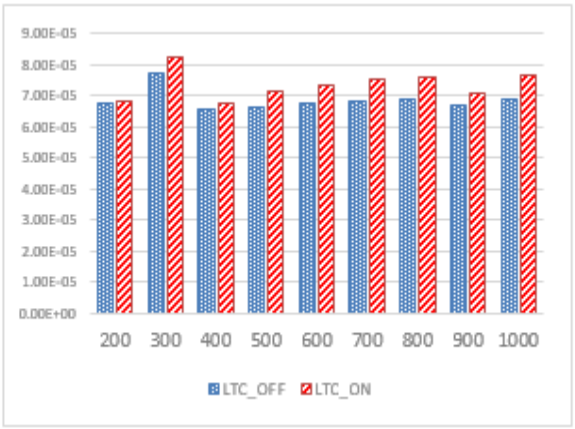


Figure 7. Delay in VCN

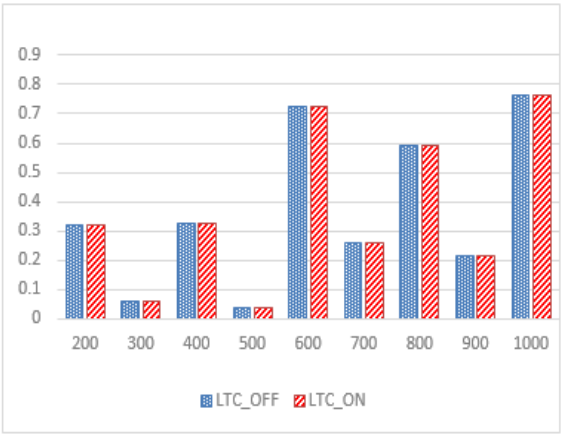


Figure 8. VCPKI impact on PDR in VCN

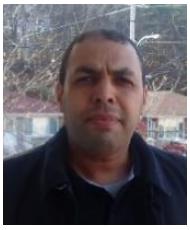
9. CONCLUSION

In this work, we have made a tour on security in Vehicular Cloud Networks; we studied attacks and their impact on the network aspects (Cloud service and security requirement). This study helps us two define the most touched security requirements by the attacks. On the base on this study, we have proposed VCPKI as a protocol to secure the network. After the implementation and the simulation of the VCPKI protocol, we conclude that the solution enforces the security of the network with a negligible impact on the network performance.

REFERENCES

[1] S. P. Godse and P. N. Mahalle, "A Computational Analysis of ECC Based Novel Authentication Scheme in VANET," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 5268-5277, 2018.
[2] T. Francis, "A Comparison of Cloud Execution Mechanisms Fog, Edge, and Clone Cloud Computing," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 4646-4653, 2018.
[3] R. Hussain, et al., "Rethinking Vehicular Communications: Merging VANET with cloud computing," *CloudCom 2012 - Proc. 2012 4th IEEE Int. Conf. Cloud Comput. Technol. Sci*., pp. 606-609, 2012.
[4] S. P. Godse and P. N. Mahalle, "A Computational Analysis of ECC Based Novel Authentication Scheme in VANET," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, pp. 5268-5277, 2018.
[5] R. P. Barnwal, et al., "Data and Application Security in Cloud," in Intelligent Systems, Springer-Verlag, vol. 70, pp. 479-495, 2014.
[6] R. M. Jabir, et al., "Analysis of cloud computing attacks and countermeasures," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2016, pp. 117-123, Mar 2016.
[7] C. Kalloniatis, et al., "Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts," *Comput. Stand. Interfaces*, vol. 36, pp. 759-775, 2014.
[8] A. Kertesz, "Characterizing Cloud Federation Approaches," *in Cloud Computing Challenges, Limitations and Solutions*, pp. 1-26, 2014.
[9] R. G. Engoulou, et al., "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1-13, 2014.
[10] L. Zhang, et al., "Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud," *IEEE Trans. Dependable Secur. Comput*., vol. 5971, pp. 1-14, 2018.
[11] "The Discrete Event Simulator OMNET++," www.omnetpp.org.
[12] "Vehicles in Network Simulation VEINS," veins.car2x.org.
[13] "Simulation of Urban MObility SUMO," sumo.dlr.de.

BIOGRAPHIES OF AUTHORS



Djilali Moussaoui received his engineer degrees in computer science from the University of Tlemcen, Algeria in 2004, and his M.S. degrees in networks and telecommunication systems within of the same University in 2007. Member of STIC laboratory in the University of Tlemcen. Now he is an assistant professor in faculty of technology university of Tlemcen, Algeria. His recent work is dealing with vehicular cloud computing networks and their security.

Mohammed Feham received his PhD in Engineering in optical and microwave communications from the university of Limoges, France in 1987, and his PhD in science from the university of Tlemcen, Algeria in 1996. Since 1987 he has been assistant professor and professor of microwave and communication engineering his research interest is in telecommunication systems and mobile networks.

Boucif Amar Bensaber received his PhD in computer science from the university of Rene Descartes (Paris V), France in 1998. In 1999, he worked as a scientist research associate at the research and evaluation center in diagnostics (RECD), CHUS Sherbrooke (Canada). Since 2000, he has been professor at the university of Quebec (UQTR), Canada. His research interest is in wireless networks, multicast protocols, distributed architectures, in formation and communication technologies and data mining.

Benamar Kadri received his engineer degrees in computer science from the University of Tlemcen, Algeria in 2004, and his M.S. degrees in networks and telecommunication systems within of the same University in 2007. Member of STIC laboratory in the University of Tlemcen. Now he is an assistant professor in faculty of technology university of Tlemcen, Algeria. His recent work is dealing with security.