Evaluate the Security Models Performances and Limitations of the Vehicular Network VANETcloudSim

Abdelilah El ihyaoui*, My Abdelkader Youssefi, Ahmed Mouhsen, and Abdelhafid ELfarnane

Hassan First University of Settat, Faculté des Sciences et Technique, Laboratoire d'Ingénierie, de Management Industriel et d'Innovation (LIMII), Morocco; Email: ab.youssefi@gmail.com (M.A.Y.); mouhsen.ahmed@gmail.com(A.M.); a.elfarnane@uhp.ac.ma(A.E.)
*Correspondence: abdelilah.elihyawi@gmail.com

***Abstract*—The Vehicle Ad Hoc Network (VANET) has been widely used to improve road safety and comfort. However, security is a big challenge for VANET, in fact, vehicle networks have the same security problems as traditional computer networks, hackers can introduce a dangerous threat to security. The issue of security in VANET networks has attracted a lot of attention from researchers to propose several security models. However, validation and performance testing of proposed solutions in a real or simulated environment remains a difficult problem. In this work, we present VANETcloudSim, it's a new cloud platform simulator for VANET security solutions. The proposed simulator allows running stress and tests performance, In contrast to the majority of existing simulators, the proposed platform evaluates the performance and limitations of security models, through the execution of performance and stress tests, it is simple to deploy, robust and efficient. This simulator can be deployed on users' local computers or on the cloud platform.**

***Keywords*—VANET, simulator, security, cloud, tests, docker, public key infrastructure (PKI), certificate Revocztion List (CRL), Vehicle-to-Vehicle (V2V), roadside units (RSU), certificate authority, Kafka, spark**

I. Introduction

Vehicular Ad-Hoc Network is becoming more relevant in today's networks and is becoming an essential part of the roads. This is mainly due to the fact of the advances in connectivity and capabilities of vehicles which have led to the introduction of autonomous vehicles [1]. The system received information about the nearby vehicles and the other vehicle through vehicle-to-vehicle V2V communication and employed it for traffic operation. The location Global Positioning System (GPS) [2] to increase the road network safety by sharing data, which can be the position, speed, direction of vehicles and warnings about dangers such as accidents and traffic jams. The research and application development in vehicular ad hoc networks have been driven by dedicated short-range communication (DSRC) technology or IEEE 802.11p, which is designed to help drivers to travel more safely and reduce the number of fatalities caused by road accidents. The IEEE 802.11p Medium Access Control (MAC) uses carrier sense multiple access with collision avoidance and some concepts [3]. Wireless Access in Vehicular Environments (WAVE) is a mode of operation used by IEEE 802.11 devices to operate in the DSRC band. Furthermore, it provides a wireless medium communication between vehicle-to-vehicle environments. It accesses to control over the IP based telephony service using 4G networks. It is based on the IEEE P1609 series of standards, which define the adaptive architecture, the communication gateway model, the security and wireless physical access features for vehicular communications [4].

There are several important requirements, for achieving security in VANET, which are discussed as follows Authentication: Vehicles should respond only to the messages transmitted by legitimate members of the network. Thus, it is very important to authenticate the message sender [5].

Availability: The network should be available even if it is under an attack by using an alternative mechanism without affecting its performance [5].

Data Integrity: It ensures that data or messages are not altered by attackers. Otherwise, users are directly affected by the altered emergency data [5].

Non-repudiation: A sender must not deny a message transmission whenever an investigation or identity of a vehicle is required.

The new vehicular networks have the same security problems as traditional computer network, there are common security attacks on Vehicular Ad hoc Network such as:

Bogus information: This attack happens when information is sent by the adversaries, including certificates, warnings, security messages, and identities, is not true [6].

Denial of service: This attack happens when adversaries send irrelevant bulk messages in order to jam the communication channel used in VANET.

Message suspension: This attack happens when adversaries hold onto messages before sending them.

Manuscript received August 15, 2022; revised September 20, 2022; accepted January 1, 2023.

Spoofing: This attack happens when the attacker adopts the persona of another network node. As a result, it receives communications intended for that node.

Reply attack: data is gathered by the attacker, who also routes packets and replays them afterwards.

VANET network presents new security concerns to protect privacy, so the researchers propose several security models to improve security and protect the privacy of vehicles and drivers. To assess the feasibility and effectiveness of their proposals, the researchers rely solely on abstract models of road traffic simulation, as there is no real implementation that takes these safety models into account.

We introduce the architecture of a new cloud simulator, VANETcloudSim is a vehicle communication simulator specially proposed to analyze and compare security and privacy concepts on the application layer, it allows comparing preferences, study the limits of each model with performance tests and stresses in a realistic environment, this platform will be integrated into Docker Image, it respects DevOps practices facilitating deployment, exposes representational state transfer REST interfaces to implement other security models and manipulates the data, it can be deployed in the cloud, and it also allows the simulation to run for a long time.

The rest of this document is organized as follows: Section II presents the basic knowledge, including the VANET architecture, the communication types, the message types. Section III provides the VANETCloudSim architecture distributed in modular cloud simulation platform and Section IV presents the evaluation and a discussion.

II. System Description

This section presents the vehicle's ad hoc network system architecture, the communication types, namely Vehicle to Vehicle (V2V) and Vehicle to infrastructure (V2I), the exchanging message types, and finally some safety models are studied.

A. Vanet Architecture

The Vehicle Ad Hoc Network has three elements as shown in Fig. 1:

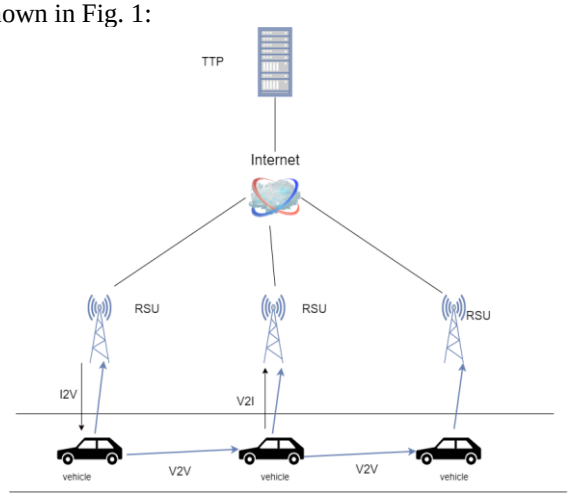

Figure 1. VANET system architecture

- **Trusted third party** is a trusted third party (TTP), which refers to a trusted administration with sufficient computational and storage resources where all vehicles register and get their certificates for VANET usage [7].
- **Roadside units (RSU)** are an immobile infrastructure node, usually it's placed in a traffic-dense area. By caching and relaying messages for vehicles in its vicinity, or serving as a gateway to the wired network, an RSU can expand the functionality and capability of a VANET [8].
- **On Board Unit (OBU)** is a device that can provide wireless communication vehicle to vehicle. It is based on the IEEE 802.11p specifications [9].

B. Communications Types

Vehicle ad hoc network includes two communication types, as shown in Fig. 2. The system received information about the nearby vehicles and the other vehicle through V2V communication and employed it for traffic operation [2], and vehicle to infrastructure the communication between vehicles and infrastructure V2I [9]. These two types of communication serve are not only to identify and avoid hazards, but also to communicate information to the driver on all kinds of amenities.

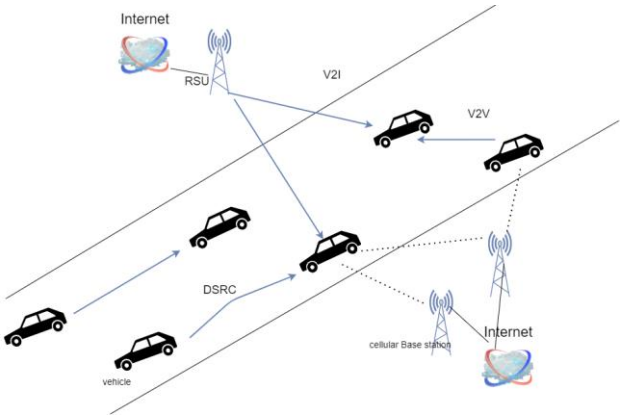

Figure 2. Vehicular ad hoc network

C. Different Messages Types

To identify the security levels to apply for the exchanged messages over the network, we classify all message types given by their criticality. These messages are segmented into three message types of level: beacon messages, alert messages, and disclosure messages [10].

- **Level 1**. When a vehicle loses control, it broadcasts an alert message to other vehicles to automatically avoid collisions.
- **Level 2.** used by the vehicle to warn nearby vehicles before changing its status of track, driving or braking
- **Level 3**. used by a vehicle in the event of poor road conditions, such as obstruction of the damaged road, the passing vehicles will broadcast warning messages to alert vehicles behind in order to remain cautious.

D. Weakness of Conventional Simulators

The most popular tools for vehicle network simulation are: Vannet, MobiSim [11], Veins and Trans [12], which connect SUMO [13] or CanuMobiSim [14], there are also computer simulators like OM net++ [15] or NS-2 [16], these can be used for road traffic simulation. But, the combination of all these tools provides a true simulation driven to a complex configuration, which targets only the network layer. Other tools integrate the road traffic, and the network layer into a simple tool like Groove sim. This tool places much greater emphasis on specific features, which limit its use to a specific researchers groups [4].

These types of simulators only target the network layer, although the only tool that integrates vehicles on a real map based on the application layer is VantSim [4], the architecture of VantSim cannot support multiple security models, it does not allow the verification of the performance and limits of the models, it is a desktop application to install in the researcher's workstation, so it does not support the simulations for a long time and manage big data.

To overcome the current limitations of simulators, we offer a highly innovative architecture for an easier use of the tool, which can be installed on the research computer or on the cloud. In addition, this tool can manage multiple security models, and evaluate the performance and limitations of the models, by performance and stress tests.

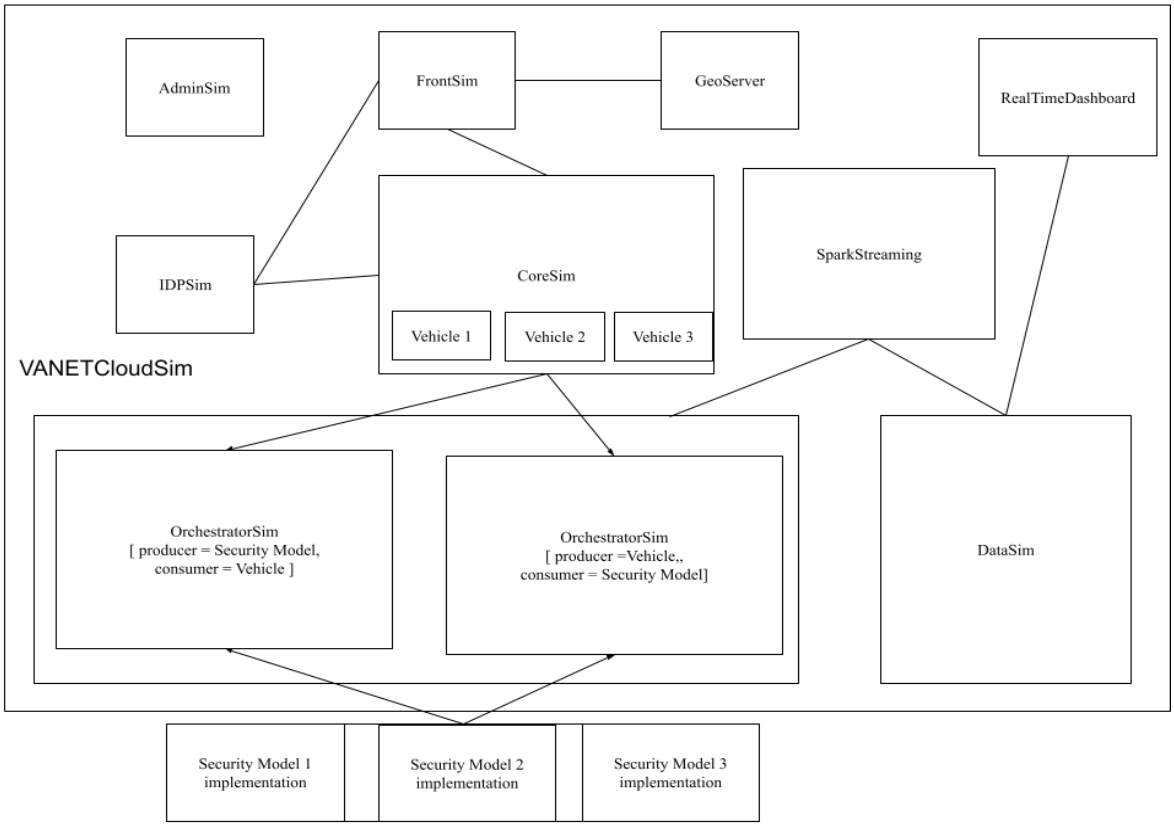

Figure 3. Global architecture.

III. Proposed Architecture

In this section, we present the overall architecture of the distributed and modular cloud simulation platform VANETcloudSim, as shown in Fig. 3.

- **AdminSim**: Presents the administration component of the platform, it allows to:
  - Manage user profile super admin, admin, researcher and supervisor, with rights assignment.
  - Manage user accounts, add, update and delete.
  - Manage vehicle, add update and delete vehicle.
  - Manage RSU.
  - Configure the test scenarios by importing the map from GeoServercity, selecting the speed and vehicles number and RSU to add them to the map.
- **IDPSim**: Identity provider Fig. 4 is a system component that able to provide an end user a single login and password (Local idp) or using Mirosoft Azure or
- Google account to access to applications, this module generates a jwt token consist of three parts separated by dots which are:
- **Header**
  The header contents two parts, the type of the token and the signing algorithm being used such as HMAC SHA256 or RSA.

{

"alg": "HS256",
"typ": "JWT"
}

- **Payload**
  The second part of the token is the payload, which contains the claims.

{"sub": "1234567890",
"name": "Abdelilah EL IHYAOUI",
"admin": true
}

- **Signature**
  The signature is used to verify that the message wasn't changing the way.

HMACSHA256(
base64UrlEncode(header) + "."
base64UrlEncode(payload),
secret)

- **FrontSim**: presents the web component of the platform, can be interfaced with GeoServer and CoreSim components and allows to:
  - Select the simulation scenario to run.
  - Display the scenario vehicles in a live map.
  - Show the V2V and V2I communication's types in an interactive way.
  - Initiate and monitor performance and stress tests in real time.
- **CoreSim**: It is a central point of the simulator, able to manage the infrastructure in a real map, it contains a database and configuration files, it stores vehicles, users and simulation scenarios, CoreSim consist of four REST interfaces in Fig. 5, each interface has an authentication API Key, this API Key used to control access for each endpoint.

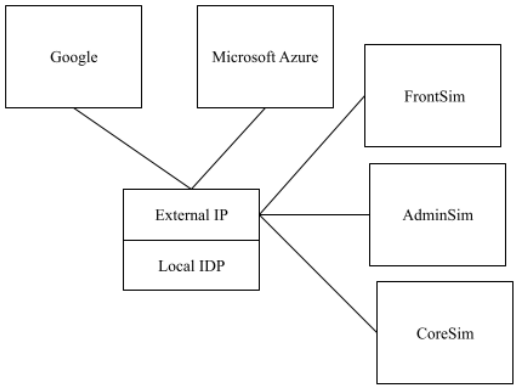

Figure 4. IDP architecture.

- IDPSim – CoreSim: exposes endpoints for authentication.
- AdminSim – CoreSim: exposes endpoints to administrate the platform.
- FrontSim - CoreSim: exposes endpoints to get vehicles and scenarios.

OrchestratorSim - CoreSim: exposes endpoints to manage vehicle to vehicle communications.

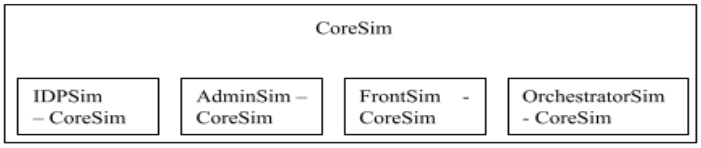

Figure 5. CorSim architecture.

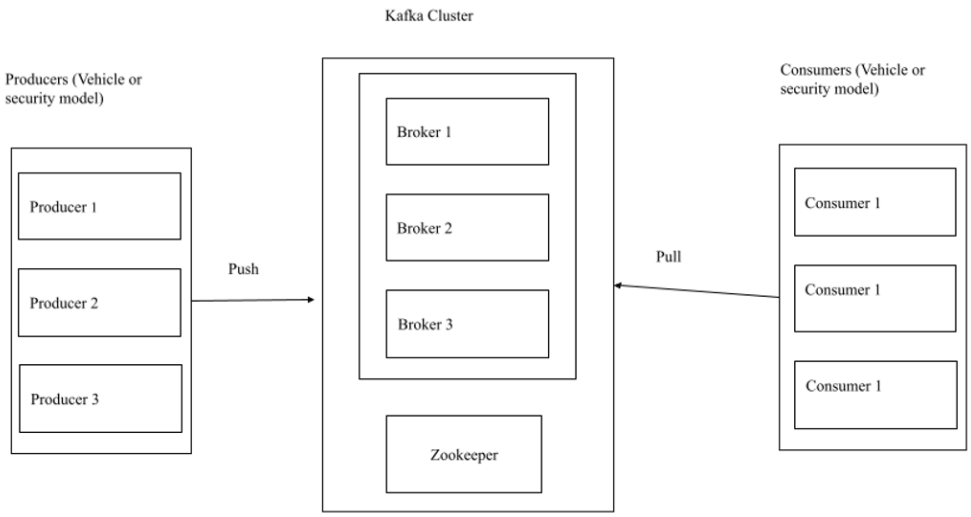

Figure 6. Architecture of OrchestratorSim.

- **OrchestratorSim:** It is an orchestrator of security models in Fig. 6, that allows security models, broadcast messages core to all security models, it logs the response time of each model, the size of messages returned by each model, so it's a bridge placed between the core and security models, contains 2 kafka clusters Sender sends message to the all security models, and receive messages by vehicle, is a distributed publish-subscribe messaging system and a robust queue that can handle a high volume of data and enables to pass messages from one end-point to another.

Kafka is a distributed messaging system developed for the purpose of the collection and a large volume of data delivery with high throughput and low latency. It is executable as a cluster on multiple servers called Kafka Cluster, and that stores streams consisting of keys, values, and timestamps in categories called topics. There are two major types of messaging models. The first is a push-type model, in which the transmitting side starts transferring data. The second is a pull type model, in which the transfer is started by the receiving side sending a data request [17].

- **Spark Streaming** has developed at the University of California at Berkeley enables scalable, high-throughput, fault-tolerant stream processing of live data streams, in our architecture the Data source is Kafka, the following diagram represent the integration of Kafka with Spark Streaming [17].

  Kafka acts as the central hub for a real-time streams of data and they are processed in Spark Streaming. Once the data is processed, Spark Streaming could be publishing results in a dashboard or DB Fig. 7.

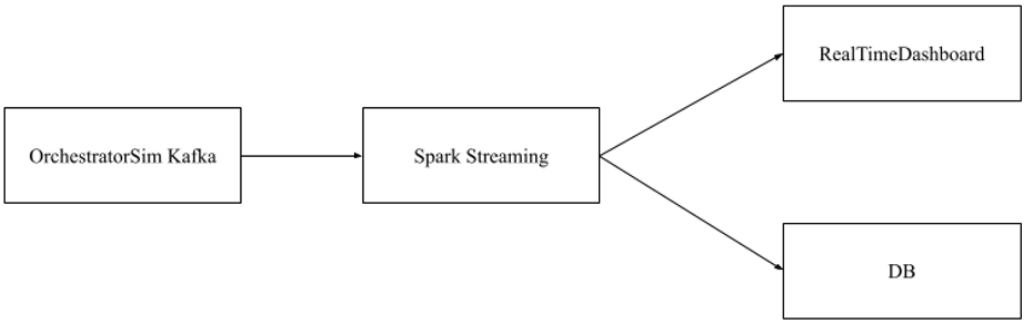

Figure 7. Spark streaming architecture.

B. Sequence Diagram of the Proposed Architecture

The following diagram in Fig. 8 shows the steps of communication with two: Vehicle 1 and Vehicle 2 by using security models to improve their performances.

- Recipient request login to FrontAPI
- FrontAPI log login event in DB
- FrontAPI redirect user to IDPSim
- IDPSim verify clientID and secret ID
- IDPSim log event in DB
- IDPSim return login page for user
- Authentication request
- IDPSim verify login and password for user
- IDPSim log event in DB
- IDPSim generate JWT token with user informations
- IDPSim return JWT to FrontAPI
- FrontAPI request Simulation configuration from CoreSim
- CoreSim load Simulation configuration
- CoreSim return simulation configuration to FrontAPI
- FrontAPI load Map of the simulation from GeoServer
- Get simulation Map in Ifram in the FrontAPI
- Launch simulation
- Launch Initialisation of Vehicle 1
- Initialisation of Vehicle 1
- Launch Initialisation of Vehicle 2
- Initialisation of Vehicle 2
- Vehicle 1 try to send sms to Vehicle 2
- OrchestratorSim for V1 broadcast the message all security models (to model1)
- OrchestratorSim for V1 log this transaction
- OrchestratorSim for V1 broadcast the message all security models (to model2)
- OrchestratorSim for V1 log this transaction
- We suppose that the first response received from Security model2
- OrchestratorSim for V1 Get secured message from security model2
- Model2 log message and the time to secure message
- OrchestratorSim for V1 send the secure message to OrchestratorSim for V2to have a real simulation, we send the first receive secure message, so to not stop the traffic in a real map.

- OrchestratorSim for V1 log transaction
- OrchestratorSim for V1 Get secured message from security model1
- Model1 log message and the time to secure message
- OrchestratorSim for V2 send secure message for verification.
- OrchestratorSim for V2 log the transaction
- OrchestratorSim for V2 Get the verified message.
- Model2 log transaction
- Vehicle 2 receive the message

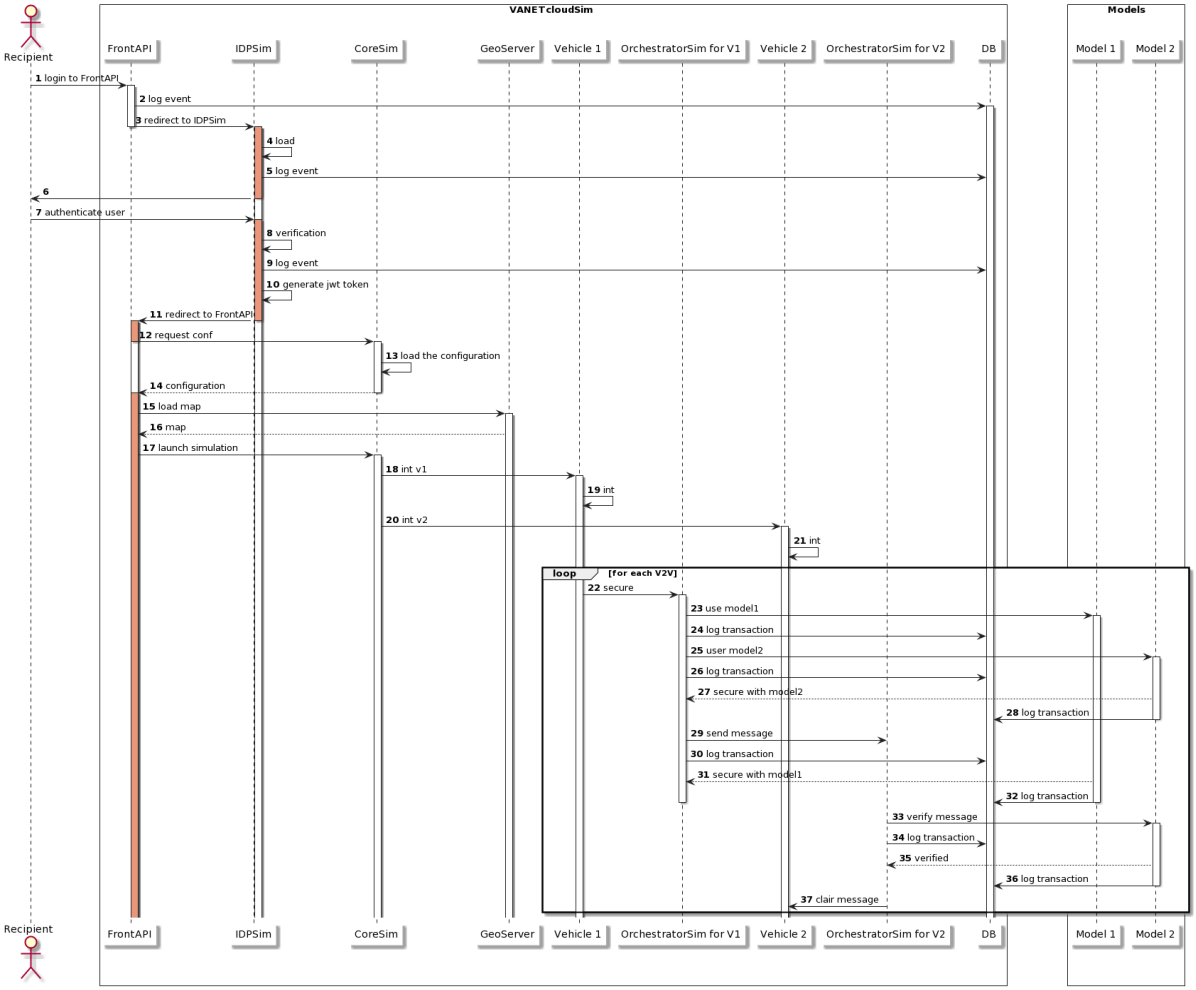

Figure 8. Sequence diagram.

IV. Evaluation and Discussion

In this section, different security models and simulators have been presented, as shown in Table I. The conventional simulators (VantSim, OM Net++ and MobiSim) are designed to simulate the specific security models on the local PC they are installed in desktop applications, which are complex to configure, so they cannot evaluate the performance and the limits. On the other, the use of the VANETcloudSim in the cloud, makes it possible to examine the performance and the limits of many security models for the application layer.

TABLE I: Security Model Simulators

Simulators	Based on real map or real scenario	Supported security models	Performance test	Application type
VantSim	yes	one security model	no	No (Desktop application)
OMNeT++	no	no	no	No (Desktop application)
MobiSim	yes	no	no	No (Desktop Application)
Proposed simulator: Vanet Cloud Sim	yes	multiples security models	yes	Yes (Modular application)

V. Conclusion

In this article, we present the architecture of a modular and distributed cloud simulation platform VANETcloudSim of vehicle communications. This platform allows performance and stress testing, in a realistic environment on a real world map, in order to study the performance and limitations of the security models. It will be improved to support the most Internet of Things IOT security models, such as the proposed model to secure IoT-based Smart Home [18], and it will be integrated into a Docker image, to manage the problem of deployment in many different environments, The platform can be deployed in the cloud and exposed REST interfaces to be used by external systems.

Our future work aims to set up the environment using an open-source technologies, we are in the process of developing all components of this models, the source code will be published in a public repository at GitHub

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

All authors conducted the research, the first author Abdelilah El IHYAOUI wrote the paper and all authors had approved the final version.

References

[1] A. Mostafa, "VANET blockchain: A general framework for detecting malicious vehicles," *Journal of Communications*, vol. 14, no. 5, pp. 356-362, 2019.

[2] E. Khoza, C. Tu, and P. A. Owolawi, "Decreasing traffic congestion in VANETs using an improved hybrid ant colony optimization algorithm," *Journal of Communications*, vol. 15, no. 9, pp. 676-686, September 2020.

[3] K. A. Hafeez, L. Zhao, and B. Ma, "Performance analysis and enhancement of the DSRC for VANET's safety applications," in *Proc. 2013 IEEE Transactions on Vehicular Technology*, 2013.

[4] V. D. Kumar, D. Kandar, and K. Sarkar, "Enhancement of inter-vehicular communication to optimize the performance of 3G/4G-VANET," in *Proc. 2013 International Conference on Optical Imaging Sensor and Security (ICOSS)*, 2013.

[5] M. S. Al-kahtani, "Survey on security attacks in vehicular Ad hoc networks (VANETs)," in *Proc. 2012 6th International Conference on Signal Processing and Communication Systems*, 2012.

[6] F. Z. Qu, Z. H. Wu, F. Y. Wang, and W. Cho, "A security and Privacy Review of VANETs" in *Proc. 2015 IEEE Transactions on Intelligent Transportation Systems*, 2015.

[7] Q. H. Bai, "Comparative research on two kinds of certification systems of the public key infrastructure (PKI) and the identity-based encryption (Ibe)," in *Proc. 2012 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, 2012.

[8] W. H. Kuo, Y. S. Tung, and S. H. Fang, "A node management scheme for R2V connections in RSU-supported vehicular adhoc networks," in *Proc. 2013 International Conference on Computing, Networking and Communications, Mobile Computing Symposium*, 2013.

[9] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for V2X communications," in *Proc. 2018 IEEE Transactions on Intelligent Transportation Systems*, 2018.

[10] Z. J. Lu, Q. Wang, G. Qu, and Z. L. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering*, 2019.

[11] W. Arellano and I. Mahgoub, "TrafficModeler extensions a case for rapid VANET simulation using, OMNET++, SUMO, and VEINS," in *Proc. 2013 High-Capacity Optical Networks and Emerging/Enabling Technologies*, 2013.

[12] M. Piorkowski, M. Raya, A. L. Lugo, P. Papadimitratos, M. Grossglauser, and J. P. Hubaux, "Trans: realistic joint traffic and network simulator for VANETs," in *Proc. 2008 ACM Sigmobile Mobile Computing and Communications review*, 2008.

[13] K. G. Lim, C. H. Lee, R. K. Y. Chin, K. B. Yeo, and K. T. K. Teo, "Modelling, simulation and computing laboratory faculty of engineering," in *Proc. 2017 IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 2017.

[14] J. H. M. Fiore, "VanetMobiSim – Vehicular ad hoc network mobility extension to the CanuMobiSim framework," 2006 Institut Eurécom/Politecnico di Torino, 2006.

[15] B. Samatha, K. R. Kumar, and N. Karyemsetty, "Design and simulation of vehicular Adhoc network using SUMO and NS2," in *Proc. 2017 Advances in wireless and mobile communications*, 2017.

[16] A. Tomandl, D. Herrmann, K. P. Fuchs, and H. Federrath, and F. Scheuer, "VANETsim: An open-source simulator for security and privacy concepts in VANETs," in *Proc. 2014 International Conference on High Performance Computing & Simulation (HPCS)*, 2014.

[17] A. Ichinose, A. Takefusa, H. Nakada, and M. Oguchi, "A study of a video analysis framework using Kafka and spark streaming," in *Proc. 2017 IEEE International Conference on Big Data (Big Data)*, 2017.

[18] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a new model to secure IoT-based smart home mobile agents using blockchain technology," *Engineering, Technology & Applied Science Research (ETASR)*, vol. 10, no. 2, 2020.