Security of Vehicle-to-Vehicle (V2V) Communication Networks

Yara Alkhalifah, Volgenau School of Engineering, GMU

***Abstract*— Security of vehicle to vehicle (V2V) become a major concern in this decade since many manufacturers adopted this new approach and implement it into their vehicles to protect the drivers, passengers, pedestrians, and vehicle as well for the safety in general. However, there are some security issues and vulnerabilities related to the systems. The Federal Bureau of Investigation (FBI) and the Department of Transportation and the National Highway Traffic Safety Administration released a warning over the increasing vulnerability of motor vehicles to remote exploits. There were many car's accidents happened to cars running this system; as an example, hackers remotely kill a Cherokee Jeep on a highway with the driver in it using a simple 3G connection (known as carjacking). There will be increasingly connected vehicles and these are a new target for attackers. Thus, there should be strongly protected vehicle communication systems. This paper discussed a new paradigm that improves current V2V communication in terms of cost, speed and most importantly the security. Vehicular Cloud Computing (VCC) is adopted by large car's manufacturer like Tesla. We will present its architecture, components, and operations. Then, we will discuss the major security requirement and possible threats and attacks with effective solutions. Finally, we propose Intrusion detection system that is designed to detect different attacks and intrusions in the VCC without depending on specific network or vehicle system. We will investigate the open issues that are not addressed yet and recommend/propose some solutions that can help to improve a safe, secure, and efficient VCC in near future.**

I. Introduction

With the vast growth of technology, the world becomes fully connected; not only humans are being connected to each other, but vehicles are also being connected together too. Researchers found that most of the accidents happen because the driver of the following vehicle cannot clearly understand or predict the actions and movements of the driver of the vehicle ahead; thus, the vehicle to vehicle communications system exists (V2V). V2V communication is the wireless transmission of data between two vehicles which can be about speed, position, or nearby accidents over ad-hoc mesh network. Also, it can be V2I communication which is the transmission of data between the vehicle and roadside infrastructure such as street lights and buildings. Vehicles can communicate with each other and with the road infrastructure to mainly improve the traffic safety and to control the congestions. This growing of connectivity delivers many enhancements in terms of driving experience, functionality, road safety, convenience, and traffic management. Simultaneously, it brings more threats and cyber-attacks; as vehicles being more connected, vehicles are more exposed to security issues.

On March 2016, the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration have released a warning to the general public and manufacturers of vehicles, vehicle components, and aftermarket devices to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles. This was because of the increasing of vulnerabilities of motor vehicles to remote exploits [1]. There were multiple attacks and vulnerabilities reported such as: in July 2015, researchers hacked into the Cherokee Jeep and they were able to remotely control the car e.g.: controlling steering, brakes, and radio volume using the 3G connection from a laptop while the car was placed on the highway ten miles away [2]. Some vulnerabilities were found in SmartGate System which is first developed by Škoda Auto in its Fabia III cars, this system allows the drivers to connect their smartphone to the car to read and display data such as the speed, fuel usage, …etc. The researchers found that attackers within the range of SmartGate WiFi can steal information about the car and disable the driver access to the system [3]. Also, many cybersecurity attacks have been demonstrated by security researchers. [4]

Besides the attacks and vulnerabilities aspect of current V2V system, there are some other limitations that may have a direct or indirect impact on V2V security. For example, the current systems with social networking activities, infotainment, location-based services, and in-vehicle multimedia demand heavy computation and large data storage. Individual cars cannot efficiently support these tasks and operation because of its constraints, it has limited storage and power capabilities. The routing will be affected and there will be a delay that could affect the driver while navigating to the destination. Also, these applications and activities require special hardware resources to support large and complex computations which costs highly. Individual vehicle with current capabilities and design cannot provide a strong protection to in-vehicle communications. Thus, the researchers have developed a new emerging computing paradigm and business model which offers the share of the information, internet connectivity and the resources to support vehicles' communications, Vehicular Cloud Computing (VCC). The VCC protects both in-vehicle communications and other connected vehicles.

II. Vehicular Cloud Computing (VCC)

A. Background

VCC was first proposed in 2010 as an extension to mobile

cloud computing [5]. VCC is a centralized solution that forms a cloud to be shared by nearby vehicles to facilitate their communication and allow them to access the resources that they need at any time. VCC protects the vehicles communication and its offered resources. There is a cooperation between vehicles, Road Side Units (RSU) and the cloud where resources are owned and handled. Each vehicle will have the access to dynamic resources such as The Data storage, Sensors, Software, and platform Computing Infrastructure. Data storage contains the contents and data generated from vehicles. Sensors will detect events from the surrounding environment and send the related information to the vehicle and to the cloud to send necessary information to other vehicles and RSU. The receiving vehicle can read the data detected by the sending vehicle's sensor.

VCC is a desirable solution because it offers many benefits in terms of its functionality, nature, and security services. For example, with the share of information between vehicles, the drivers can find a parking spot easily without wasting time and making traffic congestion. In the case of natural disasters, vehicles can share information about the nearest safe places and alarm other vehicles in the road. Regarding the security advantages, the detection of malware and attacks and the of vulnerabilities identification and assessment will be much wider and faster than current V2V because of the high speed in processing the communications and the share of information with high mobility of vehicles.

B. Architecture

VCC architecture as proposed by [6] is composed of three layers: Vehicular Cloud (VC), Infrastructure Cloud (IC), and Back-End-Cloud (BEC). VC has access to shared resources such as computing and storage. IC is initiated by RSU and these RSUs are connected together using dedicated local servers. RSUs handles some tasks such as remote navigation and traffic management with the support of road infrastructure. BEC owns the resources that can be used by vehicles such as computing and storage. Also, BEC controls some operations such as sending updates and broadcasts to the connected components, alarms monitoring, policies, media assets, and cloud members authentications and revocations. Some researchers proposed a different scheme where the cloud is initiated by the vehicles and resources of these connected vehicles will be shared together. This scheme will be similar to current V2V except for the communication and information share. In other words, we will still need efficient hardware, storage, computing resources. Also, most importantly, the security mechanisms are insufficient in their proposed scheme. The security-related operations will be discussed in the next paragraphs [7].

C. Operations

The operations in VCC scheme is different than conventional cloud operations. There should be an entity that forms or initiate the cloud, it can be done by the RSU. RSU will act as the cloud leader to invite the members in its vicinity to join the cloud and release their membership when they finished. The vehicles can respond to the request and wait for the response to be authenticated. Each vehicle will receive a unique identity and a session key that is shared between the vehicle and the RSU. After the authentication, the vehicles can access the resources and exchange their keys by the RSU and then contact each other. When the vehicle moves out of the RSU boundaries and if there is another RSU in its direction, the RSUs can exchange the vehicle's information and automatically authenticate it and join the other session with new keys. If there is no RSU, the leader will release a message that informs the cloud members of the leaving vehicle and terminates its connection and the use of resources. BEC will authenticate and control all RSUs and they will exchange information with other [6]. With BEC or RSU communications including delivering of messages and authentications functions, it provides authenticated scheme and relatively trusted compared to V2V.

III. Case Study

One of the companies that have adopted VCC paradigm is Tesla; Tesla Model S cars. The entire vehicle is managed by software from the Tesla Cloud. The cloud provider is Amazon. The car is connected to Tesla cloud using 3G connection. Tesla sends updates automatically and can fix the encountered problem in the vehicle without the driver involvement. The infrastructure behind the Tesla is capable of handling the volume of autos and data that the Cloud and the vehicles exchange. Tesla has expanded many resources to ensure the cloud is secure. The communication is encrypted, Tesla establishes a VPN directly to the car, and signs and verifies all software packages. However, In February of this year, hackers infiltrated Tesla's cloud environment and stole computer resources to mine for the cryptocurrency. Tesla spokesperson said, "The impact seems to be limited to internally-used engineering test cars only, and our initial investigation found no indication that customer privacy or vehicle safety or security was compromised in any way." The administrative portal for cloud application management, Kubernetes console, wasn't password protected; thus, the hackers were able to access the system. RedLock found that nearly 66 percent of Tesla cloud databases were not encrypted [8].

Therefore, the next section will discuss the VCC security requirements and possible issues.

IV. Security Requirements and Issues

Since there is a share of resources, there are more communication and more open channels which could be targeted by attackers. There is a risk of some common attacks like Denial of Service (DoS) attacks that affects the VCC system entirely and possibly failed it. Also, there are some possible attacks that could affect the individual vehicle. Establishing a strong and robust VCC system that protects all cloud components is very important. The related security issues should be properly addressed to offer a secure and safe system and to gain the user's trust. A high level of security is needed to be reached with minimum cost and latency. This section will explain major security requirements and some of the common attacks and possible threats that could affect these requirements. Possible countermeasures and protection

mechanisms for each type of attacks will be presented and discussed.

- The requirement: Availability

Possible Attacks: DOS, DDoS, Data loss, and Identity Spoofing
Solution: VCC DoS attacks and solutions are not yet addressed it literature; At present, some mechanisms to protect the cloud, in general, should be used.

Denial of Service (DoS) can be launched from BEC or the vehicle. This happens when the attacker floods the network by sending excessive messages which result in the unavailability of the resource. RSU/ BEC will be unable to respond to vehicle's requests and communications which may disturb the drivers while navigating to their destinations. Also, BEC will be unable to offer the needed resources and services. This type of attacks is common in cloud-based systems.

Also, it is possible to use multiple or all available sources VC, IC, and BEC to launch what is called Distributed Denial of Service (DDoS) [9].

In fact, this is can be one of the worst attacks that affect the cloud because a lot of power and resources will be consumed and when it happens, the victim will just wait until it stops. Ensuring that members can access the resources whenever they need it is essential; hence, the system should be protected to be accessible all the time. The best solution for this type of attacks is to protect it from happening in the first place and ensure that each node in the system is protected. Protection mechanisms involve: performing regular security audits to identify vulnerabilities, Intrusion detection systems (this will be discussed more in open issues section), filtering approaches, firewalls, disable IP broadcasting,
For the data loss, periodic backup plans in all components should be used. The Identity Spoofing attack is discussed in Authentication paragraph.
There are some exceptions about availability for example when the vehicle or the system needs the maintenance or updates. In this situation, the user should be aware of the vehicle's update time, and details and ensure the vehicle is secure physically and logically while updating.

- The requirement: Confidentiality

Possible Attacks: Data breach, Information Disclosure, and Eavesdropping
Solution: Encryption

The confidentiality of the system is crucial. By breaking this requirement, several types of attack could threaten the VCC system and its components. The attacker should never be able to see or know about the data stored and data being exchanged. Also, we should ensure that even if the attacker intercepts the message/data, he/she cannot decipher it or understand it. We need a strong and efficient encryption scheme that protects the contents and perform the encryption and decryption operations quickly to react to the vehicle while navigating, RSUs and other VCC system-related components. The broadcast messages such as Cooperative Awareness Message and Decentralized Environment Notification Message can be transmitted without being encrypted because they are for the public and to speed up its transmission in urgent situations. One of the proposed encryption schemes that not only ensure message confidentiality but also authenticates the identity and location of communicating is Geolock-based encryption [10]. This scheme was proposed for the vehicular ad-hoc network (VANET), current V2V, but it can be implemented for the current VCC system. This encryption scheme uses the GPS coordinates along with time and speed to encrypt and decrypt the messages. The sender and receiver should be both exist in the same location and at the same time to be able to exchange the keys and perform encryption and decryption. This practice ensures that only vehicles in the same boundaries are able to decrypt the message and read its content. This scheme assumes the vehicles use Public Key Infrastructure (PKI) to communicate. In our case, the server, RSUs will handle the exchange of keys. A hybrid encryption scheme will be used: Asymmetric encryption will be used for shared key exchange and Symmetric encryption for the communication. The Symmetric encryption is desired because of the fast speed that is needed in vehicles' communications and for the server (RSU) exchange of keys operations with other vehicles. This scheme assumes the data is protected against modification and tampering.

- The requirement: Integrity

Possible Attack: Data modification, and tampering; Man-in-Middle attack
Solution: Discussed in Authentication paragraph

Ensuring that data sent and received is not altered is very important. Many types of attacks could affect data integrity by either stealing the data and alter it or steal the identity of the user and pretend to be the original sender to deceive the receiver. In VCC, we should ensure that users cannot alter the shared data such as altering the vehicle location after an accident or delete it. The messages should be encrypted and the users should be authenticated to protect data from being altered.

- The requirement: Authentication

Possible Attack: Identity Spoofing
Identity spoofing happens when an unauthorized user takes someone's else identity.

Solution: Authentication in VCC must meet a set of metrics that qualify a user to join and use the cloud. The metrics: each vehicle should own a unique identity, each vehicle should know unique things such as password or keys, and the use of biometrics like face, voice recognition, and fingerprints. The use of metrics only is not sufficient without a control. The issue of VCC is the vehicles are on a permanent move in a high speed and there will be a frequent change of vehicle's location and the use of different RSUs along the route. The selected scheme consists of three stages: preliminary system establishment, identity authentication, and private communication construction [11]. In the preliminary system establishment, the trust authority (TA) will generate the parameters for each vehicle. The certificate authority (CA) will initialize the parameters for RSU and the vehicles. The parameters: Public key, private key, data key, and message signature. The parameters of TA can be set through many procedures involve random key generation and hash functions.

In the identity authentication stage, the vehicle/user will request RSU to be authenticated. If accepted, RSU will assign a temporary anonymous ID and a parameter. Then, the vehicle will encrypt the parameter with the previously provided public key and sent the ciphertext to RSU to complete identity authentication. The RSU through several steps and operations will verify the identity. After authentication achieved, RSU will store the vehicle identity and keys in the cloud and other authenticated devices/vehicles can communicate easily and securely. Then, the final stage is the vehicle/user can query cloud information through the exchange of encrypted messages and will be able to share and upload data to the cloud. The selected scheme uses symmetric encryption to reduce the calculation of encryption/decryption and the time complexity in private communications. The authors show that their scheme fulfills the requirements of not only authentication but also confidentiality, authentication, non-repudiation, conditional anonymity, and conditional intractability. Also, the performance of processes and operations shows good results in term of execution time. This scheme can be cooperated with Geolock scheme.

For the identity, some authors proposed a digital identity method, DIVA [12]. This scheme uses the identification of the vehicle (VID) and the driver (DrL) to form a new digital identity. For example, the DMV can be used here for the vehicle registration authority and the driver license authority, each has its separate processes and authentication and should be linked to the cloud. The authorities will issue a token and secret key with each of identities. Thus, if the keys compromised or stolen, the tokens will be still protected. The tokens can only be traced by the authorities. The authorities can inform the cloud management to take the steps to prevent the compromised or expired from using the cloud and inform the members of possible threats of communicating with the vehicle.

Some other requirement such as non-repudiation is possible to be broken in VCC. Repudiation happens when the attacker or user denies the responsibility of any action done by him/her. Digital signature and auditing are the countermeasures. Also, the previously selected scheme shows the strength against repudiation attacks.

- The requirement: Privacy

The share of information should be controlled in what to share, and to whom. The privacy is a crucial matter in the cloud because there may be many participated entities: vehicles, vehicles' manufacturers, DMV, RSU, Cloud providers, …etc. The PTVC scheme can be used to achieve a privacy-preserving and trust-based verifiable for VCC. This solution involves four phases: system setup, privacy-preserving trust-based vehicle selection protocol, privacy-preserving verifiable computing protocol, and trust management. Their analysis shows that PTVC is privacy-preserving and robust against several various attacks and effective in terms of computational cost [13].

V. Proposed Solution

One of the powerful mechanisms against attacks is the Intrusion Detection System (IDS). Intrusion Detection Systems (IDS) can differ in design by [25]:

Architecture: It can be *centralized* where the analysis can be performed on particular number of locations or it can be *distributed* through many locations within the network.
Environment: It can be a *Wireless* or *Wired* network.
The Data Source: It can be a *host-based* which monitors the activities and events of a single host only,
a *network-based* which monitors the traffic of a particular network, or a *hybrid* which is a combination of the previous two IDS.
The Detection Method: It can be a *Signature-based* that detects or matches particular pattern/signatures from the database with gathered data or the detection can be *Anomaly-based* which detects attacks by distinguishing between normal and anomaly activities.
Time of the Detection: It can be *Online IDS* which detects attacks on real-time or *Offline IDS* which detects attacks by performing post analysis of gathered/collected data.
The reason for mentioning this background is to have a clear outlook on the concepts that will be discussed next.
There is limited literature about IDS for VCC. I proposed a scheme that can help in detecting the attacks/threats in its earlier stages and preventing its impact on the entire cloud without depending on special software or hardware and does not target a particular network or protocol. Since we have the shared resources and libraries in our VCC communication system, referring to the shared library always while detecting intrusions will consume an amount of power and may cause a delay. Furthermore, the centralized defense system which exists in the cloud cannot detect host attacks because most of the communication will be encrypted and network level. We can have an adaptive and *Online* (real time), *knowledge-based*, *signature-based* and *anomaly-based*, *distributed* and *centralized* IDS in the vehicle, RSU, and BEC. The individual distributed IDS in each node learns the behavior of each individual component and network, store the normal activities to compare it against abnormal behaviors and then it can share its detections and collected signatures with the cloud. Because of the heterogeneity issue (will be discussed in open issue section), the existing systems may have a difficulty in handling different network and vehicle characteristics and it will be challenging to design many systems for each of these different components. The knowledge-based system will depend on the connected device and monitored network characteristics to detect the attack which means if there is a specific designed attack that targets individual system, the knowledge-based system can detect it. Some vehicles or RSU may fail to detect the attack and report it to the cloud because it doesn't target it. In the distributed IDS each vehicle will protect itself depending on its behavior and characteristics that may not share with others. The centralized IDS that exists in the cloud can be used and shared by all components and it has the largest up-to-date database of malware and signatures. Also, since VCC network protocols and standard mediums are heterogeneous, this IDS can learn and collect knowledge about the features of different networks and use this knowledge in detecting the attacks. This IDS has four components, first is the communication system that listens to the traffic in the different communication medium. The second component is the storage unit that imports the events from the communication system and logs it. The third is the most

important and largest component: a knowledge base that learns the behavior of different activities in the logged traffic. There can be multiple bases each for different source and type of traffic. The fourth component is the management unit that takes action after it compares the logged traffic against the signature and normal behaviors in the knowledge database. Then, these actions and data are shared with the cloud to inform other VCC components about the latest threats and attacks. This scheme combined with the discussed solutions like GeoLock encryption and DIVA can protect the VCC system. If we have only the shared IDS that is offered by the cloud, there is an issue in detecting the attacks without compromising the confidentiality and privacy of the data.

The proposed distributed and host-based IDS will help in detecting attacks because the decryption will be in the host/vehicle node; it won't compromise the confidentiality nor the privacy. Also, if one vehicle system failed to detect or mitigate the attack, we still have other distributed defense systems. It is adaptive; thus, there will be no issue in any protocol or standard used in different vehicles from different manufacturers and systems. This solution does not require any additional settings, capabilities or changes to the existing architecture and application because it is a knowledge-driven.

This solution will be investigated more on future personal research.

VI. Open Issues and future research

Vehicular Cloud Computing is a new technology solution that has some issues and questions that are not addressed yet in literature or by responsible authorities. There are some open issues that may have a direct or indirect impact on the security of VCC such as high mobility, heterogeneous characteristics including network access, …etc. This section will focus on open issues.

First the cloud itself, the cloud is a new technology that brings many opportunities and improvements which are adopted by many fields; however, it has some issues that are not properly addressed. Availability and auditing are one of the major cloud issues in VCC because as mentioned previously many entities participated in cloud management. Up to now, there are three major cloud providers: Amazon (AWS), Microsoft Azure, and Google Cloud platform. The cost of this current VCC will depend mostly on cloud usage or rent and the providers' prices. The dependency on service providers may bring many issues in VCC. These issues can be defeated by establishing the standards and regulations for both vehicles' manufacturers, the cloud provides, and vehicle's operators/drivers. There is a lack of the operational standards, regulations, and policies in VCC solution. V2V communication system received a great attention from the U.S. Department of Transportation. Hopefully, this work is extended to include cloud and vehicular cloud technologies in near future.

Another issue is the high mobility of heterogeneous vehicles. The control and management of vehicles that are on a permanent move, high speed, and connecting to cloud from different networks that use different communication standards such as Wi-Fi, DRSC, 3G, 4G, and future 5G is challenging. This heterogeneity is challenging for attackers too; attackers will need specialized tools for VCC system, which network is used to connect, and a difficulty in targeting a particular victim. However, the coming 5G technology promises for great development. The handling of operations in the cloud will improve in terms of speed, consumed power, amount of computations and data, and security.

The attacks that targets VCC specifically are not addressed yet because as its mentioned previously this field is new. The only reported attack was the Tesla cloud hacking and as it is mentioned the hack was due to the lack of password protection mechanisms. In other words, the attacks that are designed to attack VCC systems and which depend on VCC design and characteristics are not exists or addressed yet.

VII. Conclusion

In this paper, we have discussed vehicle to vehicle communication system and its issues. Then, we have presented a recent new promising solution which is Vehicular Cloud Computing and explained its architecture, components, and operations. A case study about Tesla cars presented as well. Then, we moved to the main part which is the security of VCC and its threats, along we presented some possible solutions to protect the cloud and its component. Finally, we have investigated the open issues that are not addressed yet in literature and we have suggested some possible solution that could be implemented to improve the VCC. Future personal research will go deeper into the proposed scheme of the adaptive, knowledge-based, and hybrid IDS.

References

[1] "MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS," *Internet Crime Complaint Center (IC3)*, 17-Mar-2016. [Online]. Available: https://www.ic3.gov/media/2016/160317.aspx. [Accessed: 01-Oct-2018].

[2] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway-With Me in It," *Wired*, 20-Nov-2018. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 11-Oct-2018].

[3] "Is Your Car Broadcasting Too Much Information?," *TrendLabs Security Intelligence Blog*, 12-Aug-2015. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/. [Accessed: 09-Oct-2018].

[4] M. Hashem Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," in *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45-51, June 2017.

[5] 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*, 2010.

[6] Ahmad, F., Kazim, M., Adnane, A., Awad, A., 2015, Vehicular Cloud Networks: Architecture, *Applications and Security Issues*, Proc. IEEE/ACM 8th International Conference on Utility and Cloud Computing, Limassol, Cyprus.

[7] E. Lee, E. Lee, M. Gerla and S. Y. Oh, "Vehicular cloud networking: architecture and design principles," in *IEEE Communications Magazine*, vol. 52, no. 2, pp. 148-155, February 2014.

[8] L. H. Newman, "Hackers Enlisted Tesla's Cloud to Mine Cryptocurrency," *Wired*, 21-Feb-2018. [Online]. Available: https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/. [Accessed: 1-Dec-2018].

[9] S. Haase, “The 12 biggest cloud security threats in 2018,” *INSUREtrust*, 03-Apr-2018. [Online]. Available: https://www.insuretrust.com/the-12-biggest-cloud-security-threats-in-2018/. [Accessed: 14-Nov-2018].
[10] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular adhoc networks," *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, Macau, 2009, pp. 804-809.
[11] H. Wu and G. Homg, "Vehicular cloud network and information security mechanisms," *2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE)*, Tainan, 2016, pp. 196-199.
[12] K. Zaidi and M. Rajarajan, “Vehicular Internet: Security & Privacy Challenges and Opportunities,” *Future Internet*, vol. 7, no. 4, pp. 257–275, 2015.
[13] C. Huang, R. Lu, H. Zhu, H. Hu and X. Lin, "PTVC: Achieving Privacy-Preserving Trust-Based Verifiable Vehicular Cloud Computing," *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, 2016, pp. 1-6.
[14] D. Midi, A. Rullo, A. Mudgerikar and E. Bertino, "Kalis — A System for Knowledge-Driven Adaptable Intrusion Detection for the Internet of Things," *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Atlanta, GA, 2017, pp. 656-666.
[15] W. Stallings, *Cryptography and Network Security Principle and Practices*. New Jersey, NJ, USA: Pearson Prentice Hall, 2017.
[16] T. Zhang and L. Delogrossi, *Vehicle Safety Communications: Protocols, Security, and Privacy*. Hoboken, NJ, USA: Wiley & Sons, 2012.
[17] W. Chen, *Vehicular communications and networks : architectures, protocols, operation and deployment.* Cambridge, England: Woodhead Publishing, 2015.
[18] National Highway Traffic Safety Administration, “Cybersecurity Best Practices for Modern Vehicles,” Report No. DOT HS 812 333, Washington, DC, Oct 2016. [Online]. Available: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModern Vehicles.pdf
[19] V. Vijayenthiran, “Cadillac announces V2V communications, just as CIA hacking allegations emerge,” Motor Authority, Mar 10, 2017. [Online] Available: https://www.motorauthority.com/news/1109299_cadillac-announces-v2v-communications-just-as-cia-hacking-allegations-emerge
[20] J. Zhou, Z. Cao, X. Dong and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," in *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26-33, January 2017.
[21] L. Maglaras, A. Albayatti and H. Janicke "Social Internet of Vehicles for Smart Cities," in *J. Sensor and Actuator Networks*, vol. 5, no. 3, February 2016
[22] Consumer Reports, "Vehicle-to-vehicle communication can prevent crashes," Apr-2012. [Online] Available: https://www.consumerreports.org/cro/magazine/2012/04/vehicle-to-vehicle-communication-can-prevent-crashes/index.htm
[23] H. S. Hassanein, S. Abdelhamid and K. Elgazzar, "A framework for vehicular cloud computing," *2015 International Conference on Connected Vehicles and Expo (ICCVE)*, Shenzhen, 2015, pp. 238-239.
[24] M. Aloqaily, B. Kantarci and H. T. Mouftah, "Vehicular clouds: State of the art, challenges and future directions," *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Amman, 2015, pp. 1-6.
[25] F. Sabahi and A. Movaghar. Intrusion detection: A survey. In *Systems and Networks Communications, 2008. ICSNC’08. 3rd International Conference on*, pages 23–26. IEEE, 2008.