2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)
Workshops - W3: Second Int. Workshop on Time-Critical Cyber Physical Systems

An Overview on Security and Privacy Challenges and Their Solutions in Fog-Based Vehicular Application

Zeinab Bakhshi[1], Ali Balador[1,2]
[1]Mälardalen University, Sweden, {zeinab.bakhshi, ali.balador}@mdh.se
[2]RISE SICS Västerås, Sweden, ali.balador@ri.se

***Abstract*—Fog computing is an emerging computing paradigm that extends cloud services to the edge of the network by moving computation tasks from cloud to network edges to reduce response latency in a wireless network. Fog computing inherits the principle of peer-to-peer networking, decentralization, and geographical distribution from clouds. Hence, fog computing becomes an ideal platform for readily supporting vehicular applications due to its dynamic support for mobility of client-devices and low latent heterogeneous communication capabilities. Despite many advantages, a multitude of security and privacy issues affects the platforms and renders it as a target for unknown adversaries. This has significant implication in the development of safety critical applications, such as vehicular cloud and intelligent transportation system. This paper presents, an overview of existing security and privacy vulnerabilities in fog computing, particularly in vehicular networks. Moreover, state-of-the-art security and privacy solutions for fog based vehicular networks are analyzed. In conclusion, open challenges and future research directions are discussed.**

I. Introduction

Internet-of-things (IoT) and cloud services tremendously improved the functionality of automobiles from being a medium of transportation into a smart autonomous platform fulfilling transportation and infotainment requirements in an efficient and sustainable way. Recent estimates show that autonomous vehicles generate a massive amount of sensor data (cameras, radars, LiDARS, telematics) in magnitude of 1 GB/s [1], which is multiple thousand times more than that of a typical smart phone serves, it presents big challenges for the car companies to send the data back to the cloud for real-time analysis, testing and additional training for smooth operation. Even with the upcoming 5G infrastructure, transferring such massive amounts of data will be very expensive and presents a level of risk because cloud services are often provided by a third party cloud provider. Also, cloud services suffer from large latency and jitter due to their centralized resource management, and thus may not be suitable for real-time applications in Vehicular Ad-Hoc Networks (VANETs) [2].

To address these issues, a possible solution is using Fog Computing (FC). The FC paradigm place computing resources at network edges to extend the cloud computing paradigm to enable services to devices within a one-hop access network [3]. FC enables data processing at the network edge. A vehicular network edge consists of end routing devices - Enhanced Node B (eNodeB), Wireless Access Points (WAP), Road Side Unites (RSUs) [4], edge routers, border gateways, wireless set-top boxes, network bridges and cellular base stations [5]. Edge devices are installed with dedicated server setups which are capable of enabling fog technologies [6]. Furthermore, FC has special attributes: a) physical Geo-distribution; b) facilitating mobility; c) heterogeneous connectivity; d) real-time operation and e) service localization. Vehicular fog computing extends the FC paradigm of conventional vehicular networks to overcome limitations, such as latency, location awareness, and real-time response, which is typically required in applications like smart traffic control and safety critical applications [7].

However, FC faces trust issues [8], and also suffers from classical security and privacy issues like data leakage, unauthorized access, unwanted code/malware injections, etc. [9]. On the other hand, traditional security and privacy solutions cannot be readily applied to the new FC paradigm considering characteristics, such as support for mobility and wide-area distribution [2]. There are many dimensions that should be considered in a security solution for vehicular fog computing, such as scalability, data consistency and trust in fog service providers.

In this paper, we identify security and privacy vulnerabilities in a fog-based vehicular system and then we investigate proposed security and privacy solutions for fog-based vehicular applications and scenarios. Moreover, we map existing solutions with highlighted vulnerabilities, to identify open research challenges and future research directions. The rest of this paper is organized as follow: Section II discusses vulnerabilities for fog-based vehicular systems. In Section III, we provide a summary of proposed security and privacy solutions and suggestions for fog-based vehicular systems. In Section IV we identify open research challenges and issues. Finally, Section V contains the conclusions.

II. Security and Privacy Vulnerabilities

In this section, we discuss the vulnerabilities in a fog-based vehicular system, including resources and

978-1-5386-9358-2/19/$31.00 ©2019 IEEE

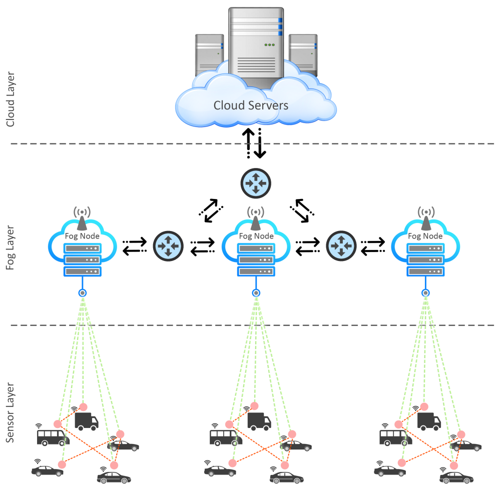

Fig. 1: Fog-based vehicular system.

services to address the challenges caused by these vulnerabilities.

As Figure 1 shows, a fog-based vehicular system consists of three main layers, cloud, fog and device (vehicle) layers. Fog nodes provide three main services including: 1) data storing, which is the fundamental service for storing data to share and process them; 2) data processing, which is the computation and processing tasks on data in the fog and 3) data sharing, which is sharing of data among system users. We consider all these three services as shared resources in the fog. Fog nodes have connections with clouds, other fog nodes and vehicles.To communicate with other entities, identity and access to shared resources are required. As consequence, we summarize the security vulnerabilities into three categories, as follows:

A. *Shared Resources Vulnerabilities:*

- **Lack of Control of System Logs**: when the system cannot log all necessary data and required logs, the system will be vulnerable to denying algorithm and transactions. In a fog-based vehicular system, denying transaction (receiving/ sending data) will force the system to resend the data, which consumes fog resources and at the same time increases latencies [10].
- **Ineligible Data Changes**: data stored in fog servers are accessible by many parties, e.g., cloud and fog service providers, Original Equipment Manufacturers (OEMs), drivers and passengers. Therefore, the system could be compromised by ineligible changes in data storages or repositories of fog server [11].
- **Data Hostages**: another vulnerability to any system, which is connected to Internet is data hostage. Ransomware and crypto wall are two potential attacks for this vulnerability. This Vulnerability stems from open access option and lack of or weak cryptographic algorithms.
- **System Overloading**: fog servers are resource constrained, therefore, if the number of requests for computation or access to fog resources increases more than the system capacity, the performance decreases. Then the system will be overloaded or crash, which will lead to data loss, latency and service unavailability [10] [11].
- **Ineligible Resource Requests**: in addition to system overloading with legible request, there is another vulnerability, called ineligible resource request. Increasing the number of fake or rogue requests to use system resources, will make the system unable to serve the eligible requests. This happens when some parties aim to decrease the system performance or make it unavailable for legible users [12].

B. *Data Communication Vulnerabilities:*

- **Intercepting the Data**: any communication can be subject to interception. This can happen when the channel is not secured or encrypted or when the encryption methods are not efficient enough to protect the communication channel from being intercepted by intruders [11].
- **Data Modification During Data Transmission**: this vulnerability can stem from weak channel encryption algorithms or an unencrypted data communication channel, which allows ineligible parties to modify or change the data. This vulnerability might causes system malfunctions, which can endanger the safety of driver, passenger(s), as well as pedestrians [12], [13].
- **Stopping Communication**: this happens when data cannot be transferred through the communication channel. Environmental noises and jamming can cause this vulnerability and thereby bidirectional communication between other entities and the fog system will be interrupted [13], [10].
- **Bandwidth Overhead**: this happens when the bandwidth of the system is not utilized effectively based on the number of user requests for transferring or accessing data. One of the main reasons that causes bandwidth overhead is inefficient cryptographic and authentication methods [13].

C. *Identity and Access Control Vulnerabilities:*

- **Fake Identities**: when the authentication or authorization mechanisms cannot detect fake and forgery credentials the system will be vulnerable to malicious commands [14].

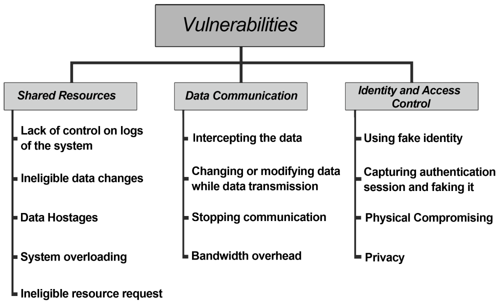

Fig. 2: Security vulnerabilities in fog.

- **Faking, Captured Authentication Session** : the identification session can be compromised by forgery parties and then replayed by ineligible parties [15].
- **Physical Compromising**: in a fog-based vehicular system, there are fog nodes, which are located in public areas like roads or streets. Hence, these fog nodes are vulnerable to physical compromising [16].
- **Privacy**: disclosure of confidential and non-confidential data of vehicles, drivers, OEMs and service providers can be used to launch an attack by adversaries [8], [17], [18].

Figure 2 also present an abstract of aformentioned vulnerabilities for shared resources, communication and identification in fog computing.

III. Security and Privacy Suggestions and Solutions

In this section, we investigate proposed solutions and suggestions focusing on security and privacy of fog-based vehicular systems in order to identify open challenges and issues.

A. *Shared Resources Solutions*

The most common objectives of papers proposed security solutions for shared resources in fog, are: a) detecting abnormal behaviours; and b) blocking malicious requests. For instance, [19] proposed an Intrusion Detection System (IDS). The proposed model is capable of detecting: a) abnormal resource requests; b) misuse of resource request rules; and c) requests that reduce system performance. Based on these mechanisms, malicious requests and activities are filtered. In [20] and [21] they use machine learning algorithms to detect abnormal behaviours and cyber-threats.

Authors in [20] introduced a proactive anomaly detection for hijacked connected cars to improve cyber-resilience. The authors utilize a new data set file for connected cars to facilitate data collection and sharing, together with analysis of travel routes in real time to proactively detect malicious behaviours through a Bayesian estimation technique, called Kalman filter. Levi et al. [21] proposed a machine learning method based on Hidden Markov Models (HMM), to detect cyber-threats against connected vehicles. The detection system monitors requests from different parties, and compares the requests with predefined policies to detect anomalous activities. Comparing to previous studies, the proposed method aims to monitor different data flows in a vehicle, for instance, Vehicle to everything (V2X) network, operating system and in-vehicle traffic. Moreover, training data for malicious behaviour detection can be applied to multiple cars with the same characteristics.

To cope with challenges, such as resisting malicious vehicles, avoiding heavy roadside sensors and single-point of failure, the authors in [22] proposed two secure intelligent traffic light control schemes using FC whose security are based on the hardness of the computational DiffieHellman puzzle and the hash collision puzzle, respectively. The efficiency of both approaches were compared when the number of vehicles increases. The results showed that the first method, DiffieHellman puzzle, is not efficient for high density scenarios. To overcome this issue, the second security method, hash collision puzzle, was proposed to reduce the computation and communication overhead in fog nodes by performing lightweight operations.

Authors in [23] propose an integration between VANETs, Software Defined Network (SDN), and 5G for a resilient VANET security design approach. They showed how their approach can defend the system against different type of attacks, such as Distributed Denial of Service (DDoS) and IP Spoofing, and how the system trace back the source of an attack. Moreover, they showed that their proposed system is capable of maintaining low overhead and minimal configuration, while enforcing different levels of real-time user-defined security.

Although authors in studied works address security solutions to detect and prevent cyber-attacks against shared resources in fog-based vehicular system, it is also observed that scalability issues are not considered. For instance, in [23] they considered only a small number of vehicles in the simulation which argues for lacking scalability. Another open issue is the effect of external factors in the proposed solutions. For instance, [20] and [21] disregard the impact of abnormal activities from other parties and detection of malicious behaviour for cars with different characteristics, respectively.

B. *Data Communication Solutions*

Solutions proposed for secure data communication are mostly based on encryption methods. Communication channel encryption and message encryption are the main solutions provided in papers studied in this subsection. For instance, Arif et al. [24] proposed a secure communication method between fog and Location Based Service (LBS), which is located in the cloud, of a vehicular environment. LBS is a service to use the real-time geo-data in mobile devices. In this method, message encryption in vehicle and fog side is performed to ensure security of data and sensitive information like location information. To prevent data disclosure in fog nodes, data are sent to fog servers anonymously. In addition, to protect data in case the fog servers are compromised, messages are encrypted before being communicated.

A different approach is proposed in [18] to measure system efficiency in fog-based automated vehicles, considering security, privacy and dependability. For this reason, the authors proposed a crowd-based intelligence approach that is inspired from swarm intelligence, called SHIELD [25]. SHIELD is based on a decomposition of the system into subsystems and selects suitable configurations for each component based on the component values of weight. Data communication between fog and vehicles are secured by authentication and encrypted methods.

In [26], a secure framework for exchange of authentication keys in a vehicular system has been proposed. Fog nodes are used to reduce latency of message authentication, message communication process and key exchange. In order to begin message communication, a key exchange process in fog nodes is required. In addition, an expiration time for processing key exchange requests is defined to prevent vehicles from doing malicious activities. Encryption methods increase data protection, but using encryption algorithms might also increase processing time and communication cost [24]. In addition, in [26] security of fog nodes against attacks, like node compromising, remains a challenge that might cause trust issues related to storing and transferring keys.

C. Identity and Access Control Solutions

Privacy preserving, authentication, authorization and access control methods are proposed as solutions for security issues against identity threats in a fog-based vehicular network. For instance, Fog Vehicular Crowd Sensing (FVCS) applications, considering, security and privacy are discussed in [8]. In this approach when a fog node receives a crowd sensing report data, it can check whether the data is duplicated or not without knowing the details of the report and its content. Regarding security challenges, such as authentication and data disclosure, a proxy encryption [29] is proposed to realize the confidentiality of sharing data. For authentication issues, a trusted authority (TA) is involved for key management task in vehicles and FVCS users. In [27], authors proposed a novel fog-to-cloud-based architecture for data sharing in Vehicular Cloud Computing (VCC). Their method is a cryptography-based mechanism for data sharing in vehicular environments. The fog and cloud servers are responsible for the complicated computation part with confidentiality and privacy preservation. Fog nodes do not have access to decrypted data which provides a confidentiality level in FC. Experiments showed significant performance improvement in response delay reduction and edge devices' overhead minimization.

Huang et al. [16] focused on passive attacks and proposed two security methods. The first one, called the evidence-based digital forensic approach, detects the abnormal behavior of fog nodes by forensically analyzing and monitoring of data and requests from both vehicles and fog nodes. The other one, called the traffic-based analysis approach, uses big data analytics and deep learning algorithms to detect abnormal behavior of fog nodes based on data gathered in the cloud servers. Moreover, they evaluated the performance of the proposed methods through simulation experiments. The results showed that a compromise attack can be mitigated by proposed approaches.

Zhang et al. [30] provided a comprehensive survey of access control of users' data for fog computing focusing on security problems and challenges. They described seven access control models and for each one, possible applications in FC are discussed. These models are as follows: 1) Discretionary access control (DAC) model; 2) Mandatory access control (MAC) model; 3) Role-based access control (RBAC) model; 4) Attribute-based access control (ABAC) model; 5) Usage-control-based access control (UCON) model; 6) Reference monitoring access control (RMAC) model; and 7) Proxy re-encryption (PRE) model. Suggested access control methods in this work help fog service providers consider access control policies based on requirements for different applications. However, threats and security issues, for instance, fog node compromising and data theft in fog level still remains a challenge [27] [16].

IV. Security and Privacy Open challenges

The cloud computing is heavily protected by cloud operators, however, this cannot be easily extended for FC [2]. As we showed in the previous section, a number of studies have already focused on security solutions for FC and especially for vehicular environments, including intrusion detection systems in fog nodes, key management mechanisms, compromised node detection methods, authentication and authorization techniques to access fog resources. However, these approaches are either partially addressing the security and privacy issues or are still in very early stages. Table I summarize the focus of each paper in the collection of papers studies in previous section.

TABLE I: A summary of security and privacy suggestions and solutions

		Security Challenges				
Paper	**Vehicular Application**	**Shared Resources**	**Data Commu-nication**	**Ident-ification**	**Solution**	**Open Challenge**
Huang et al. [16]	✓			✓	Digital forensic	Performance evaluation
Hussein et al. [23]	✓		✓		-Authentication and Authorization -Attack detection	Short-term communication
Sohal et al. [19]		✓			-Monitoring resource request activities -Detecting abnormal behaviour with IDS	Performance evaluation
Al-Khateeb et al. [20]	✓	✓			Threat detection using ML algorithms	Resource constrains
Kontorovich [21]	✓	✓			Threat detection using ML algorithms	Resource constrains
Liu et al. [22]	✓	✓			Location-based encryption	-Privacy issues -Resource constrains
Chaba & Dave [26]	✓		✓		Authentication key exchange	Bandwidth limitations
Ashish & Shrestha [18]	✓		✓		System decomposition (SHEILD)	Short-term communication
Arif et al. [24]	✓		✓		Fog anonymizer using LBS	Bandwidth limitations
Zhang et al. [8]	✓			✓	Data duplication removal	Log auditing
Xue et al. [27]	✓			✓	Access control schemes	Data theft in fog nodes
Basudan et al. [17]	✓			✓	Signcryption for privacy	Exploiting credentials
Hua et al. [28]				✓	Cryptosystem for privacy	Proximity limitations

Open challenges for shared resources, data communication and identification security vulnerabilities are briefly presented in the table. Resources constrains, bandwidth limitations, mobility characteristic, scalability, etc. are not completely addressed in proposed security solutions for fog computing in the literature. This section outlines open research challenges in fog security and privacy, especially for vehicular applications.

A. *Shared Resources*

- Data processing in FC should be more efficient and real-time comparing to the similar one for clouds. However, for the identity and data access security issues, many encryption and authentication methods are proposed which provide significant reduction of computational processing time. Therefore, significant research for new light weight encryption algorithm with minimal effects in computational costs are required.
- Fog nodes, as a source of services, should be protected against software errors. These errors are due to different problems. For instance, errors in source codes or malware injections [31].
- Another open challenge is data backup and recovery, when data corruption or data hostage happens to fog resources data backup and recovery modules can help all parties benefit to restore damaged data and keep operation with minimum service disruption.
- There should be a trade-off between the service provided by fog and its features to vehicles and sufficient resources that is designed for the fogs. Despite the fact that the level of functionality is very important in fog services, system performance is very dependent to the requests and services that fog nodes are offering to the vehicles in the system [32].
- Managing logs in heterogeneous vehicular system in a fog network is very challenging. A huge volume of logs, auditing, processing and analyzing them are the instances of issues that require further researches [33].

B. *Data Communication*

- Encryption and authentication procedures has been proposed or suggested to address data communication security issues like data interception or rouge node attacks. However, in a fog-based vehicular system, a connection between a fog node and a vehicle is established only for a short time, which raises difficulties in identifying vehicles in fraction of time [34].

- Large number of connection requests in a vehicular system is another challenging issue, which is a constraint in serving real-time response to legible requests [35].
- Fog nodes in autonomous vehicular system applications are constructed to help latency issues in the network, latency issues will cause safety issues like accidents. On the other hand, if the data traffic is higher than bandwidth capacity then there will be an overhead in communication channel. Bandwidth utilization and communication overhead as a security threat requires more researches in future studies
- Disruption in communication by surrounding noise to be transferred in a communication channel is one of the challenging issues that can stop the whole system and will bring disastrous safety and security issues in a fog-based vehicular system.

C. *Identity and Access Control*

- Fulfilling vehicles and their users privacy by anonymity at the same time, auditing identification and authorization processes to control data access and authentications is one of the important open challenges in a fog network. There should be a balance between anonymity for privacy and data access auditing.
- Exploiting credentials that vehicles use for accessing fogs to create fake sessions or gaining access to the resources in fog are the other open challenges in this area [33].

V. CONCLUSIONS

In this paper, we carried out a qualitative security and privacy analysis by studying the most important proposed solutions and suggestions for fog-based vehicular systems. First, we identified potential vulnerabilities in fog-based vehicular systems, including resources and services to address the challenges caused by these vulnerabilities. Then, we focused on security and privacy solutions and suggestions to defend the system. After a careful analysis of the most potential vulnerabilities and proposed security and privacy solutions and suggestions, several open challenges and future research orientations are identified.

ACKNOWLEDGMENT

This research has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 764785.

REFERENCES

[1] B. Gross, "Google's self driving car gathers nearly 1 gb/sec." [Online]. Available: https://www.linkedin.com/pulse/20130502024505-9947747-google-s-self-driving-car-gathers-nearly-1-gb-per-second/

[2] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and Privacy in Fog Computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.

[3] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[4] X. Chen and L. Wang, "Exploring fog computing-based adaptive vehicular data scheduling policies through a compositional formal methodpepa," *IEEE Communications Letters*, vol. 21, no. 4, pp. 745–748, April 2017.

[5] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," *Computer Networks*, vol. 130, pp. 94 – 120, 2018.

[6] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet of everything*. Springer, 2018, pp. 103–130.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," *Proceedings of the first edition of the MCC workshop on Mobile cloud computing - MCC '12*, no. March, p. 13, 2012.

[8] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 6, pp. 146–152, 2017.

[9] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing , Fog et al .: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, 2016.

[10] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in VANET security: A survey," *2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015 - Proceedings*, 2016.

[11] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *2016 IEEE Green Computing and Communications, and IEEE Cyber, Physical and Social Computing, iThings/GreenCom/CPSCom*, Dec 2016, pp. 164–170.

[12] F. Qu, Z. Wu, F. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[13] M. Azees, L. Jegatha Deborah, and P. Vijayakumar, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[14] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. ACM, 2013, pp. 61–64.

[15] R. H. Bailey, "Method and system for detecting and preventing an intrusion in multiple platform computing environments," Aug. 15 2006, US Patent 7,093,291.

[16] C. Huang, R. Lu, and K. R. Choo, "Vehicular fog computing: Architecture, use case, and security and forensic challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, Nov 2017.

[17] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, June 2017.

[18] D. H. H. Ashish Rauniyar and M. Shrestha, "A Crowd-Based Intelligence Approach for Measurable Security, Privacy, and Dependability in Internet of Automated Vehicles with Vehicular Fog," *Mobile Information Systems*, 2018.

[19] A. S. Sohal, R. Sandhu, S. K. Sood, and V. Chang, "A Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-Things Environments," *Computers & Security*, 2017.

[20] H. Al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, and H. Heidari, "Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 4822–4831, 2018.

[21] A. Kontorovich, "Advanced analytics for connected cars cyber security," *arXiv preprint arXiv:1711.01939*, 2017.

[22] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Generation Computer Systems*, vol. 78, pp. 817–824, 2018.

[23] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, "Sdn vanets in 5g: An architecture for resilient security services," in *2017 Fourth International Conference on Software Defined Systems (SDS)*, May 2017, pp. 67–74.

[24] M. Arif, G. Wang, V. E. Balas, and C. Science, "Secure VANETs : Trusted Communication Scheme between Vehicles and Infrastructure Based on Fog Computing," vol. 27, no. June, pp. 235–246, 2018.

[25] J. Noll, I. Garitano, S. Fayyad, H. Abie *et al.*, "Measurable security, privacy and dependability in smart grids," *Journal of Cyber Security and Mobility*, vol. 3, no. 4, pp. 371–398, 2014.

[26] S. Chaba and M. Dave, "Secure and Efficient Key Delivery in VANET using Cloud and Fog Computing," pp. 27–31, 2017.

[27] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 7–13, May 2018.

[28] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: a location difference-based proximity detection protocol for fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1117–1124, 2017.

[29] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 1, pp. 1–30, 2006.

[30] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, and X. Luo, "A survey on access control in fog computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 144–149, Feb 2018.

[31] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, p. 19, Aug 2017.

[32] T. Wood, E. Cecchet, K. K. Ramakrishnan, P. J. Shenoy, J. E. van der Merwe, and A. Venkataramani, "Disaster recovery as a cloud service: Economic benefits & deployment challenges." *HotCloud*, vol. 10, pp. 8–15, 2010.

[33] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to The Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. PP, no. c, pp. 1–1, 2018.

[34] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93–101, 2012.

[35] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*. IEEE, 2014, pp. 464–470.