Enforcing GDPR regulation to vehicular 5G communications using edge virtual counterparts

Jordi Ortiz*, Pedro J. Fernández*, Ramon Sanchez-Iborra*, Jorge Bernal Bernabe*, Jose Santa† and Antonio Skarmeta*

*University of Murcia
Murcia, Spain
{jordi.ortiz,pedroj,ramonsanchez,jorgebernal,skarmeta}@um.es
†Technical University of Cartagena
Cartagena, Spain
jose.santa@upct.es

***Abstract*—More and more people are concerned about data privacy and this is applicable to vehicular scenarios in which on-board units (OBU) and user devices are exposed to traceability across different access networks and service domains. General Data Protection Regulation (GDPR) in European countries indicates the way to proceed to guarantee privacy and access to sensitive data, however, applying these laws is not straightforward and may vary from country to country. Last advances in 5G communications, such as virtualisation and Multi-Access Edge Computing (MEC) can enable the proper management of data considering local GDPR regulations by using edge services. In this paper we propose the treatment of personal data in virtual OBUs (vOBU) instantiated at the edge of the network on the move. This way, vehicles and occupants benefit from GDPR guarantees compliant with current country regulations as they move across European borders.**

***Index Terms*—5G, cyber-security, CCAM, vehicular, EDGE, MEC, GDPR, privacy**

I. Introduction

Security and privacy are becoming paramount now that we are continuously connected to the Internet using a variety of mobile devices [1], [6], [14]. Traceability, identity exposure and ethical management of personal data are essential in the connected world. Because of this, the European Union defined the General Data Protection Regulation (GDPR) [3], as a framework to unify data security and privacy assurance guarantees to be implemented by EU countries. This way, local regulations had to be updated to be compliant with such directive.

Although GDPR presented new user guarantees regarding their privacy against cyber-crime, new technological challenges appeared in a globalized world. When considering macro-mobility of devices, such as the case of vehicles in cross-border scenarios, the issue is how to assure security and privacy across different countries with different applications of the GDPR using different technologies and configurations. While mobile network operators can implement solutions at European or even world-wide level, since they manage both the core and access network, a wide usage of open technologies in the 5G era imply extra difficulties regarding involved parties and their responsibilities.

Cooperative, connected and automated mobility (CCAM) is a clear example of the previous problem, since it involves vehicles equipped with connected on-board units (OBU) offering critical services in the areas of road safety and autonomous operation. Cross-border situations can imply the change of security and privacy countermeasures and the potential exposure of users to safety risks. Hence, it is necessary to provide solutions to cope with such challenge in an effective way [8]. Diverse proposals have emerged to cope with these challenges. For instance, in [5], authors propose a Secure and Privacy-Preserving Scheme based on ECC authentication mechanism, to ensure end-to-end security in 5G enabled vehicular networks. However, they do not address the GDPR regulation aspects in their research.

In this paper we present in detail the GDPR implications on CCAM when using 5G technologies, and propose a solution based on edge computing to delegate the treatment of data to the network to be compliant with country-specific security and privacy. This way, a set of transparent cross-border GDPR services are offered. For this, it is exploited the concept of virtual OBUs (vOBU) [11], as a virtualized counterpart of the OBU to be executed in virtual network domains that can follow the movement of the vehicle across Europe [12]. vOBUs include filtering, obfuscation and encryption services, among others, compliant with local regulations. Our approach relies on the vOBU concept to apply visited country GDPR laws to the OBU data while roaming operators by attaching the vOBU with the visited operator EDGE and therefore transparently capturing the traffic directed to the former vOBU to the migrated vOBU.

The paper is organized as follows. Section II presents the GDPR issues in 5G and CCAM. Then, Section III summarizes the GDPR law and the produced impact in 5G communications. Section IV describes the potential of virtualization and edge computing for CCAM scenarios, which is followed by Section V, exploiting the concept of vOBU for cross-border

GDPR assurance. Finally, Section VI concludes the paper with a summary of main findings and future research lines.

II. 5G security threads and CCAM

The first assumption that is made about 5G security is that it must include all security mechanisms already provided in pre-5G networks, and improve them if necessary, to cope with the new services and user needs. Standardization bodies have defined novel concepts in the 5G ecosystem, such as Network Function Virtualisation (NFV), Cloud Computing, Software-Defined Networking (SDN), Multi-access Edge Computing (MEC) and Network Slicing, in order to reach a full softwarized mobile network. In addition, new communication scenarios have been incorporated to the standard with different and specific requirements of QoS. Apart from the usual service of providing voice and data connectivity to mobile customers (Enhanced Mobile Broadband), massive machine-type communications (mMTC/IoT) and Ultra-reliable and low latency communications (URLLC) are now considered. The last one is the most suitable to enable Cooperative Connected Automated Mobility (CCAM) due to its specific low latency and reliability requirements. Keeping all these new services safe and secure is a great challenge and may introduce new threats that should be addressed.

Since the adoption of IP protocol in the core network in 4G, mobile networks have inherited security threads and risks of IP networks and the Internet world. 5G has indeed a more difficult challenge with the addition of millions of IoT devices to be connected, which are the perfect target of DoS and botnets attacks, among others. In addition to this, 5G has to focus on the huge fleet of vehicles that circulates roads and highways and analyze the new threads and risks that this new kind of networked nodes may introduce, especially when there may be human lives in risk.

Due to the new security needs of 5G introduced by the new actors, the NGMN Alliance, an important organization focused on providing 5G guidelines and recommendations, described the most probable threats that could appear. Those ones related to privacy receive a special attention, indicating that personal data leaking will suppose severe fines due to breaking the GDPR law, and the different personal data regulations between EU members and third parties may produce problems due to the existence of non-matching security policies between them.

Data leaking is a crucial threat to be considered, as a common procedure in CCAM systems is the periodic exchanges of messages among vehicles and with the infrastructure. For example, messages such as Cooperative Awareness Messages (CAMs), in the European architecture, and Basic Safety Messages (BSMs), in the American one, are exchanged among vehicles including their speed, position, and other additional useful data. The main issue is that these messages could be sent unprotected through unencrypted wireless channels (e.g. 802.11p) due to the processing cost of asymmetric cryptography, and the management issues for maintaining a common symmetric key. Therefore, ensuring the privacy and security of these messages against malicious cyberattacks is a key factor for protecting users and to comply with the GDPR.

III. Preserving Privacy of Personal data

A. Impact of GDPR on 5G communications

The GDPR's article 5 defines 6 clauses corresponding to six principles regarding processing personal data. 1) Lawfulness, fairness and transparency in relation to the data subject. Transparency: informing the subject about the kind of data processing to be done. Fair: the data processing must correspond to what has been described. Lawful: Processing must meet the tests described in GDPR. 2) Purpose limitations: personal data can only be obtained for "specified, explicit and legitimate purposes". Data cannot be further processed in a manner that is incompatible with those purposes without further consent. 3) Data minimisation: data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". 4) Accuracy: data must be "accurate and, where necessary, kept up to date". 5) Storage limitations: personal data is "kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed", that is, data no longer required should be removed. 6) Integrity and confidentiality, ensuring appropriate security of the personal data.

GDPR has been in force since May 25, 2018. Due to the coincidence in time with the development of 5G standards by the 3GPP WGs, all data protection and privacy issues has been considered from the very beginning in the development of those 5G standards. However, it is undeniable that GDPR will have a strong impact on 5G. Vendors, operators and standardization bodies are facing the application of this restrictive law from the beginning. In general, data protection by design and by default should be increasingly adopted by standardization. Different working groups in 3GPP are currently working in close coordination with the security working group (SA WG3), designing identifiers and protocols, and specifying test cases for privacy assurance in 5G. The same is applicable for vendors that are implementing 5G standards and developing proprietary solutions. Vendors must have, besides data protection by design and default, privacy impact assessment built into their product development lifecycle and should advise operators about the privacy impact of new technologies. Additionally, the operators must analyze how the GDPR affects their business model and take proactive steps in achieving compliance, for example, by appointing a competent Data Protection Officer (DPO).

Companies can reduce the probability of a data breach and thus reduce the risk of fines in the future, if they choose to use encryption of personal data by default. The processing of personal data is naturally associated with a certain degree of risk. Especially nowadays, where cyber-attacks are nearly unavoidable for companies above a given size. Therefore, risk management plays an ever-larger role in IT security and data encryption among other means for these companies. The GDPR recognizes these risks when processing personal

data and places the responsibility on the controller and the processor in Art. 32 to implement appropriate technical and organizational measures to secure personal data. This article does not define which specific technical and organizational measures are considered suitable in each case deliberately, in order to accommodate individual factors. However, it gives the controller a catalogue of criteria to be considered when choosing methods to secure personal data. Those are the state of the art, implementation costs and the nature, scope, context and purposes of the processing. In addition to these criteria, actors must always consider the severity of the risks to the rights and freedoms of the data subject and how likely those risks could manifest. This basically boils down to the following: The higher the risks involved in the data processing and the more likely these are to manifest, the stronger the taken security measures must be and the more measures must be taken. Encryption as a concept is explicitly mentioned as one possible technical and organizational measure to secure data in the list of Art. 32 of the GDPR, which is not exhaustive. Again, the GDPR does not mention explicit encryption methods to accommodate for the fast-paced technological progress. When choosing a method, actors must also apply the criteria catalogue above. To answer the question of what is currently considered "state of the art", DPOs usually rely on the definitions set out in information security standards like ISO/IEC 27001 or other national IT-security guidelines, provided by national NIS authorities and/or CSIRTs (Computer Security Incident Response Team).

B. Personal data protection in CCAM

The exploitation of the potential security vulnerabilities inherent to the various sub-systems comprising modern telecommunication networks could lead to massive disruptions. These issues must be properly and proactively addressed, especially in CCAM environments where human lives are at stake. Cross-border operation complicates things even further as it entails handovers between network operators that belong to different countries, raising several security and privacy concerns.

Regarding personal data preserving, application of different Data Privacy Protection laws depending on the country is a fact: GDPR requires the protection of CAM and Decentralized Environmental Messages (DENM), as they are also considered personal data due to sensitive information included like the vehicle identification number, which could be used by unauthorized parties. For example, an attacker may construct a profile of a given vehicle by observing where and when certain services are used. This issue becomes increasingly complex to handle in the external EU border where GDPR is not enforceable. Solutions like identity pseudonymization could significantly strengthen the user protection against traceability.

IV. EDGE COMPUTING IN 5G VEHICULAR NETWORKS

Adopting the MEC paradigm in CCAM scenarios is crucial to cope with the strict security and QoS requirements of vehicular services; the latter in terms of low latency, high bandwidth, and network reliability, among others. Besides, the deployment of a rich mesh of MEC nodes will permit the development of contextual services depending of fresh local information. Example of these enabled services are computation or storage offloading from end-devices, optimized content delivery and caching, Radio Access Network (RAN) management, or security management [13]. These functionalities will pave the way for the development of novel vehicular applications that will improve both driving safety and experience.

Regarding MEC, nodes will be able to provide quick response to threads detected in the road by broadcasting telematic warnings or triggering visual and acoustic alerts. This is of paramount importance when facing autonomous driving. Potential threats to be monitored are stop signals or red light violations, dangerous crossings, or risky overtakings, among many others. On the other hand, advanced driving applications such as dynamic route calculation, real-time contextual information, vehicle monitoring, or infotainment services will enhance the experience of drivers and passengers. All these applications will be enabled in the form of virtualized services that will be dynamically instantiated or migrated along this network of distributed processing units that will be placed close to the users. In this line, in a previous work [11], the concept of virtual OBU (vOBU) was exploited, to serve as a digitalized counterpart of real deployed OBUs. This strategy was followed to offload computation tasks, serves as a communication proxy to report captured data, and cache information to resolve requests from external services. This approach was further improved in [12], aiming at implementing a MANO and SDN-powered solution for migrating vOBU state from one MEC domain to another.

Moving the responsibility of applying security measurements for privacy preserving from the vehicle real OBUs to these virtual ones hosted in the closest MEC, will discharge drivers and vehicle manufacturers of being aware of all different privacy protection laws in every country. All this complexity will be distributed and shared by local mobile network operators that can easily know how to apply their local privacy preserving laws present in their respective countries.

As can be seen, all the applications mentioned above demand an extensive exchange of data between the real OBUs and their representative ones in the MEC that, in many cases, may contain user's sensitive information. For that reason, it is also necessary to develop additional security and privacy mechanisms to protect these operations at the network edge, as it is further explained next.

V. VIRTUAL OBUS AS PRIVACY PRESERVING ENFORCEMENT POINTS

A. vOBU-powered distributed privacy protection

OBUs are mobile devices that can be constrained more in terms of processing power than really in battery capacity, and therefore offloading some of their tasks to network nodes has been researched for long time. An advanced offloading technique is that of defining a virtual counterpart [11] that completely integrates with the OBU, being an extension of

the former. From the network point of view, this vOBU can be seen as the OBU itself, since every communication to the OBU is proxied through the vOBU and the other way around. The main difference with a simple proxy is the capability of the vOBU to process data and to decide whether communications should be End-to-End by simply relaying packets, or applying some more advanced aggregation, filtering or content caching schemes.

The capability of processing data sent by OBUs to the uplink, allows the application of AI/ML techniques to provide with an added value and to further reduce data sent to the cloud intelligently. One of the possibilities that such a processing offers is improving data privacy in OBU transmissions and, in particular, enforcing local laws applicable, such as GDPR. A vOBU may analyze every single piece of data and ensure that there is no data leakage.

However, OBUs are mobile devices and, as such, they can traverse country borders with different regulations to be enforced. In order to ensure this, the 5G network and its virtualized architecture may play a key role in the near future. First, communications leaving the OBU need to be redirected to a local and dynamically deployed virtual network function (VNF) on the operator's EDGE. Second, it is necessary to assure that the also called vOBU is GPDR-compliant for the visited country. Finally, providing with liability when GPDR is broken.

Figure 1 shows the proposed high-level architectural view where vOBU are migrated [12] across different edges, and the three proposed privacy-preserving mechanisms to enforce GDPR are integrated. The following subsection describes these three mechanisms.

B. Security and Privacy mechanisms to enforce GDPR in 5G vehicular networks

Enforcing communications of the OBU with its local virtual counterpart has been already presented in [12], as a seamless way to migrate the vOBU to another operator infrastructure. In this case, the enforcement is not envisioned as a experience enhancer but really as a security characteristic meaning that the objective is not to reduce the number of packets lost or reduce the time for the migration but rather make sure that the vOBU from the previous operator is not used anymore. In this case spin up time of the new VNF is critical and pools may be preallocated to avoid service delay or failure.

In order to make sure that the vOBU is compliant with the visited country legislation, the visited operator may just force an audited copy, and probably proprietary, of the vOBU module, reducing the freedom to choose and restricting the evolution of these technologies by third parties. Another option, more plausible is offering a certification mechanism for virtual counterparts to integrate those new versions on the operator VNF catalog.

It is clear that there is a need to provide with trust mechanisms that protect the operator and also protect the OBU. Using Trusted Execution Environment (TEE) [7] techniques

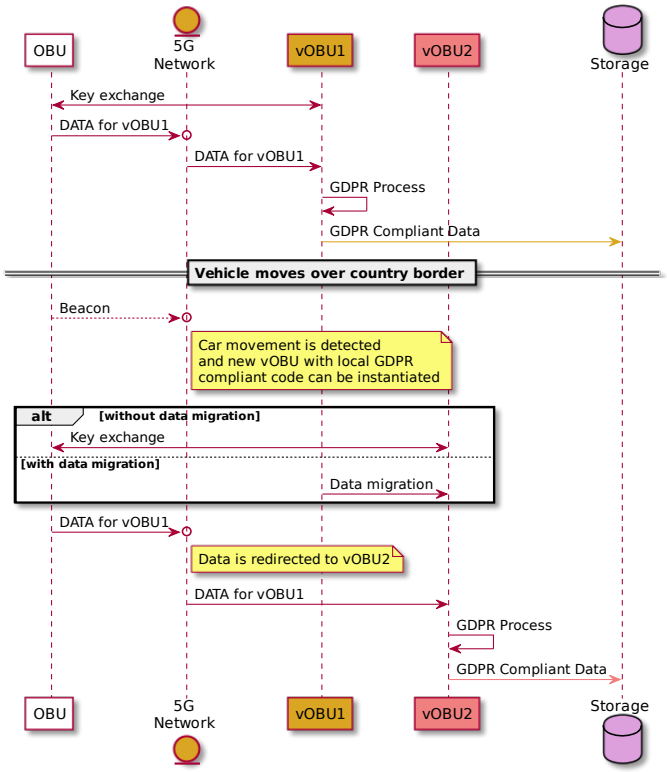

Fig. 2. Sequence diagram showing the key steps for GDPR enforcement while roaming operators

to protect OBU information from inspection while ensuring the law is not broken is foreseen as a desired functionality.

Enforcing laws is needed because if someone tries to break them, discovering the transgressors to maintain justice is a must. Smart Contracts and DLT [2] can be used in this context to determine those liable of breaking the law. It might be an infected OBU or a conscious attacker on the wireless link, it might be an infected vOBU or any other option not yet foreseen. Here the state of the chain from the OBU to the cloud can be stamped in an immutable DLT chain to further forensics.

Opening the possibility of adopting external vOBU implementations dynamically by the operator may relay on smart contracts that may delegate responsibilities to third parties such as Over-the-Top (OTT) companies offering advanced services to the car industry.

Figure 2 show the basic idea of the proposal as a sequence diagram. First the OBU needs to exchange cryptographic material with vOBU1. vOBU1 is the one in the country where the OBU is firstly switched on. Once the relation is established, data from the OBU can start flowing towards the Storage element, which may in turn be also any data processing element around the world. So the traffic is either directed from the OBU or redirected by the 5G Network, ensuring that the traffic does not avoid scrutiny. Each message that passes by the vOBU1 can therefore be analyzed to comply with GDPR. Once the car moves to another country and a

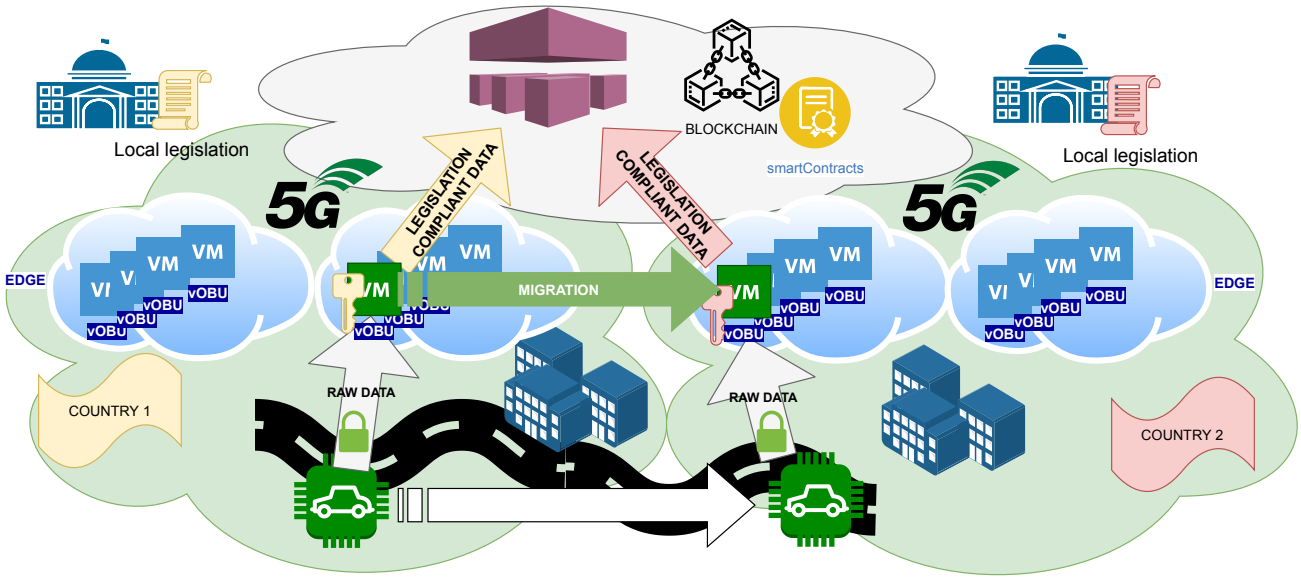

Fig. 1. GDPR compliant car roaming over 5G concept

roaming to another operator comes into play, there are two possibilities. If there is no data migration, it is not necessary to redistribute keys from vOBU1 to vOBU2, and a new key exchange mechanism may be needed (it must be noted that a keying mechanism based on eSIM might be plausible). The optimal option is that state transfer where data migration is done between vOBU1 and vOBU2, therefore both software entities need to understand the same data or at least offer a migration mechanism that can be triggered by the network. The diagram represents the OBU trying to still contact vOBU1 and the network redirecting the connection to vOBU2 in order to make sure that the GDPR of the visited country is enforced and therefore data sent to the cloud is compliant with GDPR.

C. Protecting OBUs and vOBUs

Even if 5G communications are encrypted to avoid attackers on the wireless medium to obtain data from other users, communications between the OBU and the vOBU shall be always encrypted. Several solutions have been already proposed using well known security protocols for key establishment such as IKEv2 [4], but also recent and novel security protocols used in the field of IoT such as EdHoc [10], to provide with channel protection or key exchange mechanisms that offer anonymity to the user in front of the operator. Besides, SDN-based approaches can be used to enforce dynamically security associations (SA) as IPSEC tunnels in the 5G networks, exchanging pertinent key-material among the peers [9] in a centralized way.

VI. Conclusions

Concerning about privacy protection is more and more present in 5G networks, following the security by default philosophy introduced in the design process of recent network architectures. Protecting personal information in vehicular networks adds more complexity to the problem, due to vehicles constant movement and the possibilities to switch operators and countries applying different personal data protection laws. The impact of applying GDPR law has been studied in this case. This work has proposed a novel way to reduce this complexity by delegating the responsibility of properly filtering and/or obfuscating personal data to the network, concretely to the Edge, near the user terminal, using the novelty concept of vOBU. This virtual representative discharges the vehicle real OBU of knowing and applying these different data protection laws. It is also stated that for an effective protection of personal data between the vehicle and the MEC node (vOBU), additional security measures have to be applied to protect data confidentiality and integrity and avoid relaying only on 5G generic protection at link layer. Some proposals have been formulated that can be developed in future works such as evolving cryptographic material distribution by means of SDN networks or relying on DLT and TEE technologies to accomplish the liability needed to make 5G networks trustworthy.

Acknowledgment

This work was supported in part by the European Commission, under the grants No. 871808 (5G PPP project INSPIRE-5Gplus) and No. 825496 (5G-MOBIX project), and in part by the Spanish Ministry of Science, Innovation and Universities, under the grants Ref. TIN2017-86885-R (PERSEIDES project), Ref. RED2018-102585-T (Go2Edge project) and Ref. RYC-2017-23823 (Ramon y Cajal Program). It has been also

partially funded by AXA Postdoctoral Scholarship awarded by the AXA Research Fund (Cyber-SecIoT project).

REFERENCES

[1] Jorge Bernal Bernabe and Antonio Skarmeta. Introducing the Challenges in Cybersecurity and Privacy - The European Research Landscape. In Jorge Bernal Bernabe and Antonio Skarmeta, editors, *Challenges in Cybersecurity and Privacy - the European Research Landscape*, RIVER PUBLISHERS SERIES IN SECURITY AND DIGITAL FORENSICS, pages 1–21. River Publishers, 7 2019.

[2] P. Dunphy and F. A. P. Petitcolas. A first look at identity management schemes on the blockchain. *IEEE Security Privacy*, 16(4):20–29, 2018.

[3] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union*, L 119(1):1–88, 2016.

[4] P. J. Fernández, J. Santa, F. Bernal, and A. F. Skarmeta. Securing vehicular ipv6 communications. *IEEE Transactions on Dependable and Secure Computing*, 13(1):46–58, 2016.

[5] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody. Sdn-based secure and privacy-preserving scheme for vehicular networks: A 5g perspective. *IEEE Transactions on Vehicular Technology*, 68(9):8421–8434, 2019.

[6] C. Lai, R. Lu, D. Zheng, and X. S. Shen. Security and privacy challenges in 5g-enabled vehicular networks. *IEEE Network*, 34(2):37–45, 2020.

[7] Titouan Lazard, Johannes Götzfried, Tilo Müller, Gianni Santinelli, and Vincent Lefebvre. TEEshift: Protecting code confidentiality by selectively shifting functions into TEEs. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 14–19. Association for Computing Machinery, oct 2018.

[8] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila. 5g privacy: Scenarios and solutions. In *2018 IEEE 5G World Forum (5GWF)*, pages 197–203, 2018.

[9] Gabriel Lopez-Millan, Rafael Marin-Lopez, and Fernando Pereniguez-Garcia. Towards a standard sdn-based ipsec management framework. *Computer Standards & Interfaces*, 66:103357, 2019.

[10] S. Pérez, J. L. Hernández-Ramos, S. Raza, and A. Skarmeta. Application layer key establishment for end-to-end security in iot. *IEEE Internet of Things Journal*, 7(3):2117–2128, 2020.

[11] José Santa, Pedro J. Fernández, Jordi Ortiz, Ramon Sanchez-Iborra, and Antonio F. Skarmeta. SURROGATES: Virtual OBUs to foster 5G vehicular services. *Electronics*, 8(2):117, 2019.

[12] Jose Santa, Antonio F. Skarmeta, Jordi Ortiz, Pedro J. Fernandez, Miguel Luis, Christian Gomes, Jorge Oliveira, Diogo Gomes, Ramon Sanchez-Iborra, and Susana Sargento. MIGRATE: Mobile Device Virtualisation Through State Transfer. *IEEE Access*, 8:25848–25862, 2020.

[13] Tarik Taleb, Konstantinos Samdanis, Badr Mada, Hannu Flinck, Sunny Dutta, and Dario Sabella. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Communications Surveys & Tutorials*, 19(3):1657–1681, 2017.

[14] Sébastien Ziegler, Cédric Crettaz, Eunah Kim, Antonio Skarmeta, Jorge Bernal Bernabe, Ruben Trapero, and Stefano Bianchi. *Privacy and Security Threats on the Internet of Things*, pages 9–43. Springer International Publishing, Cham, 2019.