IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Verticals in 5G MEC - use cases and security challenges

TOMASZ W. NOWAK[1], MARIUSZ SEPCZUK[1], ZBIGNIEW KOTULSKI[1], WOJCIECH NIEWOLSKI[1,2], RAFAL ARTYCH[2], KRZYSZTOF BOCIANIAK[2], TOMASZ OSKO[2], and JEAN-PHILIPPE WARY[3].

[1]Faculty of Electronics and Information Technology of the Warsaw University of Technology, Warsaw, Poland
[2]Orange Polska S.A., Warsaw, Poland
[3]Orange Labs, Paris, France

Corresponding author: Tomasz W. Nowak (e-mail: t.nowak@tele.pw.edu.pl).

This paper is partially financed by EU Inspire-5Gplus project https://www.inspire-5gplus.eu/ (Grant Agreement No.:871808, Research and Innovation action, Call Topic: ICT-20-2019-2020: 5G Long Term Evolution).

ABSTRACT 5G is the fifth-generation cellular network satisfying the requirements IMT-2020 (International Mobile Telecommunications-2020) of the International Telecommunication Union. Mobile network operators started using it worldwide in 2019. Generally, 5G achieves exceptionally high values of performance parameters of access and transmission. The application of edge servers facilitated the implementation of such requirements of 5G, which resulted in 5G MEC (Multi-access Edge Computing) technology. Moreover, to optimize services for specific business applications, the concept of 5G vertical industries has been proposed. In this paper, we study how the application of the MEC technology affects the functioning of 5G MEC-based services. We consider twelve representative vertical industries of 5G MEC by presenting their essential characteristics, threats, vulnerabilities, and known attacks. Next, we analyze their functional properties, give efficiency patterns and identify the effect of applying the MEC technology in 5G on the resultant network's quality parameters to identify the expected security requirements. Finally, we identify the impact of classified threats on the 5G empowered vertical industries and identify the most sensitive cases to focus on their protection against network attacks in the first place.

INDEX TERMS 5G mobile communication, communication system security, MEC, mobile computing, network servers, next generation networking, performance parameters, software protection, telecommunication computing, telecommunication services, vertical industries

I. INTRODUCTION

CONTEMPORARY networks offered by Mobile Network Operators (MNOs), based on 5G wireless communications technologies and supported by MEC network architecture, requires coordinating and adapting new security capabilities for themselves and Mobile Virtual Network Operators (MVNOs). Such operators provide services for different vertical industries (a concept first proposed for 5G networks in the 5G PPP white paper [1]) with their new business models, network requirements, and modes of operation [2]–[4]. Contemporary mobile standards need interfaces well-defined to the service layer [5]. Moreover, the 5G verticals [6] coexisting in such a new network ecosystem require specific security services, individually configured security functions implemented on different network planes and layers, and flexible deployment procedures; see, e.g., [7]. To provide adequate network functionalities for a vertical, one can use the standardized types of 5G networks, e.g., suitable for real-time and other Fixed Wireless Access (FWA) services, the enhanced Mobile Broadband (eMBB), which needs to support large payloads and high bandwidth and which can use to the greatest extent the protection offer of edge devices [8], Ultra- Reliable and Low-Latency Communication (URLLC), which supports use cases with very low latency for services that require short response times, or massive Machine Type Communication (mMTC) for Machine-to-Machine (M2M), which should support many devices in a base station, see [9], [10]. The expected values of the 5G network quality parameters of these types of networks, drawing on the scale of all expected maximal values of the quality parameters of IMT-2020 for 5th generation networks, are presented according to ITU-R M.2083 [11], see Fig. 1.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

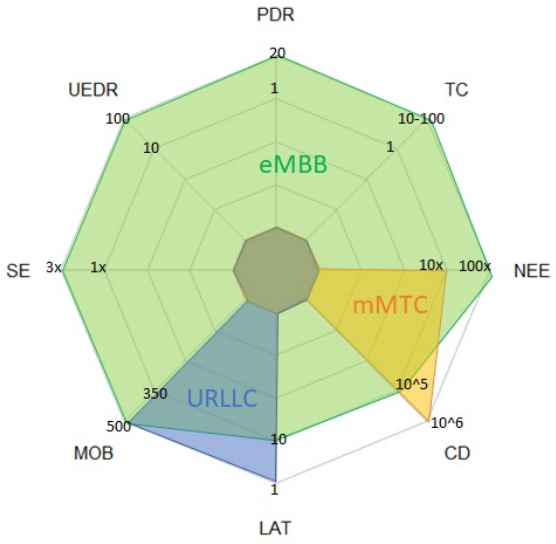

FIGURE 1. Standardized types of 5G networks IMT-2020 (5th generation) according to ITU-R M.2083 [11].

To effectively create such (and other) types of networks satisfying the needs of vertical industries [12], three 5G fundamental pillars are used: Software Defined Networking (SDN), Network Function Virtualization (NFV), and MEC, see [13]. The SDN technology has been created to shift the network management from hardware-oriented to software-based solutions and separate the control and data traffic into two planes, see [14]. It has been applied in new mobile networks, including system architecture, resource management, mobility management, and interference management, see [15]. The paradigm of NFV has been the milestone in decoupling network functions from the physical devices on which they run to a virtualized environment, see [16]. Application of Virtual Network Function-based (VNF-based) entities (called Reusable Functional Blocks) can provide a high level of flexibility and scalability in 5G, deployment of new services with increased agility and faster time-to-value and significant reductions in operating and capital expenses [17]. Moreover, NFV and its relationship with complementary fields of SDN are very useful for building 5G network slices, see [18], and provide integrated complete 5G network security solutions [19], [20]. MEC, the third essential pillar of 5G, is particularly important in the context of meeting the diverse requirements of 5G vertical industries, see Fig. 2. MEC intends to shift an IT service environment and cloud-computing capabilities to the edge of the mobile network, near mobile subscribers, to reduce latency and improve network operation and service delivery. It supplements the NFV-based network functions with applications running at the edge of the network. MEC is based on a virtualized platform, hosted by the infrastructure placed at the edge of the mobile network, within the Radio Access Network (RAN). It opens services to end users and enterprise customers and associated industries (5G vertical industries) that can now deliver their mission-critical applications over the mobile network and improve their operation using this technology, see [21]. Initially, the MEC framework developed by ETSI, was treated as a complete Edge Computing solution, with strictly defined components and relations and rigorously specified communication at the interfaces. Recent concepts of MEC are opened to specifications of other research groups, see [22].

From the End User perspective, the MEC environment should work at least as a cloud or on-premise solution but with some additional benefits. From the vertical point of view, the system's users' behavior might be used for resource optimization. This concept was described in [23], originally for Mobile Social Networks, but it could be extended to other systems with communication between End Users. The service usage data might be exchanged between verticals and the MEC Operator to obtain better resource allocation and utilization predictions.

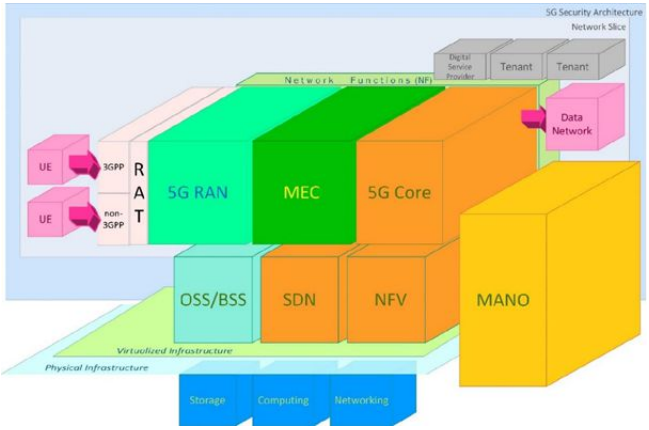

FIGURE 2. Schematic diagram of the 5G MEC network architecture, according to ENISA [152].

Generally, considering the new network solutions for the 5G verticals, one must unify known and future security concepts of 5G. They can be automated security and orchestration functionality for slices dedicated to multiple service providers and multiple tenants, as well as for the MEC architecture, leading to possible End-to-End security solutions, see, e.g., [24], [25]. In the literature, one can find many papers concerning different aspects of enabling 5G networks to vertical industries, see, e.g., [26], and verifying models and experimentally trialing 5G [27], and mobile edge [28] verticals' infrastructure. However, in the literature, there is no complete security analysis for 5G MEC verticals. On the other hand, several papers consider specific security models and approach helpful in this topic. For instance, the paper [29] investigates mobile network operators' security challenges and mitigation mechanisms for cloud layers as well cloud deployments. The chapter [30] provides an overview of different IoT-based verticals, associated security requirements, threats, and possible mitigations. The paper [31] analyzes the properties of MEC pertaining to the requirements of vehicle safety applications and presents the MEC-related security problems in Vehicle-to-Everything communication. In [32] a new approach to network threats utilizing three

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 1. Summary of Acronyms

Acronym	Definition	Acronym	Definition
2FA	Two-Factor Authentication	**IoMT**	Internet of Medical Things
2G	the second-generation cellular network	**IoT**	Internet of Things
3PL	third-party Logistics	**KaaS**	Knowledge-as-a-Service
4G	the 4th Generation of mobile technology	**LAN**	Local Area Network
4PL	fourth-party Logistics	**LAT**	Latency
5G	the fifth generation mobile network	**LPWA**	Low-Power Wide-Area
5G PPP	5G Public-Private Partnership	**LTE-M**	Long Term Evolution (4G), category M1
5G-IA	the 5G Infrastructure Association	**LoRa**	Long Range
5G MEC	5G MEC Multi-access Edge Computing	**mMTC**	massive Machine Type Communication
6loWPAN	IPv6 over Low-Power Wireless Personal Area Networks	**M2B**	Mobile-to-Bank
A2A	Authority-to-Authority	**M2I**	Mobile-to-Insurance
A2B	Authority-to-Business	**M2M**	Machine-to-Machine
A2C	Authority-to-Customer	**MaaS**	Mobility-as-a-Service
AAA	Authentication, Authorization, and Accounting	**MEC**	Multi-access Edge Computing
AALHP	Ambient Assisted Living Health Platform	**MFA**	Multi-Factor Authentication
ACL	Access Control List	**MIPS**	Million Instructions Per Second
ACM	Agile Cloud Migration	**ML/AI-based**	Machine learning/ Artificial Intelligence-based
AI	Artificial Intelligence	**MNO**	Mobile Network Operators
AOSP	Android Open Source Project	**MVNE**	Mobile Virtual Network Enabler
API	Application Programming Interface	**MVNO**	Mobile Virtual Network Operators
APT28	Advanced Persistent Threat 28	**MaaS**	Mobility-as-a-Service
APT	Advanced Persistent Threat	**NB-IoT**	Narrow-band Internet of Things
AVA	Availability	**NFC**	Near Field Communication
B2B	Business-to-Business	**NFV**	Network Function Virtualization
B2C	Business-to-Client	**NIST**	National Institute of Standards and Technology
BAN	Body Area Network	**OAuth2**	Open Authorization 2
BFSI	Banking, Financial Services and Insurance	**OPC UA**	Open Platform Communications United Architecture
Bit4id	Best Information Technology for Identification	**OTT**	One-way Trip Time
CAM	Cooperative Awareness Messages	**OWASP**	Open Web Application Security Project
CAP	Capacity	**PCI DSS**	Payment Card Industry Data Security Standard
CCTV	Closed Circuit Television	**PDR**	Peak data rate
CDC	Centers for Disease Control and Prevention	**PHI**	Protected Health Information
CDNs	Content Delivery Networks	**PKI**	Public Key Infrastructure
CIA	Confidentiality, Integrity, Availability	**PO**	Property Owner
CIM	Cooperative Information Manager	**PWA**	Progressive Web App
CI	Confidentiality and Integrity	**QoE**	Quality of Experience
CPU	Central Processor Unit	**QoS**	Quality of Service
D2D	Device-to-Device	**RACI**	Responsibility Assignment Matrix
DAS7	DASH7 Alliance Protocol	**REL**	Reliability
DD	Device Density	**RFID**	Radio-Frequency Identification
DER	Distributed Energy Resources	**RPL**	Routing Protocol for Low-Power and Lossy Networks
DSS	Decision Support System	**RTT**	Round Trip Time
DoS	Denial of Service	**SDN**	Software Defined Networking
eMBB	enhanced Mobile Broadband	**SES**	Smart e-commerce Systems
eMTC	enhanced Machine Type Communication	**SSLA**	Security Service Level Agreement
eNodeB	Evolved Node B	**TCO**	Total Cost of Ownership
EC-GSM-IoT	Extended coverage GSM IoT	**TI**	Tactile Internet
ECG	Electrocardiogram	**TLS**	Transport Layer Security
ECU	Edge computing usage	**TTM**	Trust to MEC platform
ENISA	The European Union Agency for Cybersecurity	**TaaS**	Transport-as-a-Service
EVITA	ESafety Vehicle Intrusion Protected Applications	**UAS**	Unmanned Aerial System
FLOPS	Floating Point Operations Per Second	**UAVs**	Unmanned Aerial Vehicles
FWA	Fixed Wireless Access	**UE**	User Equipment
gNodeB	Generation Radio Technology Base Station	**URLLC**	Ultra-Reliable Low-Latency Communication
GSM	Global System for Mobile Communications	**US CISA**	United States Cybersecurity and Infrastructure Security Agency
HA	High Availability	**UX**	User Experience
HIPAA	Health Insurance Portability and Accountability Act	**V2I**	Vehicle-to-Infrastructure
IACS	Industrial Automation and Control Systems	**V2N**	Vehicle-to-Network
IB	InterBank	**V2P**	Vehicle-to-Pedestrian
IDS	Intrusion Detection System	**V2V**	Vehicle-to-Vehicle
IL	Isolation level	**V2X**	Vehicle-to-everything
IMT-2020	International Mobile Telecommunications-2020	**VNF**	Virtual Network Function
IPS	Intrusion Prevention System	**VR/AR**	Virtual Reality/Augmented Reality
IP	Internet Protocol	**VTF**	Vertical Engagement Task Force
ISO	International Organization for Standardization	**WAN**	Wide Area Network
ISP	Internet Service Provider	**WHO**	World Health Organization
ITU	International Telecommunication Union	**WWW**	World Wide Web
IT	Information Technology	**Wi-Fi**	Wireless Fidelity

pillars of 5G is proposed. It integrates multi-layer collective security intelligence to a converged SDN/NFV architecture in standard MEC technology. These and other papers available in the literature point out the directions of our investigations. However, to find satisfactory security solutions for 5G MEC verticals, we must analyze their functional specifications, principal vulnerabilities and attacks that threaten critical assets, and expected security requirements.

Over the past few years, 5G mobile networks have become a mature ICT project with many publications. There are also review articles devoted to the basics of 5G networks [33], its security [34], and key technologies supporting commu-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

nication such as SDN [35], NFV [36], [37], and MEC [38]–[40]. The concept of 5G vertical industries also has its review literature, see, e.g., [41]. One can also find papers considering vertical industries in 5G networks with MEC technology in the literature. A competent overview of such an area of development of 5G networks can be found in the paper [42].

The purpose of this paper is to present the application of MEC technology within 5G networks and its effect on the development of 5G vertical industries. After a brief overview of the verticals proposed by various authors and standardization organizations and selecting the set to be analyzed in this paper, we present several topics regarding their implementation and security in the 5G MEC system. The scope of the paper covers the following points:

- Systematic presentation of twelve 5G vertical industries according to three aspects (Section II):
  - -- Their characteristics, including a description of the most important use cases,
  - -- Known threats and vulnerabilities described in the literature,
  - -- Identified attacks and proposed countermeasures.
- Presentation of performance and security requirements for 5G MEC verticals and their use cases (Section III):
  - -- Selection of nine parameters required to characterize the performance and security of the 5G MEC network applied for verticals (Subsection III-A),
  - -- Estimation of values of these parameters for the verticals and their use cases, based on literature (Subsections III-B-III-M),
  - -- Indication of the possible impact of using MEC technology on the functionality of 5G verticals use cases on their functionality (Subsections III-B-III-M),
  - -- Collection of the identified advantages and drawbacks of using MEC technology for 5G verticals (Subsection III-N).
- Indicating the impact of known network threats on the 5G MEC performance and security parameters (Section IV).
- Indication, which 5G MEC network performance and security parameters are crucial for the proper functioning of the verticals (Section IV).
- Identification, which threats are most dangerous for the verticals using 5G networks with MEC technology (Section V).
- Giving an outline of challenges to provide security for verticals using 5G MEC networks (Section VI).

II. 5G VERTICALS

A. BACKGROUND

Enabling users to move to different geographic locations within a mobile network while continuously operating across the full range of service requirements is and will be a key challenge today. It means meeting the criteria of the required performance, reliability, flexibility, and scalability of traffic for a constantly growing number of end users [43]. In addition to such technological solutions as network slicing and edge computing, it requires the use of new mobility management solutions. 5G mobile network is very often appreciated for its ability to meet the requirements associated with verticals, depicting different areas of the economy with their specific communication nature. The vertical industries in the 5G network take advantage of the scale and guarantee high-quality performance, such as throughput, low latency, reliability, etc., that 5G offers. Therefore, the 5G Infrastructure Association (5G-IA), representing the private side in 5G-PPP, included verticals engagement as the main objective to optimally adapt the operation of the network to the specific needs of a given sector of human activity. Moreover, the 5G-PPP Vertical Engagement Task Force (VTF) has been established to coordinate and monitor activities related to working with vertical sectors. The sectors which are considered in frames of 5G-PPP VTF are (see [44]):

- Automotive,
- Manufacturing,
- Media,
- Energy,
- e-Health,
- Public safety,
- Smart cities.

Moreover, in a blog post on current cybersecurity issues [45], the author indicates vertical security as the most crucial problem to be solved and lists important vertical industries. Among them, except for some sectors mentioned above, there are additional ones:

- The Financial Sector, Banking, Financial Services and Insurance (BFSI),
- Retail,
- Telecommunications,
- Authorities.
- Automotive,
- Manufacturing,
- Media and Entertainment,
- Transport,
- Energy and Utilities,
- Healthcare,
- Agriculture,
- Public Sector/Municipal,
- Financial Services,
- Retail.

Thus, any list of verticals would not be complete, especially that new application fields of 5G networks arise and some verticals lose their importance in business. In this paper, we decided to consider twelve different vertical industries that are considered essential by both practitioners and international organizations, and that let us present different aspects of the functioning of 5G MEC verticals. Most of the vertical industries, which we will consider, belong to the developing future economy areas, see [49]. However, we include one more vertical:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

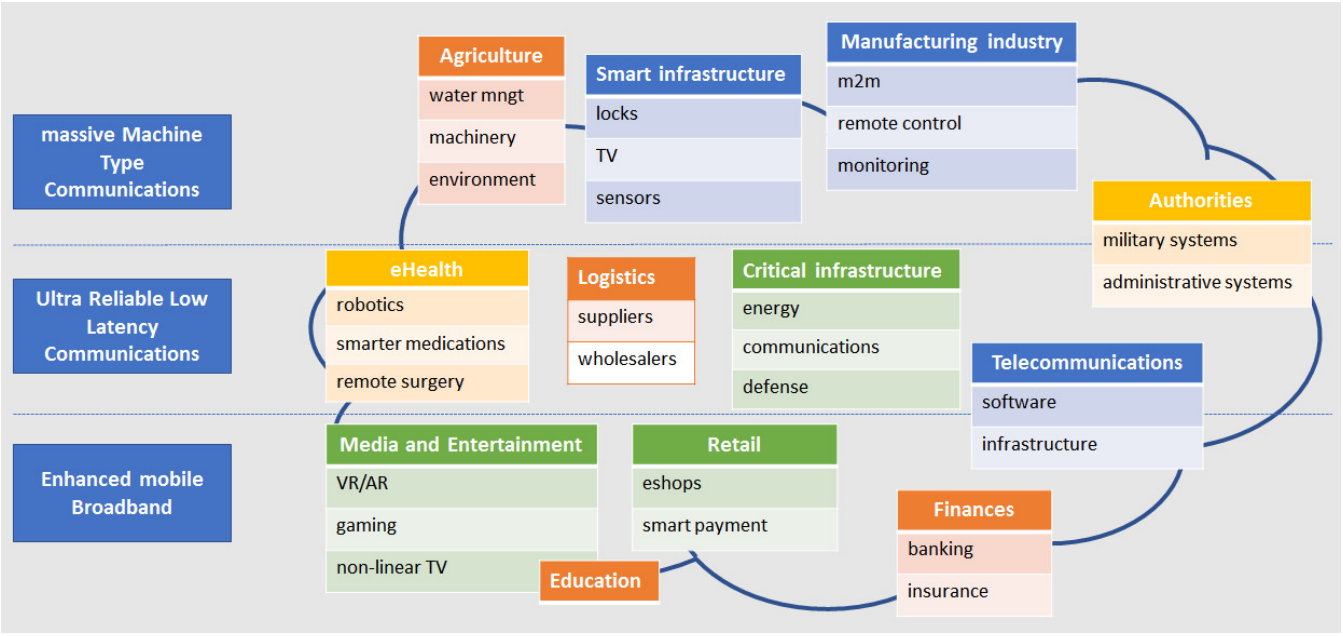

FIGURE 3. Vertical division in the 5G network.

- Critical Infrastructure [47],

which covers a large set of industrial sectors considered from a very narrow perspective of their safety and security. The verticals considered in our studies are consistent with the classification proposed and analyzed in the 5G PPP & 5G IA technical report [48]. They have different requirements that enable them to work properly. Fig. 3 shows the assignment of verticals to the application scenarios defined for 5G: enhanced Mobile Broadband, Ultra-Reliable Low Latency Communications, and massive Machine Type Communications. Naturally, verticals can be assigned to several applications, e.g., agriculture is associated with many sensors and low latency and reliability. In the following subsections, we will present these 5G verticals, depict their functional characteristics, present identified threats and vulnerabilities, and describe known attacks to critical assets and possible countermeasures.

B. MANUFACTURING INDUSTRY

1) Characteristics

The need to designate the manufacturing industry as a separate vertical sector of 5G network has been noticed quite early (see [50]). In this document, the authors identified five different use cases for the modern industry to be supported by 5G communication:

- *Time-critical processes optimization inside factory*: real-time feedback communication between machines for control, efficiency and flexibility purposes, augmented reality applications for training and maintenance, and real-time interaction between collaborative robots and humans.
- *Non time-critical communication in factory communication*: tracking assets inside the factory, non-real-time data sensing for processes control and optimization, and collecting data for design and forecasting new products and technologies.
- *Remotely controlling digital factories*: End-to-End communication between remote workers and the factory, including remote control of applications running on tablets and smartphones, new augmented-reality devices and new remote services, and creating virtual back office teams. It may also provide augmented-reality support in the production and assembly of products and maintenance and repairing machines without training due to augmented information and operational guidance.
- *Intra-/Inter-Enterprise Communication* for tracking goods in End-to-End value chain, reliable and secure interconnections of premises, and exchanging data for design purposes.
- *Connecting goods during product lifetime* to monitor product characteristics, sense its surrounding context, and offering new data-driven services.

The paper [51] proposes two special use cases that demonstrate how NFV enables flexible smart manufacturing. In NFV technology, Virtual Network Functions are used in network services. The first use case applies vertical-specific network services that enable augmented reality on-demand. In contrast, the second one is the flexible interconnection of production machines with services in the company's cloud back-end. In turn, the authors of the paper [52] consider four use case classes for the manufacturing industry:

- *Infrastructure retrofit,* including large-scale infrastruc-

ture improvement, wireless connectivity between sensors and actuators, the ability for critical communication, reliable network, and information multiplexing.
- *Mobile robots*, including applications with different automated driven vehicles, possibly equipped with artificial intelligence.
- *Inbound logistics* for manufacturing, flexible and modular assembly area, plug-and-produce.
- *Massive wireless sensor network and process monitoring* making possible application of many sensors using different sensing technologies (acoustic, X-ray, laser light, etc.) for detecting defects over a production space and with the engagement of different actors (human workers, artificial intelligence solutions, augmented reality-based solutions, etc.).

As it is seen, the present use cases pattern is stable concerning how 5G communication can be applied. Concerning network quality parameters and types of 5G network used in the manufacturing industry, the studies made in the literature [53], [54] show that each of the usual network quality parameters: peak data rate (Gb/s), mobility (km/s), capacity (Gb/s), number of connected devices per cell, user plane latency (ms), and energy savings must be satisfied at a high level. However, the critical parameter is the latency, so the 5G URLLC network type will be used in most industrial use cases. Generally, the manufacturing industry includes different industrial sectors of different scales, integrated with supply chains, research and development institutions, and the financial sector.

2) Threats and vulnerabilities

The manufacturing industry is not safe from hacker attacks. According to different studies, the production industry belongs to the sectors most vulnerable to security breaches. In this area, hackers focus mainly on data espionage as a very lucrative activity within the range of their possibilities. The main targets are networked machines, robots, and 3D printers. Vulnerabilities of production devices enable attackers to get production data. In addition, they can interfere with processes, sabotage production, and even destroy technological infrastructure. Not only can these vulnerabilities lead to potential financial damage, but they can also put the lives of factory workers at stake. Modern industry is integrated with the Internet by Web applications, used for customer rights management, products online monitoring, and updating or implementing supply chains. Such applications are gateways for different attacks, annually reported by OWASP, NIST, or MITRE [55]. The spectrum of most frequent threats involved in using web applications evolves in time, extending beyond a set of about 30 methods [56]. Since some use cases of Industry 4.0 include mobile applications, both at the manufacturer and the end user side, the mobile vulnerabilities should be considered [57]. These vulnerabilities open wide the gates for hackers by exposing direct access to manufacturers' assets and communication, affecting industrial automation and control systems and product maintenance and monitoring systems. Such vulnerabilities also enable hackers to inject malware into the manufacturing industry's protected environment, which makes it possible to do autonomous and long-term damage or disable computers and computer-based systems and functionalities.

3) Attacks and countermeasures

The manufacturers should continuously monitor their production lines for vulnerabilities and implement mechanisms that control access to all areas of the production system. They should also limit access or isolate an area which is already affected. Industry 4.0 [58] comprises the topic of permanent maintenance and monitoring of products, which also must be protected. The main areas of providing security within the manufacturing industry can be classified according to the fields of standardization considered by national and international organizations, see [59]. They could be presented in the following order:

Communication Security. It includes networks using security gateways, Virtual Private Networks, secure networks with IP convergence, and secure wireless/radio networks. On the external network's interface, adequate access control and access rights management system must be applied. Internally, the manufacturing systems need the application of secure industrial automation and control systems (IACS) [60], which have their own communication components. Usual communication security control measures should provide communication security in such distributed and heterogeneous systems [61], [62] and, additionally, enhanced by risk assessment methods and dedicated network design techniques (system secure by design).

Security during product development. Modern industry manages the products' lifecycle, which requires, except for providing secure communication, comprehensive security management. It starts from the design phase (a product secure by design), which includes detection of vulnerabilities in software and protection of products' code [63], and the testing phase, which covers the formulation of security requirements, threats and vulnerabilities mitigation, and penetration testing. Next, one should securely manage defects and updates and propose security guidelines for the products' lifecycle (including adequate documentation for end users).

Supplier Relationships Security. It starts from establishing requirements for security capabilities to be supported by security software integration and maintenance service providers. Next, one should identify IACS assets owners, negotiate between IACS asset owners and IACS maintenance service providers, define security profiles which are capability sets defined by selecting a specific subset of requirements for secure automated solutions. Finally, one must ensure security of cloud services, storage and communication technology supply chain, using best supply chain risk management practices, see [64].

Security Incident Management. In this area, the security procedures start from establishing incident management principles using the most up-to-date guidelines to plan and

prepare for incident response. The results are the security information and event management systems satisfying legal (country-dependent) and security management standards requirements. Moreover, business continuity and disaster recovery procedures should be prepared and exercised. Finally, digital forensic techniques must be ready to use if needed.

Asset Management. Assets security is one of the main objects to protect within a company. Therefore, the assets must be well-identified, validated, and managed [65]. Relations between key elements of the asset management system and other systems should be well-defined. The key procedure is IT and software asset management, including a system of software identification, license, patch, and version management.

Interoperability. The manufacturing communication system should provide a way for considering security, reliability in data transport, as well as compliance and portability. It must be used in different automation systems and by different suppliers, not always using the same communication protocol. Different communication service models must be supported: data transmission in client/server and peer-to-peer types of communication, fast and reliable system-wide distribution of data, based on a publish-subscribe model, etc. Following solutions are possible using OPC UA standards [66], exploiting SDN advances [67] for heterogeneous industrial networks, integrating 5G mobile networks with existing industrial communication standards [52] or creating 5G-based private networks [68].

C. THE FINANCIAL SECTOR

1) Characteristics

The Financial Sector, sometimes called Banking, Financial Services, and Insurance (BFSI) sector, is under increasing pressure from different sides. It is due to competitors with digital offerings and the constant pressure to modernize their existing systems. The pressure also arises from the changes in technology, where the role of 5G and MEC solutions is becoming more prominent. The value of customers' data is increasing as customers demand more comfortable and personalized services, both fixed and mobile. Trust remains a crucial value in BFSI sector, so it must be provided by secure technology, high-quality services, education, and reasonable PR. Trust is also essential because players of the black market and white market [69] coexist in BFSI security. The first group consists of individuals/groups of cyber-criminals who perform different malicious actions using technologies, including peer-to-peer network sites. The second one, the white BFSI market, unifies networked BFSI organizations, software and other security product vendors, cyber insurers mitigating risks of the other BFSI players, infrastructure and services providers (cloud, Internet services), governments protecting the critical infrastructure of a nation by organizing collaboration with the private sector as well as creating and enforcing legal regulations. The security of BFSI is also provided or enforced by IT governance and auditing agencies, information security providers, security reporting agencies, ethical hackers, and all IT security experts engaged in this vertical industry [69]. Moreover, in recent years banking industry is evolving from just a journal and ledger entry paradigm to data and analytics-driven banking operations, see [70]. They assume online and offline customer behavior when using BFSI services, each with own assets and security requirements. The paper [70] discusses various scenarios in BFSI areas, where Big Data analytics is essential for the service construction. In such systems, special benefits are due to the application of modern technologies: Internet of Things (IoT), Blockchain, Chatbots, and automated solutions using robotic systems.

2) Threats and vulnerabilities

The BFSI sector belongs to vertical industries where main assets and operations are in virtual space. Therefore, the model proposed in the paper [71] which presents a Unified Resource Descriptor, and the Knowledge-as-a-Service (KaaS) framework could be a basis for security analysis of this vertical. In such a framework, the key challenge is capturing relevant and authentic information for knowledge building and decision-making. Thus, the main threats are [71]: improper thought process, inappropriate development framework, lack of reliable infrastructure, lack of data collection and integration mechanisms, inadequate test plan, all at one go (planning to develop and onboarding applications), weak project management, inappropriate assignment of the level of information access authority, and mistakes in integrated collaboration channels among stakeholders.

The financial organizations, especially of the banking sector, extensively use web-based services and mobile applications [72], which expose them to all vulnerabilities and threats identified by OWASP, already presented in Subsection II-B2. The real identified banking systems vulnerabilities are usual programmers' mistakes, application of weak or insufficient cryptography, or inappropriate security management [73]. These publicly known security concerns make the BFSI consumers worry about such problems as personal data and identity theft and governmental collection of personal information, dumpster diving threat or mailbox theft, financial organization data breaches, and not trusted Internet security for bill payment [74].

3) Attacks and countermeasures

Most attacks observed in cyberspace are common for several vertical industries because they use similar communication and data storage technologies. The paper [75] presents an overview (from the historical perspective) of attacks perpetrated against Banking, Financial Services, and Insurance, Healthcare, and e-retail industries, as well as government agencies (some aspects of administration and critical infrastructure). The main categories of attacks are malicious software, DoS, financial fraud, system penetration, theft of proprietary information, and unauthorized access. All these attacks lead to excessively high risks and high financial losses. The high exposure to the threats presented above and

large-scale attacks against BFSI institutions observed in the past [75] show that this sector must adapt to these and other, sometimes still undefined risks. So, banks and other financial institutions must invest more in security solutions to ensure 24/7 protection. Distributed ledgers will significantly shape the future of the banking sector. The most popular technology, the blockchain, is the backbone of cryptocurrencies like Bitcoin [76]. The blockchain method provides a permanent record of transactions. It is thus part of the accounting control procedures that cannot be manipulated and have the potential to completely redesign the BFSI sector [77].

D. HEALTHCARE

1) Characteristics

The healthcare sector can be considered in two aspects: user/patient relation, including its social context and the area of health professionals, services, and health insurance providers. Especially Healthcare, including telehealth, is essential in the context of COVID-19 pandemic [78], [79]. Telehealth was initially reserved for patient care in hard-to-reach areas with limited in-person physician availability. However, with the COVID-19 outbreak and facilitating social distancing recommendations, hospitals began to cover routine office visits via telehealth. Due to these circumstances, most hospitals have also switched outpatient care to telehealth. Furthermore, in the context of the COVID pandemic, telehealth has been promoted by major public health organizations such as WHO and CDC as the standard of care in place of routine office visits. Due to that, we can list several scenarios where the new capabilities offered by the 5G network can improve e-Health category [80], [81]:

- assets and interventions management in hospitals,
- robotics,
- remote monitoring of health or wellness data,
- smarter medication.

The assets and interventions management in Hospitals refers to assets tracking and management and planning of operations and follow-up. Assets in hospitals are limited goods which are very often expensive, too. The hospital should be protected against the unauthorized displacement of its valuable items. The robotic category is associated with telesurgery scenarios. Very often, specialists are not available at some hospitals and they can join the surgery only remotely. In [82] the authors present consideration about robot-based telesurgery on the 5G Tactile Internet (TI) and artificial intelligence technology. The architecture, elements, characteristics, and benefits of telesurgery are explained considering two aspects, intelligent tactile feedback and human-machine interaction data. Similar considerations about Tactile-Internet-Based Telesurgery can be found in [83]. Moreover, the authors propose an architecture for telesurgery with two different types of communication channels: traditional network and 5G-enabled TI. The conclusion of the comparison is the fact that TI as a network backbone has a faster response time and higher reliability comparing to the existing system. Such telesurgery needs to be protected against privacy, data tampering, and availability. Paper [84] presents a blockchain solution, called HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0, where security can be achieved with immutability and interoperability by a special piece of code written in solidity or other blockchain specific languages to ensure the trust between all the parties connected via blockchain and eliminate unnecessary data sharing. Medical Video Communication is another aspect that should be considered in the context of telesurgery. Many papers in the literature refer to the quality of such communication, users' experience, challenges, and open issues (e.g., [85], [86]).

Another very essential aspect of e-Health is remote monitoring of health or wellness data. Telecare and telemedicine offer new opportunities for providing medical care to the home, including monitoring the well-being of patients, alarming when health conditions get worse and allowing to share patient data among health providers. Paper [87] presents an architecture for e-Health monitoring of chronic patients. The architecture from the user perspective includes wearable devices used to gather measurement data from the body and a smartphone used to process information received from the wearable devices. Therefore, it uses a database with an intelligent machine learning system that can send a notification when it detects an anomaly. A similar solutions can be found in [88] (called Ambient Assisted Living Health Platform (AALHP)) and [89]. Feng et al. in [90] propose a Home-based Elderly Care solution that uses 5G mobile network slicing. The solution contains Emergency Call Service, which ensures that appropriate medical personnel can provide help in a shorter time. Another similar approach using the cloud, called eWALL has been proposed: An Open-Source Cloud-Based e-Health Platform for Creating Home Caring Environments for Older Adults Living with Chronic Diseases or Frailty is described in [91]. Finally, besides monitoring, smarter medication can be a new opportunity. Applying medications to the patient on a remote basis could be made not only through monitoring from the patient's body but also through registering various high-risk factors (e.g., air pollution, temperature, pressure, etc.), with the city-wide monitoring devices. Currently, personal or sensitive data are an essential target for an attacker. Medical data may be of interest in illegal and unethical activities of insurance companies and even a potential employer. Therefore, this type of data should be appropriately managed and protected in transit and at rest. In [92] authors describe a novel IoT-oriented e-Health system powered by 5G network slicing for collecting heterogeneous medical data from different types of medical devices connected via a 5G network. The system includes various sub-mechanisms that aim to gather, analyze, and visualize data collected by all the devices. Paper [94] refers to using the blockchain approach to ensure proper audit logs for cross-border exchange of e-Health data. It provides traceability and liability based on the blockchain log management system and extends Bit4id's SmartLog solution [95]. Authors in [96] present a solution that protects

communication through health system monitoring based on the IoT. Due to using different communication technologies such as 6loWPAN, RPL, NFC, the solution includes two protocol stacks: one for device interfaces and the second is the Internet protocol stack. Such an approach guarantees the protection and safety of data processing inside an e-Health system monitoring.

Naturally, all use cases described earlier require proper planning, development, testing, and deployment in the context of new services. In [93] authors propose a framework for future planning of telemedicine services using 5G. The framework assumes planning with a basic understanding idea of service, estimation of cost and affordability, showing defects and benefits that are essential elements to be considered to avoid future problems.

2) Threats and vulnerabilities

According to the authors in [97] e-Health system architecture includes three areas:

- wireless body area network (BAN) which represents sensors on a human body,
- communication network which refers to communication channel and infrastructure,
- healthcare services which are associated with organizations providing medical services.

The studied literature [98]–[103] presents numerous threats and vulnerabilities in these areas, which are:

BAN: attacks on data (e.g., data leakage, data spoofing, data dropping, data exposure, data sniffing), frequency jamming attacks, attack on routing (e.g., path spoofing, sinkhole, Sybil attack, malware) and attack on availability (e.g., data flooding, Denial of Service).

Communication network: attacks on data (e.g., data sniffing, data tampering, data spoofing, leakage of geolocation data), rogue access point, man in the middle, Denial of Service.

Health organization: unauthorized data access, social engineering, phishing, malware, malicious removable device, physical threats (e.g., floods, earthquake, fire, terrorism attack, etc.), lack of backup and redundancy.

From an attacker's point of view, attacks on data seem to be very attractive. As medical data is gathered, transmitted and stored in e-Health databases, attackers can try to get access to them and cause havoc that influences the proper operation of all system components (e.g., modifying data or changing routing rules). Besides, the attacker can perform actions directly on the devices supporting the transmission (sensors, relay stations) or buildings where the data is stored (of course, natural threats are a separate issue). Another area of potential attacks is the availability of the system. In this area, the potential adversary can try to perform different flood attacks to stop the system.

3) Attacks and countermeasures

Protection of e-Health information systems is one of the most critical issues in the context of the law. Thus, every country must fulfill requirements to ensure the security of e-Health systems and their data. In [104] ENISA describes recommendations and comments regarding e-Health security issues for each European Union member state, for example, End-to-End encryption of exchanged personal health data, access control, security policy, or secure platform for the collection, analysis, and sharing of digital medical records. Another guide in which recommendations about health data can be found is The Health Insurance Portability and Accountability Act (HIPAA) [105]. HIPAA rules layout of privacy and security standards that protect the confidentiality of protected health information (PHI).

Many approaches on how to secure PHI or e-Health services can be found in the literature. Lots of them focus on cloud storage security. In [106] authors show a privacy-preserving e-Health cloud system. The proposed solution uses a Symmetric Searchable Encryption scheme which allows patients of an electronic Healthcare system to encrypt their medical data and search them without decryption. Another cloud protection solution is proposed in [107]. Paper [108] proposes The Privacy and Security Architecture Process, which must be ensured to protect medical information. Similar consideration can be found in [109]. Naturally, there are many more protection solutions in e-Health. To summarize, protection solutions and recommendations in e-Health focus on ensuring Authentication, Authorization, and Accounting (AAA), encrypting sensitive data, ensuring redundancy of systems and their high availability, protecting communication between patients and hospitals. However, the area of e-Health is still vulnerable to many different attacks.

E. RETAIL

1) Characteristics

The retail consists of institutions of a different type: from classic stationary shops, through various mixed solutions to Internet shops, whose number is growing rapidly during COVID-19 pandemic. Shops and shopping malls are using mobile applications to track customers, provide them with special offers, manage the sales and marketing processes. Many of them have their web pages which might provide the same functionality as mobile applications. Some pages are using *Progressive Web App* (PWA) approach [110], where the web page is a regular WWW page and a mobile application at once. All of them might use customers' data like locations to provide services from the nearest available shop. Retailers could better manage stockpiles of their products and adapt price strategies by using the collected data about customer demands and needs [111].

Retailers (and wholesalers) can be supported by 5G network. The paper [112] provides some use case scenarios, e.g.:

- smart bags that automatically count inventory items and handle transactions,
- better asset tracking with 5G enhanced connectivity,
- interaction with a customer in a more dynamic way,
- e-commerce, faster mobile payment,
- decreasing labor costs by applying online shopping.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

The working paper [112] concludes that the most important service in 5G applications for retail will be *massive IoT*. The *enhanced Mobile Broadband* will have a significant impact on this kind of verticals [112]. There are concepts like *intelligent e-commerce systems*, *smart e-commerce systems* (SES) [113] which are supported by Artificial Intelligence (AI) techniques. It leaves some space for using the advantages of 5G MEC because calculations might be shifted to the edge of the network to provide results faster, in the best time and place. Such a shift could be considered as a part of the context-awareness of SES [113], [114]. The 5G network might provide a higher degree of enjoyment for the customer, and his or her engagement in e-commerce activities [114]. The paper [113] also describes key issues and challenges related to the security layer that SES builder has to solve.

2) Threats and vulnerabilities

The connection between a customer and a retailer might be affected by an attacker employing well-known attacks like the DoS attack, session hijacking, session spoofing, and the Man-In-the-Middle attack. The victim might be a customer, a retailer, or both at once. In this domain, customers very often share credit card numbers or their social media accounts with retailers. This kind of data is valuable for attackers. It might be an element of further attacks. Access to retailer's services might be gained by using external identities with, e.g., OAuth2 protocol - the implementation in the retailer's system might be vulnerable.

For the customer, it might be valuable to obtain complete privacy for his or her data [115], not only during the transmission. Personal and contact data, credit card numbers, e-mail addresses, or phone numbers are very sensitive nowadays, and customers might require anonymization of part of the data. Ensuring privacy will protect the data against attackers and their usage unwanted by data provider [115]. The problem of trust between a customer and a retailer (e-commerce company) is wide and was discussed, e.g., in [115], [116].

For both main parties, the customer and the retailer (merchant), the crucial part is the payment process, which must be adequately secured, to avoid a money theft, a double spend, or a payment without *Two-Factor Authentication* (2FA) which becomes an industry standard. On the other hand, merchants are supporting *paypass* technology or mobile payment using the NFC standard, which allows low price payments without authenticating the payer.

The paper [113] describes five challenges for SES systems in terms of security and privacy: access control, auditing, intrusion detection, encryption, and authentication. It other words, retailers should consider using *Authentication, Authorization and Accounting* services, *Intrusion Detection System / Intrusion Prevention System* (IDS/IPS) solutions and using proper symmetric and asymmetric encryption, including *Public Key Infrastructure* PKI solutions.

3) Attacks and countermeasures

In the retail market, customized shopping experiences are becoming increasingly important, so data analysis tools help merchants implement them. However, there is a great responsibility to protect this data, which can include more than just shopping habits and login data and account details, personal data, and addresses. Thanks to Internet technologies, augmented reality, and face recognition, the shopping experience is becoming increasingly networked, but here, too, stronger networking entails a greater risk of data loss. Therefore, creating a resilient strategy approach, such as in the banking and healthcare sectors, is crucial for trade.

Retailers should implement security standards for processing payment, and credit card data like PCI DSS [117]. The high-level requirements in this standard are defined as follows:

1) Install and maintain a firewall configuration to protect cardholder data.
2) Do not use vendor-supplied defaults for system passwords and other security parameters.
3) Protect stored cardholder data.
4) Encrypt transmission of cardholder data across open, public networks.
5) Protect all systems against malware and regularly update anti-virus software or programs.
6) Develop and maintain secure systems and applications.
7) Restrict access to cardholder data by business need to know.
8) Identify and authenticate access to system components.
9) Restrict physical access to cardholder data.
10) Track and monitor all access to network resources and cardholder data.
11) Regularly test security systems and processes.
12) Maintain a policy that addresses information security for all personnel.

For implementing retailers' systems in 5G MEC, all points related to software and processes, except point 9, are of the highest importance. This point is also valid, but it is the Network Operator or the MEC Provider that is usually accountable for it (in RACI matrix model). Of course, if the merchant provides local networks available for customers, network elements should be adequately protected, e.g., from unattended physical access. The rest of the rules applies to all typical e-commerce software like online shops, API backend for mobile applications, or PWA web pages.

F. TELECOMMUNICATIONS

1) Characteristics

The network evolution is a huge opportunity for the Telecommunications sector, but it generates many new risks and vulnerabilities. Moreover, connectivity providers have to continuously improve their security methods and be aware of new threats because they are responsible for protecting data transported on their infrastructure in pursuance of the national regulations [123], [124].

According to the new virtualization paradigm, Mobile Network Operators can provide services even without having their own physical infrastructure [125]. In this case, they use resources shared with other independent Telecoms, so they play a new role called Mobile Virtual Network Operators. In some papers [126], [127] there are more precise definition of MVNO business model types (for example, MVNE, where a virtual operator implements own virtual network from the core part and offers it, Full MVNO, where an operator deploys own virtual network from the core network part and provides distribution channels, Light MVNO scenario, where the operator mainly prepares offers and provides distribution channels) but all are based on network virtualization. Of course, this type of business model is very popular because it is open for many companies that do not have their own network [125]. On the other hand, it gives an opportunity for better utilization of hardware resources [128]. Moreover, the physical infrastructure provider is obligated by governments and the regulatory agencies to ensure proper isolation and protection following security regulations [129].

Another challenge for Telecommunications sector is connected with realization of Edge Computing, which allows deploying services in the nodes situated closer to the users [130]–[133]. It means that new computation elements will appear in the network infrastructure, which other third parties can manage. Moreover, the responsibility of protecting such services belongs to the operator, and all new risks are inherited with them [134].

2) Threats and vulnerabilities

The principal vulnerabilities for Telecommunications verticals are caused by network virtualization, shared resources, and edge paradigm ecosystem. This trend is noticeable, especially in the case when more and more typical network functions (NF) are virtualized (VNF) and launched in different places in the network [135]. Their location often depends on the requirements of latency or bandwidth limits, so they are hosted where necessary (see [136]) or for economic purposes where the resources are available. What is essential, such relocation is not indifferent to security level because it indicates new threats [137] to VNFs which were usually not present in the legacy architecture and had additional perimeter protection.

Another issue related to elastic core network functionalities is the higher attack surface on the charging and policy system. It can happen when some of the data is not provided directly by all core components but only forwarded to the closest gateway situated at the edge for further redirection [138]. Moreover, a network operator has less awareness and control mechanism at its edge site, so in consequence, this area is more exposed to the standard network threats [139].

Besides the dynamic distribution of network functionalities, new technologies enable Telecoms to provide new types of services that are not directly connected with the operation of the network itself but can enhance its operation [140]. An example of such a scenario can be MEC which allows running service logic closer to the user [141], [142]. In this case, network elements cooperate with third-party applications, which can significantly affect their security [143]. Moreover, such untrusted or not well-protected elements can pose new threats by generating different types of attacks, data leakage, and other integration vulnerabilities [144].

The most challenging part for Telecommunications verticals is to manage all isolation between customers and ensure proper Quality of Service (QoS) for each defined slice or vertical. Opening of the own infrastructure for different edge solutions or VNFs might cause new risks connected with management. The management system should verify each request from MVNO because it can be generated by a malicious or misconfigured element of its virtual infrastructure and causes real danger affecting the resource utilization or the slice parameters [145]. In legacy networks, operators do not expose management API or its services to the customers, but in realizing dynamic network configuration and new network needs, it becomes essential. On the other hand, this feature causes many potential vulnerabilities, which are not known because such a management configuration was dedicated only for internal operator systems and should be secured in a standardized manner [146].

3) Attacks and countermeasures

The telecommunications vertical is one of the sectors most exposed to cyberattacks. Moreover, attacks are targeted on its many dimensions like infrastructure [147], communication [148], isolation [149] and many more. Another thing that is worth mentioning is presented in papers [150], [151], and concerns attacks that are not focused on the operator but affect its network, for example, high traffic caused by Denial of Service impacts its operation of all other network elements.

According to more global and grouped analyzes prepared by ENISA [152] the MVNO faces attacks related to network components like Core Network threats, Access Network threats, Multi-access Edge Computing threats, virtualization threats, physical infrastructure threats, SDN threats, and generic threats. The updated ENISA report can be found in [153].

To summarize, the Telecommunications sector is one of the most important verticals. It gives other verticals the opportunity for the realization of new services. However, due to its specificity, it is vulnerable to attacks on many different layers.

G. AUTHORITIES

1) Characteristics

Authorities sector as a vertical represents many administrative and government systems, which in some papers [156], [157] can be classified as a component of the critical infrastructure. Taking this into account for more precise characteristics of this ICT area, it is worth mentioning that its original purpose relates to Public Administration [158]. The needs of automation, increased productivity and economic aspects

in some regular authorities' operations result in growth and popularization of the e-Administration [159]. For this reason, public services became computerized and open for cooperation with other systems. The subject of its integration started to be necessary after the evolution of 5G network. Finally, each country has its own regulations, which should be compliant with policies defined by international entities [160].

Another type which is very often associated in the literature with the Authority sector is e-government. Its evolution rate is very high nowadays, and users can sort out more and more cases remotely [161]. All these operations are possible because the information is shared between multiple systems. It causes new challenges which relate to the data format and data protection [162].

Increasing number of e-Administration, e-Governments, and other public services is related to higher needs of IT resources. Therefore, according to global trends of cost optimization, these types of systems can be hosted in the cloud [163]. Installation of Authorities in the distributed environments requires, besides economic benefits, new models of clouds [164] and carries new risk and challenges for administrators [165], [166].

Protection of this system is very difficult because it stores very sensitive data. However, there are some best practices which describe security fundamentals [167], but more information about vulnerabilities and attack can be found in the following sections.

2) Threats and vulnerabilities

Authorities sector holds very sensitive data which are the target of attacks. Therefore security aspects are crucial and often were a barrier to the implementation of public services in many countries [168]. Moreover, even after the successful development of a typical e-Government system, it consists of three main elements [169] which can involve additional risks and involve data leakage (technologies, processes, and people).

From the technical perspective, as mentioned in the previous section, there is a trend to host public services in the cloud. It allows avoiding data losses by using redundancy but causes new issues related to interconnection and integration with other distributed systems [170]. Some of these problems can be solved using security framework [171], using additional proxy and tokens to verify and authorize components located in different places. NIST proposed a similar solution in [172] but, apart from detection and protection, it comes with new functionalities which allow preparing recovery operations.

Automation of regular process is the main task for each e-Administration services, but at the same time, it needs to interact with a user, which can provoke a threat. Public services use Web portals to avoid exposure of all sensitive data. This type of data presentation should be divided into a minimum of three parts (frontend, backend, and external) and be implemented under best practices [173].

Security risks related to the people are the most difficult to predict and to avoid. Nevertheless, using specific policy and standards for users, their accounts, their roles, passwords, and privileges [174], it is possible to minimize vulnerabilities in this area.

3) Attacks and countermeasures

Cyberattack challenges in the Authority sector are mainly connected with data protection, which can be very sensitive, like information related to ministries, voter information, and even military defense plans. It can be confirmed by the results of the survey presented in [175] where 82% of companies associated with the public sector declared concerns about data loss in the first place.

One of the primary roles of e-Administration is data exposure to authorized users only. According to [176] this security mechanism is often not implemented well or not updated so it precipitates typical attacks, which can be avoided using proper practices and policy rules [177].

Some other aspects which provoke cyberattacks in the Authorities domain are mentioned in [178] and are related to poor risk management and increased numbers of phishing attacks in the e-administration.

According to publications cited in the previous and this section, another increasing type of attack on the public sector is Cyber terrorism [179]. This attack is often prepared by another country to paralyze the opponent system or to steal crucial and sensitive government data.

In summary, the security needs of Authorities and their main requirements are related to data protection, distribution, and AAA.

H. MEDIA AND ENTERTAINMENT

1) Characteristics

Nowadays, media and entertainment business experiences huge changes in habits of users [182]–[184]. Customers do not want to watch only linear TV, but on-demand content, user-generated content, e-sport, games, too. Therefore, it is essential to have the environment where the content is consumed (e.g., at home, on the move, during holidays, etc.). Also, the type of device that directly provides the user's content (e.g., TV, mobile phone, PC, tablets, watches, remote controllers, virtual reality devices, etc.) is crucial. On the other hand, the game sector with online games tends to provide as much realism as possible, a high-level user real-time interaction and experience.

One of the main factors which cause a change in users' behaviors is the Internet. The growth of network speed, both fixed and mobile Internet, together with data centers and cloud computing, has impacted user positive experience. Also, the growth of the capabilities of devices with various services has influenced the way people perceive media and entertainment. Paper [185] presents considerations on the study and deployment of the MEC for tactile Internet using a 5G gaming application. Moreover, the authors show the implementation of the proposed ACM protocol (Agile Cloud

Migration) in a delay-sensitive gaming application located in Mobile Cloud Computing. The server is migrated live during the game between users and transparently to them. The agile Migration approach can be found in [186], too. Authors focus on realizing the Mobile Edge Cloud for low delay 5G applications through a game to engage the audience. Without a doubt, the usage of the MEC infrastructure can cause offloading problems, which can impact latency and energy consumption. Paper [187] illustrates a study on computation offloading in the overlapping coverage area of service scope under the system of adjacent edge nodes. Results obtained during this research can help to increase the management of the MEC resources.

We have been observing an increase in the number of people playing computer games for years. It is possible because of the current technological progress, which ensures the appropriate realism of games. The 5G network can affect even more playability. Many solutions concerning the use of 5G infrastructure can be found in the literature. Authors in [188] created a game platform for developing the game streaming platform. Paper [189] presents an implementation of a VR game with the ability to move game servers across the world without any service interruption. Mobile open-source cloud gaming system, which uses the Android Open Source Project (AOSP) mobile operating system in the cloud, can be found in paper [190]. These are only selected examples confirming the increase in the importance of virtual reality in 5G.

To provide good quality of media and entertainment from the 5G network, what is required is the high speed of connection, mobility, End-to-End low latency, coverage reliability, and proper resources management. However, what is even more important is the tremendous immerse experience associated with virtual reality. Paper [191] refers to a solution in which players' mobile devices can offload particular game tasks to a server or neighboring mobile devices. Due to such an idea, it is possible to increase users' experience, better use available energy resources, reduce the bandwidth and computing costs of the system. Zadtootaghaj et al. in [192] discuss the results of subjective research in which the impact of two factors, frame rate and bit rate, on the gaming Quality of Experience was examined. The results demonstrate the existence of a trade-off between sufficient and interaction video quality. Naturally, the entertainment environment can be used in many areas associated with our life, such as connected car communication [193] or In-Flight Entertainment [194].

From a security point of view, it is crucial to consider identity management and identification and reliability of content sources to ensure that only authorized subscribers can use them.

2) Threats and vulnerabilities

Considering threats in media and entertainment, we can distinguish three components that may be the target of a potential attack:

Application and device - which refers to the device and applications installed on it, which are used for entertainment purposes;

Communication channel - which includes all aspects of communication between user and service provider;

Server - which contains service that is provided to users and the necessary infrastructure;

In this subsection, we will not discuss threats to applications, communication, and services. We will consider only specific cases of the Media and Entertainment category. Detailed threats associated with VR/AR can be found in Subsection II-L *Education and culture science*. Here we focus on connected cars and in-flight entertainment. One of the most crucial security problems is the fact that vehicles and their entertainment systems are connected to large and open networks such as the Internet. If this access is not secured correctly, an adversary can manipulate, destroy or spoof data [120], [121]. Therefore, from the privacy point of view, such a vehicle or in-flight entertainment often allows tracking user location, which hijackers or stalkers can use.

Presently, vehicles are sophisticated systems that have a connection to the network. As a result, an attacker can take control over microcontrollers and cause harm to passengers or people on the roads (for example, by brakes or whole engine manipulation).

Another problem with entertainment is user interaction with it. Very often, such a solution enables a user to input data. It may be done intentionally or unintentionally and lead to at least data disclosure and even data manipulation.

Finally, problems may occur with Denial of Service, black hole attack, and warm hole attack associated with routing threats and timing attacks.

3) Attacks and countermeasures

Countermeasure against threats described in the previous subsection are listed below:

- As usual, proper authentication and access control for vehicle environment that is connected to the Internet is an important solution to avoid unauthorized access.
- Usage of strong cryptographic algorithm and protocols can be mitigation against routing attacks, timing, replay, or session attacks.
- Usage of proper transport layer protection mechanism (such as TLSv1.2) to protect the communication channel.
- Sanitization is the process of cleaning or filtering input data. Whether the data is from a user or an API or web service, sanitization can be used when we do not know what to expect or do not want to be strict with data validation.
- Installation of the dedicated malware detection system is highly recommended, too. For instance, the E-Safety Vehicle Intrusion Protected Applications (EVITA) [122].
- Frequent updates of entertainment software will help maintain a high level of security.

I. SMART CITY

1) Characteristics

One of the essential branches of new technologies for 5G MEC is the Smart City. This concept consists of various *smart* objects like intelligent buildings, smart homes, innovative infrastructure, or smart mobility. It includes many other domains, stakeholders, and activities [206] like the intelligent economy, smart living, innovative environment, smart governance, and smart citizens. Some of them are considered in other parts of this paper.

Different definitions for a Smart Home, known as the Connected Home, Home Automation or Domotics, were discussed in the paper [207]. They listed the most popular Smart Home applications:

- smart locks,
- smart TVs,
- smart security cameras and sensors,
- smart blinds,
- smart thermostats,
- smart lighting,
- smart appliances,
- smart irrigation.

The main goal for the Smart Home is to satisfy the needs of the residents whether they are inside the home or not [206]. Homes might send massive information outside their local networks, including such traffic as video, Virtual Reality, and Augmented Reality connections.

5G envisages the usage of various radio network interfaces like 4G eNodeB, Wi-Fi or pico- and femtocells. Applying a proper wireless technology is crucial due to signal interferences, path losses, and penetration losses [208], which are critical smart home network challenges. Due to the significant impact of used materials in building on the signal power loss, the *Quality of Service* (QoS) and *Quality of Experience* (QoE) might be different even in the same apartment or office.

The cooperation between real estate owners and 5G MEC providers might be defined differently. The radio infrastructure must be deployed closer to the User Equipment, which means that the building owner might be responsible for providing some support for it, e.g., in office buildings. Property owners might use the infrastructure to provide their own services, like shopping malls, airports, train stations, universities.

There are new possibilities for structural monitoring of buildings and infrastructure against anomalies and critical situations even in emergency conditions like earthquakes [209]. Those solutions may use IoT devices, especially sensors or drones, which connect in the *Device-to-Device* communication (D2D) [211] or to the same shared point, e.g., MEC server. Those devices may transfer much data that must be processed or analyzed, and it might be done in the MEC infrastructure using MEC applications. This approach allows processing data from multiple sources, which may be required in some algorithms, e.g., triangulation or surveillance.

One of the most critical parts of Smart City is smart infrastructure. All devices measuring used resources like power meters, water meters, gas meters, or heat meters might be connected to the Internet to provide up-to-date information about actual and expected resource consumption. In the case of the electrical network, this approach is called *smart grid*.

There are also some general recommendations (best practices) in [212] that EU suggests following. Those guidelines are related more to an administrative and financial point of view; however, this is a crucial part of every severe ICT project and solution in practice.

2) Threats and vulnerabilities

One of the biggest concerns about smart homes and smart cities is privacy [213], which is strongly protected, especially in the EU by General Data Protection Regulation [214]. Intelligent devices are continuously analyzing our voice, localization, and behavior. Mobile applications that are used for managing IoT devices are using data and sensors available on the mobile phone, so the amount of data that is processed and might leak at some point in time is enormous.

Devices used for surveillance and threat detection might be abused, causing false alarms. The cost of such an attack might be huge in case of evacuation or launching physical systems like water sprinklers in buildings. From the network perspective, such an alarm will produce additional traffic with high priority and might exhaust network resources in the nearest MEC server.

In Smart City, the *Property Owner* (PO) might be a proxy between User Equipment and *Internet Service Provider* (ISP) or 5G MEC operator. The attacker might use public or semi-public networks hosted by PO to launch an attack. The infrastructure used by PO might be used in such scenarios, including DoS attacks.

For infrastructure and smart grid scenarios, data transferred between devices might be changed, which might cause damage to the infrastructure or other devices (in case of electricity). The range of attacks might be enormous, just like in other disaster scenarios, e.g., blackouts.

3) Attacks and countermeasures

In the paper [210] following attacks violating smart cities were enumerated:

- eavesdropping,
- DoS attack,
- Man-in-the-Middle attack,
- side channel attacks,
- identification attack,
- secondary use (reply attack, forging attack),
- phishing,
- spoofing,
- attack to data integrity.

All these attacks are generic and might be applied to other verticals. Recommendations ITU-T SG 13 (Future Networks), ITU-T SG-17 (Security), ITU-T SG 16 (Multimedia) could be implemented in Smart City solutions [215].

Network Operator should prepare a safe place for processing private and fragile data from clients in the 5G MEC envi-

ronment. The solution should use firewalls, disk encryption, proper data transfer encryption, strict Access Control List (ACL) with appropriate policies for data access. Access to web services must be authenticated and authorized correctly. Network Operators should use the IDS or IPS system as well.

The MEC infrastructure and physical neighborhood might be affected by false alarms detected by IoT devices connected to the MEC server. Such special services should be consulted or designed with cooperation with 5G MEC providers.

J. AGRICULTURE AND FOOD INDUSTRY

1) Characteristics

The agriculture and food industry is one of the crucial parts of each national economy. Therefore, to increase the efficiency of production in this sector and at the same time minimize losses caused by natural disasters or extreme weather changes, multiple factors are monitored and managed with IoT devices. Collection of such data in these environments requires specific protection from infrastructure due to limited access to power, exposition to dust, rain, vibration, and other conditions present in the rural areas [219].

Another challenge for implementing these systems is to provide extensive coverage of connectivity and low costs deployment of a high number of sensors. Consequently, from an economic perspective, most IoT devices used for agriculture are very simple and connect with applications with relatively low needs in terms of bandwidth and latency [220]. Low requirements for communication parameters allow to use of legacy 2G network and low-power wide-area (LPWA) technologies for this purpose, but on the other hand, using free frequencies can be open for additional threats [221]. Moreover, in agriculture applications, some evolution can be observed, which enforces usage of more advanced data operations (Edge Computing, Augmented Reality, AI analyzes, etc.) and needs higher network parameters provided by the new generation of 5G network [222].

Having this in mind, it is challenging to prepare one common characteristic for all farming systems because there are many agriculture application types (Irrigation, Fertilization, Pest control, Animal monitoring, Forestry, etc.). They have different realization scenarios with different needs (type of radio transmission, message frequency, latency, protection, data processing, access to external systems) [221], [223]. Therefore, to have one reference architecture that can be an abstraction for all of them, it should be presented as a set of common layers (realization of each of them is dependent on the use case and needed technology) [220]:

- Sensing layer - includes all types of sensors.
- Bridge layer - includes all types of connection with sensor and gateways to the next part of the system (e.g., Wi-Fi, Bluetooth, ZigBee, RFID).
- Backbone layer - includes devices that have a role of data aggregation and gateway to the network (e.g., Internet).
- End layer - includes all data collecting systems.

The final implementation of the presented layers mainly dependent on purpose, economic aspects, and the regional stakeholders, which for different countries can differ, and examples of that can be found in [224], [225].

2) Threats and vulnerabilities

As it was described in the characteristic of the food and agriculture sector, it has many implementation combination variants, which causes a similar number of threats. Most of them are closely connected to the susceptibility of LPWA communications mechanisms because the farming IoT devices support different radio access connection types (both in licensed, e.g., LTE-M, NB-IoT, eMTC, EC-GSM-IoT, and 2G [226] and not licensed spectrum, e.g., NFC/RFID, LoRa, Wi-Fi, SIGFOX, and DAS7 [227], [228]). In the case of licensed radio spectrum standards, they are protected well, but more information about its vulnerabilities can be found in [229], [230]. Sensors that use not licensed radio frequencies are vulnerable to common threats for IoT devices, for example, presented in papers [227], [231].

What is essential, threats presented above in the bridge layer can propagate deeper into the entire system. On the other hand, protocols like Bluetooth or ZigBee are sometimes used in farming systems for mesh network realization. In this case, it provides connectivity for peer-to-peer wireless communications [232], which cannot be seen in the upper system layer, and in consequence, some of the threats are hard to be detected [233], [234].

Next abstraction layer for the agriculture sector is the backbone layer. Its primary role is to collect all data from the device and send it to the proper end system. The principal vulnerabilities of these elements are Denial of Service caused by fake requests and unauthorized access attempts [235]. Of course, both infected sensors and external devices not belonging to the system can be sources of these threats [236].

For the end layer, it is common for all types of IT systems, and its security is high implementation-dependent (data collection system, cloud realization, openness).

Threats aspects which can be presented in each agriculture system layer, their categorization and impact on Confidentiality, Integrity, and Availability are presented in [237], [238]. To conclude, they can be divided into:

- Intentional theft from Agriculture systems (for example, Decision Support System - DSS, Unmanned Aerial System - UAS).
- Intentional falsification of the data to disrupt work of systems supporting Agriculture (for example, crop or livestock sectors, machine learning modeling system, or rogue data into a sensor network).
- Intentional disruption of data connected with positioning, timing, and equipment availability.

The last thing which is important and characteristic for agriculture devices is its distribution over large rural areas and, consequently, susceptibility to theft.

3) Attacks and countermeasures

Attacks on the agriculture sector known in the literature (see [231], [236], [239]) can be classified by many criteria, application types, and farming models, but all of them are based on the IoT systems, so in consequence, the security risks are connected with the common IoT architecture [240].

Therefore, from the smart farming perspective cyberattacks, can be grouped into four categories (data attacks, network and equipment attacks, supply chain attacks, other relevant attacks) [231], [236].

Data Attacks are mainly made by hackers who want to analyze or manipulate data to provide wrong information or steal sensitive data. For this purpose, techniques of Interruption, Interception, Modification, and reply of data are used.

Network and Equipment Attacks can be realized by compromising both hardware (reprogramming device with malicious code) and software (usage of application or software vulnerabilities) components. These criteria include all types of attacks that can compromise network protocols used for communication.

Supply Chain Attacks are similar to the previous point and can be realized, e.g., by malware injections. The difference is in the attacker objective, consisting mainly of interruption of system operation by fabrication of data or stooping some of the crucial elements.

Other Relevant Attacks are used to classify all other cyberattacks that can be realized in the agriculture sector, including aspects of Cyber Terrorism and others.

K. LOGISTICS

1) Characteristics

Proper supply of resources and items is essential for many businesses and end customers. The End-to-End supply chains might be considered on various scales: from a micro-scale related to a single store or warehouse to supplying thousands of shops. The second branch delivers items to end customers (Business-to-Client model - B2C), strongly increasing with online shopping in recent years. There is also a Business-to-Business (B2B) model, where the receiver is not a reseller but requires deliveries for its own purposes. There are multiple parties for contracts, e.g., [195]:

- suppliers of raw materials, semi-finished products, and finished products,
- wholesalers,
- retailers,
- outsourced partners,
- providers of simple services such as transport or storage,
- third-party logistics (3PL) - offering logistics services in areas of procurement, distribution, and movement of goods in the manufacturing process, packaging, warranty management,
- integrators in the supply chain,
- fourth-party logistics (4PL) - companies offering services far more complicated than simple storage or transport.

There are other categorizations, e.g., [196] divides the transportation sector into the road, rail, aviation, and maritime sub-sectors. Each of them has its own security characteristic. From 5G MEC Network Operator perspective, solutions based on road and rail are the most interesting and are much easier to adopt than aviation- or maritime-based. On the other hand, maritime transport is the cheapest for long distances and sometimes it is the only acceptable solution due to the high costs of typical air traffic. On shorter distances, drones might be used; this includes the possibility of using advantages of 5G MEC network because a drone might use lower flight altitude than airplanes. The interesting part is a set of airports, water ports, and terminals that might be treated as a part of the Smart City concept, described in Subsection II-I.

Logistics companies might use ICT systems in the order picking process, manage routes for couriers in real-time depending on end user availability, monitor supply levels. Companies could use smart transportation systems [206] for their vehicle fleet to improve drivers' and items' security and safety. Such companies might share information in Vehicle-to-Vehicle (V2V) manner, including speed, location, directions of travel, braking, loss of stability, traffic jams, icy road, or fog [206]. The driving itself might be assisted or autonomous and empowered by 5G [209]. The information can be sent to other vehicles and a central point as well [206]. The point might be in the MEC infrastructure, e.g., [197] shows such a concept where *Cooperative Awareness Messages* (CAM) are shared by vehicles and stored in a *Cooperative Information Manager* (CIM) database located within the MEC host. There are other positive aspects of incorporating telecommunications solutions based on 5G within the whole transportation ecosystem, e.g., described in [111]: quickly identifying free parking spaces or reducing urban concentration. The paper [31] shows the advantages of introducing the MEC platform in Vehicle-to-everything(V2X) scenarios like bird's eye view due to collecting data from multiple sources. It is not available in cellular networks like LTE-based. Close to logistics is personal mobility, which includes various applications of public transport. Those solutions are implementing *Mobility-as-a-Service* (MaaS), also known as *Transport-as-a-Service* (TaaS) concepts [198]. The concept of MaaS provides the customer an answer to the question: *How can I get to this place?* including multiple transportation solutions like buses, trams, taxi rides, public scooters, or shared cars. It may be used both by customers and couriers to deliver objects like packages or food.

2) Threats and vulnerabilities

In typical situations, the biggest threat in logistics is the physical safety and security of items. It includes thefts, confiscation of items, damage during transport, e.g., by accident. Those risks were described widely in [199] as political, economic, and operational risks. There might be possible attacks on ICT infrastructure, including 5G MEC infrastructure, to hit the logistics process. However, the risk

is relatively small, mainly when humans supervise the whole process. The valuable transports (money, jewelry) are often guarded, which increases the risk significantly for attackers. More possible is an attack on documents or credit cards sent by standard mail.

Due to possible consequences, V2V traffic should be treated carefully. This traffic might be affected not only by an intentional attack but also by software defects and incidents. Also, raw packet jitter and lack of signal are very dangerous in some scenarios, where reliability and latency must be stable. Vehicles must be able to do necessary computations with their own computation power, even if results are worse than results obtained with services supported by the MEC environment. Couriers are affected by variable Internet access quality, and their applications might not work correctly in some physical places.

Drone-based delivery approach as well suffers from various security problems. The most important security issues are related to communication between the drone and its controller (dispatcher). It includes all typical attacks on wireless networks. Essential is power management and attacks, which are overusing the device's battery.

3) Attacks and countermeasures

Logistics applications used by couriers, deployed in stationary stores or lockers might be treated as other mobile applications in terms of attacks (e.g., DoS attacks on MEC applications, rogue gNodeB) and typical countermeasures (load balancers/anti-DoS systems, CDNs, proper AAA mechanisms). Those typical attacks are described with real incidents in [196], mainly related to airports or railways. Traceability and provability might be improved by applying the blockchain technology [200]. It is not only a security feature but might be a significant improvement in the business process by reducing the amount of undetected or late detected human errors. Those errors are indicated as significant, e.g., by [201].

Automotive scenarios might require reliable responses from the MEC server, which can be affected by the jamming attack, communication hijacking, natural network jitter, or changes in the propagation channel between the device and gNodeB. In such a scenario, the application must be self-sufficient as long as possible to avoid significant damage or accident, e.g., by autonomous drive or flight. This assumption can be satisfied using iterative or adaptive algorithms with a starting feasible solution calculated directly by the autonomous device.

Other untypical class of attacks is exhausting the device's power resources to make it unavailable for the dispatcher or prevent communication between the device and other services, primarily hosted on the MEC server. Devices should monitor their available energy and report to the dispatcher any suspicious situations and trends.

L. EDUCATION, CULTURE AND SCIENCE

1) Characteristics

In the 5G context, education will be changed a lot. Some of the use cases refer to [246]–[248]:

- Tactile Internet & Virtual Reality (VR),
- Augmented Reality (AR) & education,
- walled-off classroom,
- personalized learning,
- student wireless backpack,
- student with special needs,
- IoT & smart classroom.

The International Telecommunication Union (ITU) defines the Tactile Internet as an Internet network that combines ultra-low latency with extremely high availability, security, and reliability. It also enables tactile interaction with visual feedback, with technical systems supporting audiovisual interaction with a minimal delay. The Tactile Internet will improve learning experiences based on the haptic overlay of the teacher and learner. Applications such as VR and AR will improve. For example, by combining the Tactile Internet with VR and AR, the learning experience will go far beyond the learning methods used nowadays and give students more opportunities to learn, mostly through exploration and discovery. Therefore, there will be minimal involvement from teachers and less pressure.

Like Virtual Reality, the Augmented Reality has started to present its role and usefulness in education. AR can be an efficient solution for providing the proper amount of information at the exact time to the right people. Additionally, AR can enable new ways of learning and work in teams. On the other hand, it can help teachers get more data about the student, their needs, and capabilities. Authors in [249] describe the connection between 5G technologies and education, focusing on activities based on VR and AR. Moreover, they present a few examples dealing with the evolution of online academic courses.

Walled-off classroom can change an approach to remote learning due to VR and Tactile Internet. It can remove physical barriers associated with localization and helps many students to share files. It is crucial in the context of conducting experiments with the use of expensive devices. Authors in [250] propose a training workplace for mobile devices e-learning that uses Wi-Fi and 5G technology. What is worth to emphasize, the created solution provides a new learning method based on mobile e-learning, micro-lectures and flipped classroom and teach many subjects remotely. Paper [251] considers the influence of the 5G network on music education. Besides, the paper includes a few educational scenarios, proposing several advanced didactic services and applications in music education, which seems to be a good testbed for creating and deploying to demanding environments. On the other hand, paper [249] refers to the role of 5G networks in medical sciences education.

As a result of easy access to the Internet of mobile devices, personalized learning can allow individuals to connect to educational systems. It means an evolution of solutions that

suggest learning pathways, aggregative student data, and experience and finally analyzes students' progress and better decision-making about further learning and education.

Modern approach of access to storage service in cloud computing offers work with some delay even with a high Internet speed. The use of 5G technology will enable faster access to the whole content through distributed cloud and Mobile Edge Computing with ultra-small latency. As a result, students will be able to access their files and resume work at any time and place using different devices with an impression of immediate response time.

Advance progress in mobile technology and robotics can offer a new opportunity for a student with special needs. Cloud-based robots can be used to make learning easier for that student. For example, such a robot can be treated as a full-time assistant for disabled students, helping them in the education field and with peers. Besides, instead of contacting teachers and asking for help, which can be painful to the student and take the time from the teacher, the student can ask robots to help solve an issue.

Because of the significant increase in the importance of IoT in our lives, this concept can be used in teaching areas such as teaching or learning and administrative support of the school. IoT can change the role of the teacher in the classroom, reducing administrative work and focusing on the individuals. The student who will be authenticated to the classroom will be monitored during the lecture. He or she will get comments from the teacher about topics that still need to be improved, etc.

2) Threats and vulnerabilities

According to papers [253]–[258] eLearning and education in general in the 5G context are exposed to cybersecurity threats. The threats refer to categories listed below:

Data which is usually collected by the system to be processed in future actions.

Input which is gathered and inputted to the VR/AR platform.

Output which is sent to the VR/AR reality device to be displayed or rendered.

User Interaction such as sharing and collaborations in VR/AR.

Devices represented by physical VR/AR devices and the physical input and output interfaces of these devices.

Data, in this case, should be considered in three aspects of data: collection, storing, and processing. The main threats are connected with data collection are tapering, unauthorized access to them, and Denial of Service. After gathering data, systems usually process them to decide what to do in the next step. During processing, other applications can try to access user data which can contain sensitive information. Therefore, data is exposed to leakage, linkability (it is possible to link all the events or records that belong to the same data subject together), and identifiability (we can correctly assign an event or record to an identifiable or known individual with a high probability). Finally, after data gathering, the system stores them in databases (locally or in cloud computing). From the privacy, there is no certainty whether the data is used in any other way than the purpose for which it was obtained. Besides privacy, security threats can be listed: tampering, unauthorized access, or spoofing.

The main risk involved with input data is unauthorized or unintended (accidental and purposeful) data disclosure. The threats in this aspect refer to issues connected with confidentially, detectability, and user awareness of data. Another crucial input that needs to be protected is gesture input. Nowadays, the most popular interfaces among users are tactile types such as the keyboard, PC mouse, and touch interface. Due to this, physical threats can occur (e.g., shoulder surfing, external inference), and spoofing, Denial of Service, or data manipulation can be performed.

Security problems with the data output, in general, are associated with display output: reliability of output and proper rendering. As a result, an attacker can potentially modify or spoof outputs that may compromise user safety.

The significant concerns related to collaboration arise from data sharing within boundaries of shared spaces. It can potentially cause spoofing during this action. Consequently, a legitimate user can be exposed to Denial of Service or interception and leakage of sensitive data.

Threats on the device level comprise two areas: device access and display protection. With the device, access is associated at least two problems with the user's identity: identity spoofing and unauthorized access. Potential attackers can masquerade as a valid user to get access to the system. In the context of display, VR/AR are vulnerable to malicious interference, which can cause exposure of display information or capture data from display leakage. Moreover, in some cases, abuse of resources of the device, such as battery power limits or computing, can be a threat as a potential source of the attack.

3) Attacks and countermeasures

Protection of data should be considered in the same areas as threats: collection, storing, and processing. Firstly, privacy-preserving data collection solutions should be considered (e.g., [259]). Secondly, encryption methods and proper access control to data should be ensured. Finally, encryption-based solution during processing (e.g., homomorphic encryption [260]) and secret sharing technics [261].

The major technic which protects input data is input sanitization (e.g., context-based sanitization [262], video sanitization [263]). Moreover, to protect the user's gesture secure gesture detection and recognition solution that sends only gesture events to the applications must be deployed (e.g., [264]).

To protect output, output control policies responsible for the management of rendering priority can be used. Of course, the least privilege rule is always worth implementing in the context of proper rendering. Finally, to protect display,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

content hiding methods (e.g., [265]) and visual cryptography (e.g., [266]) can be deployed.

To protect collaboration and sharing, the primary strategies are detailed policy specifications for users and its enforcement. Therefore, since every interaction is possible through the same sharing channel, it is good to protect it (e.g., using a solution such as [267]).

The access control is a selective restriction of access to data (access only for an authorized person) based on two components: authentication and authorization. Nowadays, passwords are still the most popular and most commonly used authentication method. Passwords have some weaknesses. To increase the strength of this method, the multi-factor authentication (MFA) was introduced. MFA uses two or more independent authentication methods (e.g., password with a biometric feature of a particular person). In context, VR/AR devices in literature can be found several authentication solutions based on user gestures recognition [268]–[270] or other biometric methods [271]. To protect against data display, solutions based on the concept of visual cryptography can be used.

M. CRITICAL INFRASTRUCTURE SECTORS

1) Characteristics

According to the US Cybersecurity and Infrastructure Security Agency (CISA) the critical infrastructure contains the following sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems, and Sector-Specific Agencies. These sectors can be quite different if considering the technologies they apply, their social role, and the stakeholders. The common aspect is that their assets, systems, and networks, whether physical or virtual, are considered so vital to countries (and international cooperation) that their exclusion or destruction would have a weakening effect on national security, economic security, national public health, and public safety, or any combination thereof, see [47]. So, let us consider the critical infrastructure as a 5G MEC vertical industry. We must not consider it from the point of view of its component sectors and their specific stakeholders. We should treat the critical infrastructure as the infrastructural skeleton of a country and analyze its functioning from a high-level perspective and on a wide scale. Countries and international organizations, especially European Union, see [272], identify essential services crucial for the functioning and security of the critical infrastructure. According to legal regulations, the state authorities impose specific regulations on operators serving such services concerning business continuity, disaster recovery, and security. The existing network communication technologies are being adopted for requirements of the critical infrastructure, see, e.g., [273], [274], to satisfy enhanced network performance and security parameters. Moreover, some sectors of critical infrastructure use dedicated communication networks isolated or partially isolated from the Internet or using specific technologies [275]. An alternative solution can be applying dedicated secure network slicing [276], [277].

2) Threats and vulnerabilities

Resources assigned to the national critical infrastructure become the target of individual hackers, terrorist organizations, and rogue states. It is especially dangerous when Advanced Persistent Threat (APT) attacks [278] are carried by highly skilled (very often state-sponsored or state-protected) cybercriminal groups who have access to practically unlimited resources for their use. The chapter [279] presents three APT groups attacking the critical infrastructure of western countries, called: *APT28*, *Red October*, and *Regin*. One can identify types of organizations targeted by such attackers and vulnerabilities attractive to such APT groups. The paper [279] presents attacks and exploited vulnerabilities of the three APT groups. They tend to move quickly to take advantage of recently disclosed vulnerabilities (e.g., zero-day exploits), use modules to actively scan the Local Area Network (LAN) to find vulnerable hosts, use security vulnerabilities inside Microsoft Office suite (especially MS Excel and MS Word), pdf files, and exploit Adobe Flash vulnerabilities and web application vulnerabilities.

3) Attacks and countermeasures

The critical infrastructure consists of several vertical industries (some of them already presented in the previous sections), where each of them has its own dedicated security countermeasures. However, if we consider them as components of the particular importance infrastructure, they need additional protection, which is reflected in legal regulations, standards, and enhanced security solutions. Among security countermeasures for critical infrastructure, dedicated legal regulations are essential. The authorities oblige digital service providers (especially essential service providers) to apply risk management procedures, incident reporting, and apply string security protection mechanisms, see, the EU regulation [280] for the specification of the elements to be considered by digital service providers for managing the risks posed to the security of network and information systems and the parameters for determining whether an incident has a substantial impact.

Another important group of regulations affecting critical infrastructure security is national and international standards. Initially, this sector has its own dedicated security standards. However, in the 1990's the US government (and following it most western countries) moved away from the customized military specifications and military standards philosophy to a common for other sectors general commercial-based standards approach [281]. Now, both NIST and ISO standards cover all security management and security algorithm requirements for critical infrastructure expectations [282].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 2. Threats defined in ENISA paper and their relation to verticals

Threats [ENISA]	Manufacturing industry	The Financial Sector	Healthcare	Retail	Telecommunications	Authorities	Media and Entertainment	Smart City	Agriculture and food industry	Logistics	Education, culture and science	Critical Infrastructure Sectors	#X	#V	#?
Malware	V	V	V	V	V	V	V	V	V	V	V	V	0	12	0
Web Based Attacks	V	V	X	V	X	V	V	V	?	V	?	V	2	8	2
Web Application Attacks	V	V	X	V	X	V	V	V	?	V	?	V	2	8	2
Phishing	X	V	V	V	?	V	?	V	X	V	V	V	2	8	2
Denial of Service	?	V	V	V	V	V	V	V	V	V	?	V	0	10	2
Spam	X	V	X	X	?	V	?	X	X	X	?	?	6	2	4
Botnets	?	V	?	V	V	X	V	V	V	V	X	V	2	8	2
Data Breaches	V	V	V	V	V	V	?	V	V	V	V	V	0	11	1
Insider threat	V	?	V	V	V	?	V	V	V	V	V	?	0	9	3
Physical	?	X	X	X	V	X	X	V	V	V	V	V	5	6	1
Information Leakage	V	V	V	V	V	V	?	V	V	V	V	V	0	11	1
Identity theft	V	V	V	V	V	V	?	V	V	V	V	V	0	11	1
Cryptojacking	?	X	?	V	X	?	X	V	?	V	X	?	4	3	5
Ransomware	?	V	X	V	X	V	X	X	?	V	?	?	4	4	4
Cyber Espionage	V	V	V	X	V	V	?	X	?	V	V	V	2	8	2

Dedicated military and confidential solutions are only a supplement to the public, and commercial tools [283].

Except for usual protection methods, the critical infrastructure vertical has its dedicated enhanced security systems and methodologies. Such methods are Cyber Kill Chain [284] and Diamond Model of Intrusion Analysis [285] (or a combination of the two [279]). Moreover, modern approaches for providing security in this sector are considered, like game-theory-based [286], blockchain-based [287], or AI-based methods [288].

N. SUMMARY

In this Section, we presented basic properties of the twelve most prospective 5G vertical industries, which will fix the development of the future digital economy. Making an extensive literature overview, we briefly presented characteristics of these industries, including their role in the present society. We also made an overview of an ecosystem of each vertical industry and presented specific threats and vulnerabilities for their critical assets, with an initial estimation of the degree of danger, expected attacks, required security, and known countermeasures. Table 2 presents a list of the most common threats defined by ENISA [290] and an analysis of their possible occurrence for each of the twelve verticals presented

in Section II. Suppose the risk exists and is relevant for a given vertical. In that case, the symbol 'V' is inserted in the appropriate cell that intersects the row of the threat with the column corresponding to the vertical. When a given threat does not exist or has a negligible impact on a given sector, the symbol 'X' is inserted in the cell crossing the row of threat with the column corresponding to the vertical. When a given threat was not considered in the literature study of the characterized vertical, or there is insufficient information about its occurrence, the symbol '?' was inserted in the appropriate cell.

In some cases, in addition to the primary type of threat, the second column describes, in particular, the types/variants of threats for the verticals described in Section II. The last column presents a summary that includes the sum of the occurrences of individual threats versus all verticals and, analogically, the number of threats not considered for a given vertical. Having such information, we can notice which type of threats are most common for all verticals and then analyzes how they can be remedied with the help of 5G MEC. The compendium of knowledge on the security of 5G vertical industries presented in this Section will provide the basis for a deeper analysis of the proposed methods of protecting resources during the provision of services. However, before presenting such an analysis in Section IV, in the following Section III we will deal with the specific use cases of these twelve verticals and the role of the MEC technology in their practical implementation. It will allow us to indicate in further considerations how the MEC technology can affect the security of the 5G vertical industries against the principal security vulnerabilities identified in Section II.

III. COMPARISON OF PERFORMANCE AND SECURITY REQUIREMENTS FOR VERTICALS IN 5G MEC

A. 5G MEC PARAMETERS

The 5G has been proposed as a universal communication platform which is facing problems, both, of high increase of the scale of present networks and services (rapidly rising traffic, mostly due to video streaming, a growing number of connections with multiple devices of a single user, handling a huge number of IoT devices, often on a small area, etc.), and delivering significantly increased operational performance of newly proposed network use cases and new applications, which are classified into three main groups: enhanced Mobile Broadband, Ultra-Reliable and Low-Latency Communications, and Massive Machine Type communications. For the new IMT-2020 radio interface, the ITU formulated minimal performance requirements as limit values of network parameters [292]. Such values are, for instance:

- Latency: user plane 4 ms for eMBB, 1 ms for URLLC, control plane: 20 ms,
- Reliability: $1 - 10^{-5}$ success probability of transmitting a layer 2 PDU (protocol data unit) of 32 bytes within 1 ms,
- Peak data rate: Downlink 20 Gb/s, Uplink 10 Gb/s,
- Device Density: 1 000 000 devices per km^2,
- Capacity: eMBB 10 Mb/s/m^2.

The capabilities expected for IMT-2020 are much higher than those available in the 4th generation network IMT-Advanced. Moreover, the critical capabilities obtained by the present implementations of 5G networks are less than expected in [292].

Since vertical industries are specific applications of 5G (or 5G MEC), each vertical has minimal requirements for critical parameters' values related to its use cases. These parameters should describe the following aspects: 5G quality of access and transmission, MEC-based reinforcement of computation performance, and provided security level. For our analysis, we decided to use nine quality parameters characterizing the 5G MEC networks. Some of them are from the IMT-2020 suite [292], the others are proposed to reflect the MEC role in the network and security requirements. Later in this Section, we present these parameters (see Table 3) and how they characterize 5G MEC.

The choice of parameters is not random but directly related to the possibilities offered by MEC. The first parameter is latency. MEC creates an opportunity to reduce communication latency, making MEC a promising enabler for latency-critical 5G applications. The requirement for low-latency computing is increasing rapidly. It is a fundamental metric for network performance, especially for many emerging applications (e.g., VR/AR, interactive gaming, e-Health, and mission-critical controls). Naturally, the reliability of the services is related to the low latency in the network. The reliability describes the capability to transmit a given amount of traffic within defined time duration and computing/processing with a high success probability. This feature is essential for sectors such as Healthcare, Industrial Internet, or V2X. Availability is associated with reliability, representing access to data or service for authorized users whenever needed. Obviously, 100% availability is not possible, but some services are more resistant to unavailability. The proximity of services in the MEC and their type requires different data transmission. The peak data rate parameter is the fastest data transfer rate for a device available for a particular service. Moreover, the previously mentioned parameter depends on the device density. MEC allows us to connect multiple devices with adequate quality, so the number of devices connected to the network should be monitored. Peak data rate and device density are linked by the capacity defined as the number of connections at an average transmission level of 1 Mb/s estimated for typical service realization per $1km^2$. The following parameter is the isolation level. It specifies how much a given service must be isolated from the others. It is crucial in the context of services that use sensitive data (data from one slice cannot be accessed by another unless required by the proper functioning of the service) and much less critical for publicly available data. Another significant parameter from the MEC point of view is the trust in the MEC platform. It characterizes trust in MEC resources in the context of stored data (some services allow to delegate their data to the MEC environment) or security functions such as authentication, authorization, or

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 3. Selected 5G MEC quality parameters

Parameter	Unit	Description
Latency	ms	The parameter describes the duration between the moment when a particular packet was sent from the source node and its successful reception in the destination node
Reliability	% or 10^{-x}	As defined in [307] - *refers to the continuity in the time domain of correct service and is associated with a maximum latency requirement*. The latency requirement is a threshold for the Round Trip Time (RTT) or the One-way Trip Time (OTT) and times obtained while service proving must be below the threshold.
Peak data rate	Gb/s	The parameter describes high data rate provision during high traffic demand periods
Device Density	devices/m^2	The parameter describes average number of devices which are expected for typical service operation per 1 m^2. According to this parameter, it is possible to estimate possible number of resources which are needed to support functionalities offered by a vertical.
Capacity	Gb/s/km^2	The parameter can be interpreted as a number of connections at an average transmission level of 1 Gb/s estimated for typical service realization per 1 km^2. It can be calculated based on the Device Density parameter, where the sum of all transmissions generated by them are presented per 1 km^2.
Isolation level [293]	C/E/I/NE/N	Parameter describes how isolating an individual network slice affects the protection of the entire network; it takes values (from the most important to the least important): • *critical* [100-91%]: Slices with services must be isolated from the others. Getting traffic from another slice causes interference in the correct operation of services, in particular critical services. • *essential* [90-61%]: Slices with services should be isolated from the others. Getting traffic from another slice may cause interference in the correct operation of services. Such value is dedicated to uncritical services. • *important* [60-40%]: Slices with services should be isolated from the others. Getting traffic from another slice may cause interference in the correct operation of services, but services will work properly in most cases. • *non-essential* [39-11%]: Isolation between slices is not so important. Getting traffic from another slice may cause interference in the correct operation of services, but such interference is admissible. • *negligible* [10-0%]: Isolation between slices is negligible. Services without isolation will work or not, and good work or safety is not important.
Trust to the MEC platform	%	Parameter specifies service dependency on functionalities provided by MEC platform and can be described as: • *critical* [100-91%]: Service delegates to the MEC platform execution of most of its logic and essential operations like authentication, authorization, or store critical data. Without the MEC platform, or in case it is compromised, it cannot work properly. Even after the MEC system restoration, it needs to be rebuilt from scratch because all secrets or user accounts can still be compromised. • *essential* [90-61%]: Service delegates to the MEC platform most of the operations or stores essential data. Without the MEC platform, or in case it is compromised, it cannot work correctly. After the MEC system restoration, it can work in normal mode. • *important* [60-40%]: Service delegates to the MEC platform some of its operation logic or store important medium data. If compromising the MEC platform or data loss, the service can continue working in an emergency mode without part of its functionalities. • *non-essential* [39-11%]: Service delegates to the MEC platform non-crucial operations or store less important data. The MEC platform is used for service performance improvement or better user experience. In case of compromising the MEC platform or data loss, the service can work but with less performance. • *negligible* [10-0%]: Service does not delegate any functionalities to the MEC platform, and in consequence, it can work independently even if MEC platform is not working.
Edge Computing usage	%	Parameter describes the ability to handover calculations to the MEC servers. Absolute values might be described by *Floating Point Operations Per Second* (FLOPS) or *Million Instructions Per Second* (MIPS). Due to differences between CPU architectures used by mobile devices and servers FLOPS and MIPS values are not directly exchangeable between different architectures. This approach also does not include other time-consuming operations like memory or network access. Thus, we decided to define this parameter as *ratio of original processing time, which might be handled by the MEC server*.
Availability	% or 10^{-x}	Authors in the document [307] are defining two aspects of availability - related to *resilience* and *coverage*. The *resilience* meaning is connected with the level of disruption of the information process supported by the service when the network access is reduced. The coverage approach is similar to the reliability parameter - it shows the percentage of the selected area where Quality of Experience for a particular service is satisfied [307]. We will use the following levels: • *critical* [100-99.99%): the access to the network is required for the service, and outages of the network access have a crucial impact on the service. • *essential* [99.99-99.9%): the access to the network is required for the service, and outages of the network access have a significant impact on the service, which might be exceptionally tolerated. • *important* [99.9-99%): the access to the network is required for the service, and outages of the network access have a significant impact on the service, which might be tolerated. • *non-essential* [99-90%): the access to the network is required for the service, and outages of the network access are not impacting the service. • *negligible* [90-0%]: the access to the network is not required at all, might be unavailable for long periods, etc.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

traffic steering. The last selected parameter but not least, is Edge Computing usage. This parameter describes the ability to handover calculations to the MEC servers that can help in the excellent work of services. The selected parameters define the features that characterize the concept of the MEC network and are sufficient to compare the various services provided by it.

In Fig. 4 we present the scale values of the 5G MEC quality parameters defined above. In this section, we use these scales to present the properties of the 5G vertical industries and their use cases. For the latency (**LAT**), we use the inverted logarithmic scale of the range from 10 s to 1 ms. The three MEC and security parameters: Isolation level (**IL**), Trust to MEC (**TTM**) and Edge Computing Usage (**ECU**) are described in enumerative scale C/E/I/NE/N, from the negligible level to the critical level, with possible percentage for the more detailed description of each parameter within each enumerative level, if needed. Availability (**AVA**) and Reliability (**REL**) are described in the inverted logarithmic scale, ranged from $(100 - 10^{1})\% = 90\%$ to $100 - 10^{-7}\% = 99.9999999\%$ with the multiplier of 10^{-2}, representing the percentage of time of availability of the system or its reliable functioning, respectively. Peak data rate (**PDR**) is expressed in bits per second and presented in a logarithmic scale, ranged from 100 kb/s to 10 Gb/s, with the multiplier 10. Device Density (**DD**), expressed in $number of devices$/km^2 and Capacity (**CAP**), expressed in Gb/s/km^2, are represented in a logarithmic scale, ranged from 10^{-2} to 10^{6}, with the multiplier 10^{2}.

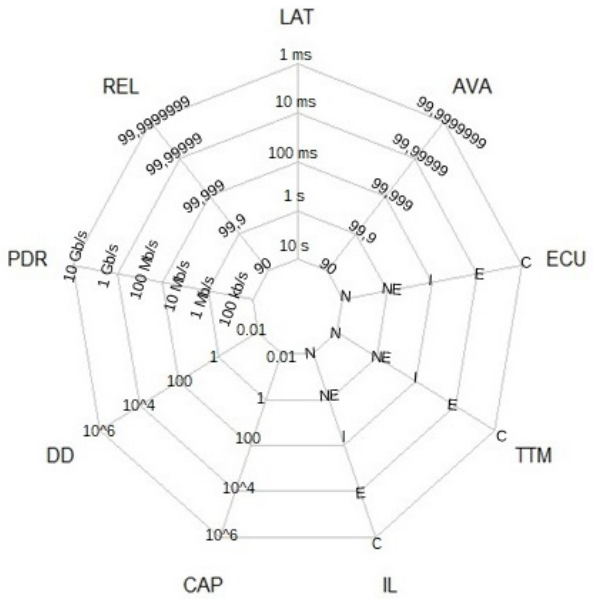

FIGURE 4. The scale values of the selected 5G MEC quality parameters.

In the following steps, we identify (using literature resources and experts' knowledge) their values for typical cases of the verticals considered in Section II and next present a representative area of the parameters' values for the whole vertical.

The crucial question could be: how the expected requirements concerning parameters change when 5G MEC is used instead of 5G alone.

- The edge server can cause that the traffic is reduced over the network since some data normally sent from the cloud service can be generated in the edge server. The response might be finally faster than in a cloud-based scenario.
- The edge server can cause the traffic from user devices (e.g., sensors) to be consolidated in the edge server and then sent to the cloud service as a compressed or aggregated stream.
- The edge server might get a response faster than the cloud server because it might be closer to the User Equipment.
- The edge server could cache requests and responses as a part of the Content Delivery Network, which will reduce the response time.

B. MEC FOR MANUFACTURING INDUSTRY

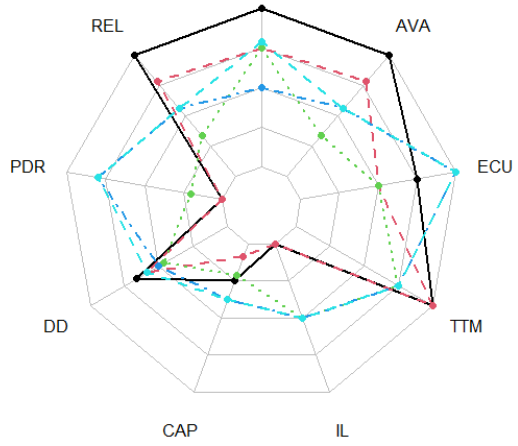

FIGURE 5. Requirements for use cases in the manufacturing industry ((1) black: Robotic control; (2) red: Automated guided vehicle; green: (3) Video surveillance; (4) blue: Quality check; (5) light blue: Augmented reality).

- *Robotic control*, especially robotic arms control, is an element of factory cell automation. It consists of sensors mounted over the arms or the automated production line connected to mechanical actuators. Such a system must be controlled in real-time, reliably, remotely, and often autonomously in order to achieve precise manipulation of the items that are automatically produced. Due to the high concentration of such items, it is considered as IoT URLLC 5G application. The MEC technology is suitable here to provide extremely high reliability and availability required for controlling particular production lines, nests, and multi-purpose robots. It can help provide high computational capacity for robots, particularly for supporting decision-making and adaptation of autonomous machines.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 4. Parameters for the manufacturing industry use cases in 5G MEC, according to [53]

PA	(1)	(2)	(3)	(4)	(5)
LAT	1 ms	10 ms	10 ms	100 ms	7 ms
REL	99.9999999	99.99999	99.9	99.999	99.999
PDR	0.1 Mb/s	0.1 Mb/s	1-5 Mb/s per camera	1 Gb/s	1 Gb/s
DD	2000/km^2	500/km^2	50/km^2	100/km^2	500/km^2
CAP	1 Gb/s/km^2	0.05 Gb/s/km^2	0.5 Gb/s/km^2	10 Gb/s/km^2	10 Gb/s/km^2
IL	NE	NE	I	I	I
TTM	C	C	E	E	E
ECU	E	I	I	C	C
AVA	99.9999999	99.99999	99.9	99.999	99.999

- *Automated guided vehicles* are used to transport materials and components within a factory and on the way parts warehouse - factory - finished products warehouse. They must be integrated with other production elements to assure business continuity and optimize different aspects of logistic. Thus, they belong to the class of URLLC applications. MEC technology could be useful here to relieve the main communication and computing system and provide physical (communication) security for both humans and vehicles.
- *Video-surveillance* is used for security of production infrastructure, personal safety of humans, and safety of working machines. The main new application provides pictures for precise control of autonomous devices, applications using pattern recognition, and industrial access control. These new applications require high bandwidth, traffic, and connection density, with relatively low latency, so the video-surveillance can be considered a URLLC service category. In this case, the modern applications of video-surveillance can be delegated to MEC applications to improve latency parameters, relieve a communication network and increase the security of locally performed manufacturing processes.
- *Quality check* is a remote new solution of the manufacturing industry. It can be applied at any stage of production, for semi-finished and finished products, using high-resolution images, also those obtained by sophisticated tomography techniques. As in the video-surveillance use case, the quality check needs high bandwidth and high other communication parameters with the support of MEC technology as a URLLC solution. Suppose we also include permanent monitoring of finished products, which is important for some devices and applications. In that case, the quality check will require URLLC performance and MEC-based support to handle locally grouped devices.
- *Augmented reality* is the main component of the manufacturing industry characterizing its 4th generation. It is suitable at any production stage: from concept incubation, designing, and prototyping phase, through manufacturing and testing, to marketing, exploiting, and recycling. Among products involved in the augmented reality, wearables as components of other products or independent devices are the most important category. This use case needs high availability, fast response, strong security, and high reliability. Moreover, augmented reality components need energy efficiency, high bandwidth for video transmission with low jitter, which are the expected properties of the URLLC service category. In such a case, the MEC technology could increase or reduce global data transmission, improve network quality parameters, and provide additional computational resources and security solutions supporting weak wearables' resources.

The properties of Manufacturing industry use cases are given in Table 4 and presented graphically in Fig. 5.

C. MEC FOR FINANCIAL SECTOR

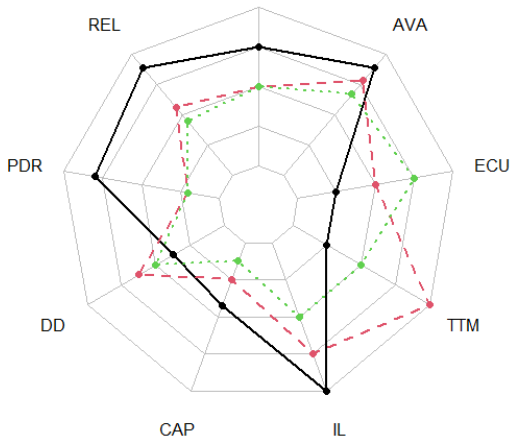

FIGURE 6. Requirements for use cases in the financial sector ((1) black: IB; (2) red: M2B; (3) green: M2I).

This sector unifies subjects and objects of completely different ranges of responsibility, level of risk, and self-protecting abilities into a mesh of interdependent stakeholders expecting reliable and secure services. To present expected functional requirements of the financial sector and a role of the support by MEC technology, we propose three use cases representing typical BFSI activities.

- *InterBank (IB)*: Traditional banks with a head office and bank branches belong to the past. Now a bank (and with some respect, other banks) work as a single centralized enterprise with instant and secure access to all resources and services. Therefore, IB communication must be efficient, reliable, and secure. Such requirements locate IB communication in URLLC 5G service category, with relatively low latency and high data transmission vol-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 5. Parameters for the financial sector use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	10 ms	100 ms	100 ms
REL	99.999999	99.999	99.99
PDR	1 Gb/s	1 Mb/s	1 Mb/s
DD	10/km^2	1000/km^2	100/km^2
CAP	25 Gb/s/km^2	1 Gb/s/km^2	0.1 Gb/s/km^2
IL	C	E	I
TTM	NE	C	I
ECU	NE	I	E
AVA	99.999999	99.99999	99.9999

ume. Strong integration of bank servers marginalizes the MEC role, or even the presence of additional edge servers could increase access latency and decrease data transmission rate. Due to security requirements, the isolation level of data links must be very strong.

- *Mobile-to-Bank (M2B)*: This type of communication carries out financial transactions of clients ordered to the bank from mobile devices or private workstations, supports card payments in Points of Sale, [295] and gives bank customers access to their accounts. Thus, it is a use case of an eMBB communication network. Required connection quality parameters can be more liberal than those for IB, but the MEC technology support is recommended here. MEC-based services can improve the quality of service for users' transactions, increase the security of off-line transactions [296] and provide end users' low computing devices with extra security services.
- *Mobile-to-Insurance (M2I)*: It is, like M2B, the eMBB communication network but with a lower risk of individual transactions and lower requirements on 5G performance parameters. In such a case, the MEC server can be an essential part of a service to reduce the network load with data transmission and links occupation and, as it was for M2B, to increase the end user security. For insurance-associated eSafety services, e.g., eCall, the automobile emergency calling service [297], [298], the MEC host can be a local safety management center monitoring mobile customers and initiating emergency services, if required.

The properties of Financial sector use cases are given in Table 5 and presented graphically in Fig. 6.

D. MEC FOR THE HEALTHCARE SECTOR

- *Remote monitoring of health or wellness data through wireless devices*: By using IoT devices, healthcare providers can monitor patients and collect data that can be used to improve personalized and preventive care. Due to this, it is possible to decide on behalf of doctors and perform the patients' decision. When rapid action is required, such an approach can have a dramatic impact on the probability and time of patients' recovery. This use case requires continuous access to patient sensors, service availability, and proper management of the received data.
- *Smarter medication*: The decision for treatment could be made not only based on monitoring from the patient's body conditions but also considering various high-risk factors (e.g., air pollution, temperature, etc.). Moreover, new devices connected to the network for automatic drug dosing could be used to treat Asthma, Diabetes, and Multiple Sclerosis and manage chronic diseases and pains in general. For this purpose, it is necessary to provide services of low latency, high availability, and reliability.
- *Wireless tele-surgery*: Remote surgery involves the transmission of medical information. Medical information, such as images, audio, and video, is digitized and transmitted via a medium (wired or wireless) of telecommunication networks. Surgeons can use the surgical robot to perform operations over a long distance

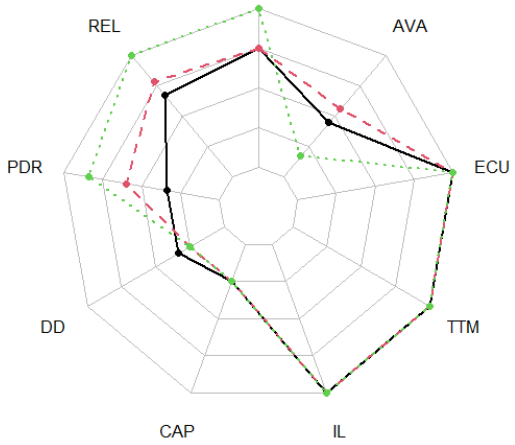

FIGURE 7. Requirements for use cases in healthcare ((1) black: Health monitoring; (2) red: Smarter medication; (3) green: Robotics).

TABLE 6. Parameters for the healthcare use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	10 ms	10 ms	1 ms
REL	99.9999	99.99999	99.9999999
PDR	5 Mb/s	100 Mb/s	1600 Mb/s
DD	5 /km^2	1 /km^2	1 /km^2
CAP	1 Gb/s/km^2	1 Gb/s/km^2	1 Gb/s/km^2
IL	C	C	C
TTM	C	C	C
ECU	C	C	C
AVA	99.99	99.999	95

through the networks. For telemedicine to be real, it is required to provide services with ultra-low latency and reliability.

- *Assets tracking and management in Hospitals*: Assets tracking and management refers to Hospitals have to manage their assets as they are limited goods and can be located in different parts of the hospital. Therefore, from the hospitals' point of view, it is necessary to prevent their high-value assets, for example, wheelchairs, ECG (electrocardiogram) monitors, infusion pumps, etc., from being removed from the hospital (not always with bad intention). To achieve such a use case, it requires access to the data and proper management of them (which includes security such as data encryption, too).

The properties of the Healthcare sector use cases are given in Table 6 and presented graphically in Fig. 7.

E. MEC FOR THE RETAIL SECTOR

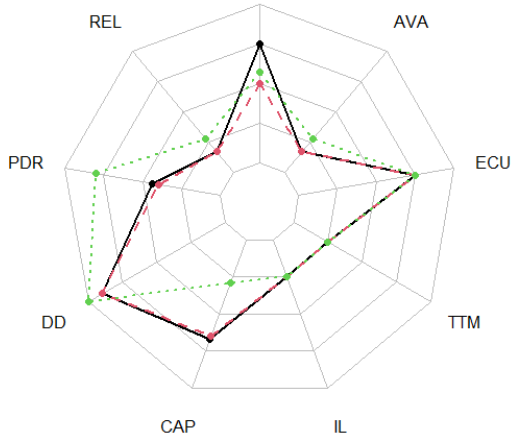

FIGURE 8. Requirements for use cases in retail ((1) black: Stationary shops (video content streaming); (2) red: Smart bags; (3) green: On-site live events).

TABLE 7. Parameters for the retail sector use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	10 ms [303]	100 ms	50 ms [80]
REL	95 (basic)	95 (basic)	99.5 [80]
PDR	15 Mb/s [303]	10 Mb/s	1000 Mb/s [80]
DD	150 000 / km^2 [303]	150 000 / km^2	1 000 000 / km^2 [80]
CAP	2250 Gb/s/km^2	1500 Gb/s/km^2	2 Gb/s/km^2 (2000 m^2 store) [80]
IL	NE	NE	NE
TTM	NE	NE	NE
ECU	E	E	E
AVA	95	95	99.5

Customers visiting stores and shops might use different devices to access services helpful in the sales process. It includes customers' devices like smartphones, tablets, smartwatches or bands, shared public devices like touchable screens, or retailers' devices. Customers might use services in the product searching process, ordering process, or customization process. MEC and edge servers might provide accurate information about available products, even in other stores, and support the item reservation process. Another branch of scenarios is to provide audio-video content with the highest quality and supported by Augmented Reality / Virtual Reality (AR / VR) solutions. In this vertical, we are considering the following main use cases.

- *Stationary shops (video content streaming)* - customers would like to see additional content related to some items and services. It applies to a wide range of places, including supermarkets with hundreds of customers in a single shop. The most crucial from a User Experience (UX) point of view is to obtain the content without recognizable latency and with acceptable quality. This use case is a mix of use cases described in [303] as *user generated content*, *immersive media*, and *new distribution technologies*.
- *Smart bags* - customers are using bags for collecting items. This process could be supported by an intelligent bag that counts the current value of products, locates missing objects, and suggests other products.
- *On-site live events* - retailers might arrange events and meetings in their shops supported by MEC services. Services might combine data streams from multiple points in a particular shop, e.g., actual views from drones, IoT sensors, and devices. It includes scenarios like streaming town halls or small concerts to the Internet and other screens located near the place where the event appears. This use case is described in [303] as *Cooperative/off-site media production*.

The properties of the Retail sector use cases are given in Table 7 and presented graphically in Fig. 8.

F. MEC FOR TELECOMMUNICATIONS

The Telecommunications sector situation is different from in other verticals because parameters for use cases are almost the same for all business models presented in Section II (MVNE, Light MVNO, Full MVNO). It is caused by very similar types of services in this domain - mainly based on providing resources from virtual infrastructure. The differences are in the number of available network elements and their functionalities, but this does not impact network requirements - they are still very high. One thing which differentiates Telecommunications use cases is MEC usage. Not all business use cases will need it on the same level. MEC for Operator will be used to extend the portfolio of available services and many more:

- Closing network traffic at the edgeless data will be sent to the core network.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

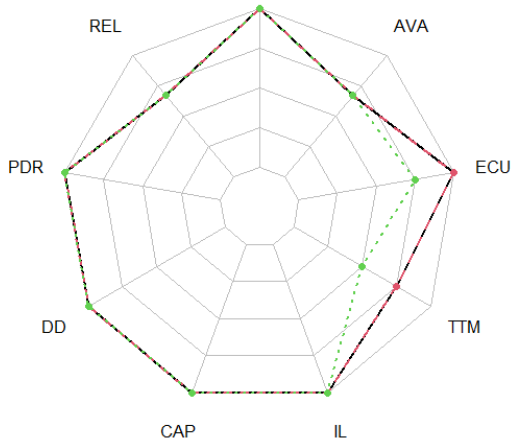

FIGURE 9. Requirements for use cases in telecommunications ((1) black: MVNE; (2) red: Full MVNO; (3) green: Light MVNO).

TABLE 8. Parameters for the telecommunications use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	1 ms [154]	1 ms [154]	1 ms [154]
REL	99.9999 [140], [155]	99.9999 [140], [155]	99.9999 [140], [155]
PDR	10 Gb/s [154]	10 Gb/s [154]	10 Gb/s [154]
DD	1000000/km^2 [140]	1000000/km^2 [140]	1000000/km^2 [140]
CAP	1000000 Gb/s/km^2 [155]	1000000 Gb/s/km^2 [155]	100000 Gb/s/km^2 [155]
IL	C	C	C
TTM	E	E	I
ECU	C	C	E
AVA	99.9999 [155]	99.9999 [155]	99.9999 [155]

- Fast and dynamic implementation of needed network services at the edge resolves the issue of lacking access infrastructure.
- Fast and dynamic implementation of new own or third-party services at the edge, which extends operator portfolio, e.g., improved caching.
- Providing new customer-oriented services that reflect the customer service requirements of each user [125].
- Improvement of network performance and the same time higher QoE.

Therefore, some virtual operators like Light MVNO will not care about MEC usage for resource utilization or network service improvement because they receive it from a lower-level operator and sell only new services based on that. In the case of low-level Operators like Full MVNO, usage of MEC will be more important because it helps improve QoS. Parameters for defined types of Virtual Operators in the Telecommunications sector are shown in Table 8 and presented graphically in Fig. 9.

G. MEC FOR AUTHORITIES

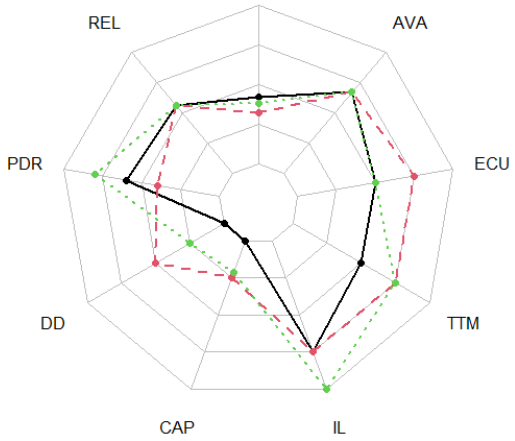

FIGURE 10. Requirements for use cases for authorities ((1) black: A2B; (2) red: A2C; (3) green: A2A).

TABLE 9. Parameters for the authorities use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	200 ms	500 ms	300 ms
REL	99.999 [180]	99.999 [180]	99.999 [180]
PDR	100 Mb/s [180]	10 Mb/s [180]	1 Gb/s [180]
DD	0.1/km^2	100/km^2	1/km^2
CAP	0.1 Gb/s/km^2 [180]	1 Gb/s/km^2 [180]	0.5 Gb/s/km^2 [180]
IL	E	E	C
TTM	I	E	E
ECU	I	E	I
AVA	99.9999 [181]	99.9999 [181]	99.9999 [181]

The Authorities sector use cases can be grouped into three main service model scenarios - Authority-to-Authority (A2A), Authority-to-Business (A2B), and Authority-to-Customer (A2C). Services classified to the same group have similar operation logic. Therefore their needs can be represented by the common average parameters presented in the Table 9 and presented graphically in Fig. 10:

- *Authority-to-Customer* - this group represents all use cases where Authority service, for example, e-Government is exposed to the Customers for the realization of some public operations like online transaction services or distribution of some public data sets through API. In this model, the same service is dedicated to many customers and shares both public and confidential data with them.
- *Authority-to-Business* - this group represents all use cases where Authority services are exposed to the Businesses Partners to realize some common operations like financial entities, IT support, or even emergency

systems. This type of service is mainly used for internal communication and exchange mostly confidential data.

- *Authority-to-Authority* - this group represents all use cases where Authority services need to use other Authority services, for example, some internal synchronization between different entities or backups.

MEC for Authority can be mainly used for some quick decision-making and facilitation of some simple administration. For example, according to Gartner (2018), every 60 seconds in the USA, more than 80,000 records of information are sent to the department's computers on winter days. All this data should be analyzed to deal with snow on roads. Edge Computing servers can analyze such data, and therefore, they do not have to be sent to the central department. Such data processing can be very easily adopted from central computers to the MEC, which will release bandwidth and cause a decentralization of management.

Another example of usage of MEC infrastructure for all mentioned categories of Authority sector can be an implementation of AI algorithms for checking forms before sending them to the central department. It is very important at the end of the period of some declaration as in such a situation many documents are sent to one central office at the same time. Using Edge Computing, it is possible to distribute such a request into many computing locations.

Similar use case connected with computing distribution can be an implementation of governments avatars in the secured MEC resources. Such avatars can very quickly give advice or help with some e-administration problems. In this scenario, all confidential data will be processed on certified resources located near the customer, and there will be no need to send it outside the region or state.

H. MEC FOR MEDIA AND ENTERTAINMENT

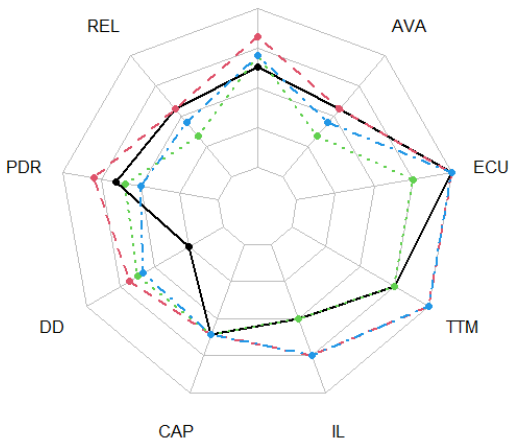

FIGURE 11. Requirements for use cases in media and entertainment ((1) black: Ultra High-Fidelity Media; (2) red: On-site Live Event Experience; (3) green: User & Machine Generated Content; (4) blue: Immersive and Integrated Media and Gaming).

Media and Entertainment services need to deal with increasing need in the context of data rates, the number of simultaneous users connected, and/or higher Quality of Service requirements. High-quality and high-resolution audio-visual services are important in terms of increasing downlink data rates, where 5G MEC promises to provide cost-effective alternatives to today's Content Delivery Network approaches. Below, a list of most popular use cases in Media and Entertainment can be found (based on [183]):

- *Ultra High-Fidelity Media*: The continuous increase in technology means that users require the reception of media in high-quality images and sound on their devices. Both linear (e.g., live streaming) and non-linear (on-demand) content will need to provide Ultra High-Fidelity Media experience. 5G MEC network needs to support proper network management and achieve high-speed transport capabilities to guarantee the high quality of Ultra High-Fidelity Media experience(e.g., local and network content caching).
- *On-site Live Event Experience*: Big entertainment events in stadiums, cinemas, or concerts are increasingly connected to provide a better user experience with replay, choice of a specific camera, language, etc.
- *User & Machine Generated Content*: Undoubtedly, we observe a constant increase in the content created by users and machines, which go to the computational cloud. These contents are then shared with other users and machines. It means that the 5G MEC must support on-demand high uplink bandwidth and streaming from different devices.
- *Immersive and Integrated Media and Gaming*: The created games more and more resemble the world around us, providing users with more and more realism. Thus, it is possible to improve the ability of users to collaborate in the game and no limitation on the number of simultaneous users.

TABLE 10. Parameters for the media and entertainment use cases in 5G MEC

PA	(1)	(2)	(3)	(4)
LAT	30 ms	5 ms	15	15 ms
REL	99.999	99.999	99.9	99.99
PDR	200 Mb/s	1000 Mb/s	100 Mb/s	30 Mb/s
DD	1 /km^2	3000 /km^2	1000 /km^2	500 /km^2
CAP	750 Gb/s/km^2	750 Gb/s/km^2	750 Gb/s/km^2	750 Gb/s/km^2
IL	I	E	I	E
TTM	E	C	E	C
ECU	C	C	E	C
AVA	99.999	99.999	99.9	99.99

The properties of the Media and Entertainment sector use cases are given in Table 10 and presented graphically in Fig.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

11.

I. MEC FOR THE SMART CITY

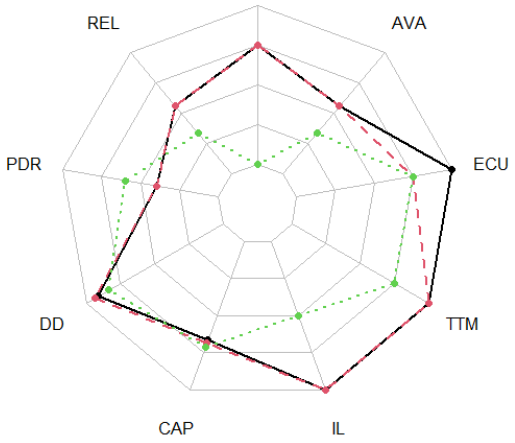

FIGURE 12. Requirements for use cases in the smart smart city ((1) black: Smart grid; (2) red: Emergency situation management; (3) green: City surveillance).

TABLE 11. Parameters for the smart city use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	10 ms [216]	10 ms [3]	na
REL	99.999 [216]	99.999 [3]	99.9
PDR	10 Mb/s	10 Mb/s [3]	100 Mb/s [209]
DD	200 000/km^2	300 000/km^2 [3]	50 000/km^2 (1 CCTV camera per 20 m^2)
CAP	2000 Gb/s/km^2	3000 Gb/s/km^2	5000 Gb/s/km^2
IL	C [216]	C [3], [4]	I
TTM	C	C	E
ECU	C	E [3] [4]	E
AVA	99.999	99.999 [3]	99.9 [209]

We will focus on the following use cases that are the most promising for 5G MEC.

- *Smart Grid* - this concept consists of many scenarios and implementations, see [217], but we will focus on the basics. The document [216] defines four scenarios: intelligent distributed feeder automation, millisecond-level precise load control, information acquisition from low voltage distribution systems, and Distributed Energy Resources (DER). The first two scenarios are covering the problem of providing power continuously. The third scenario focuses on power grid monitoring and has different requirements than other mentioned scenarios. The last scenario touches on power generators which might support daily power management and might be popular in the medium-range future. MEC environment might support those scenarios by providing computation power for data acquisition and analysis for a distributed set of meters. It might provide a forecast for power consumption based on the information about the location of users, their typical habits, or current service requests handled in MEC services.
- *Emergency situation management* - in this case, various persons and devices might be interested in obtaining recent information and instructions on how to survive the critical situation - called in [217] 5G+ smart governance. The MEC service could manage and orchestrate the process of evacuation, recovery after a disaster, terrorist attack, or electricity blackouts. This case might use IoT devices, sensors, automated parts of a building like doors, gates, ventilation, water sprinklers, etc. Those mechanisms might be used for planned situations like football matches with thousands of fans. The good examples of disaster management are described in [218], e.g., intelligent forest fire detection or autonomous car accident reporting.
- *City surveillance* - this use case includes obtaining audio-video streams from Closed Circuit Television (CCTV) systems supported by IoT devices with own cameras, microphones, motion sensors, etc. The traffic from various sources should be processed and analyzed without significant delay. Devices do not have sufficient computation resources to do near real-time image and video processing, so the MEC server might be used to provide computation services. It might correlate results from various sources to improve decision credibility. The service should be deployed with High Availability (HA) approach and strongly isolated from other data streams due to processed sensitive content and possible integrations with other services like alarms, evacuation calls, terrorist attack prevention, etc. The paper [217] describes related use cases like 5G UAV, smart security, 5G patrolling robots, or 5G AR mobile policing.

The properties of the Smart City use cases are given in Table 11 and presented graphically in Fig. 12.

J. MEC FOR AGRICULTURE

In the Agriculture sector's realization, there are many IoT sensors, devices, remote vehicles, and even robots. Therefore it is not easy to define common needs for all components of this vertical. For this reason, for better representation of the Agriculture domain, it was divided into four groups.

- *Group 1* - represents all simple devices used mainly to send small-size data, including basic parameters from sensors. Usually, this type of device does not need to confirm data transfer or high up-link throughput, and information is sent not very often. Examples of such groups can be systems for pest control, irrigation, fertilization, air and soil temperature sensors.
- *Group 2* - represents all devices that sent data with similar frequencies like group 1 but with higher data size. They are more vulnerable to lack of connectivity,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

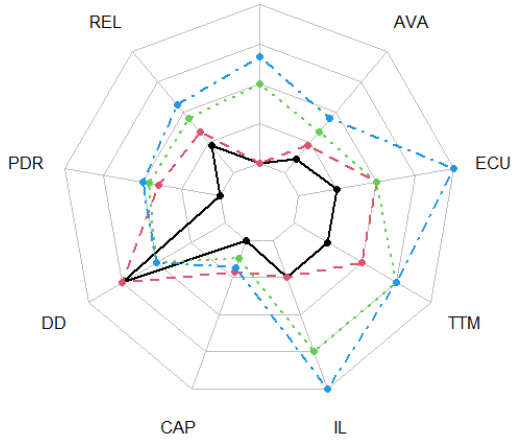

FIGURE 13. Requirements for use cases in the agriculture and food industry ((1) black: Group 1 - Pest control, Irrigation, Fertilization, Air and Soil temperature sensors; (2) red: Group 2 - Still picture camera, Animal monitoring, Multi or hyper spectral camera, Acoustic sensors; (3) green: Group 3 - video streaming cameras, Smart vehicles; (4) blue: Group 4 - Drones, Remote control, Agribots).

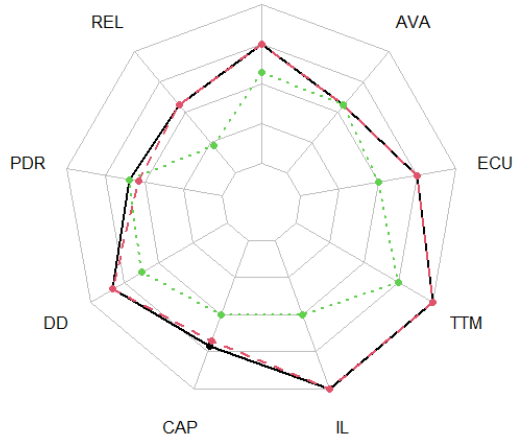

FIGURE 14. Requirements for use cases in logistics ((1) black: V2X communication; (2) red: Automated vehicles; (3) green: Automated logistics).

TABLE 12. Parameters for the agriculture and food industry use cases in 5G MEC

PA	(1)	(2)	(3)	(4)
LAT	60s [220], [223]	10s [220]	100ms [220], [234]	20ms [241]
REL	99	99.9	99.99	99.999
PDR	0.8 kb/s [220], [223]	10 Mb/s [220]	20 Mb/s [220], [234]	30 Mb/s [242]
DD	10000/km^2 [309]	10000/km^2	100/km^2	100/km^2
CAP	0.8 Mb/s/km^2 [309]	0.5 Gb/s/km^2	0.1 Gb/s/km^2	0.3 Gb/s/km^2
IL	NE	NE	E	C
TTM	NE	I	E	E
ECU	NE	I	I	C
AVA	90	99	99.9	99.99

but it is not critical for them. Examples of systems that include devices belonging to this group can be animal monitoring, still picture camera, multi or hyperspectral camera, acoustic sensors.

- *Group 3* - represents more advanced Agriculture devices that need lower latency than previous groups in case of some reaction features. They are still not requiring huge data transfer, but lack of connectivity will block their operation. Examples of devices selected for this group can be real-time cameras, smart vehicles, or services based on video streaming.
- *Group 4* - represent the most advanced devices with very high requirements for both data transmission and latency. The operation of this type of device is strongly dependent on network parameters and is sensitive to their changes. Examples of devices in this group can be drones, agribots, or all remotely controlled machines.

Additionally, for all four groups, MEC can be used for data selection and advanced analysis to select data for transfer to the cloud and, therefore, eliminate irrelevant data from the system. As a result, this can decrease the cost of cloud usage (bandwidth, storage, and requests). Having the opportunity to analyze data in the edge allows for immediate feedback from systems that process them and decide on some control mechanism, such as irrigation systems. Of course, in this case, the usage of MEC can be similar to typical cloud computing like Big Data analyzes or historical comparison.

For more advanced use cases (presented in the 3 and 4 groups) like UAVs and Agribots, MEC for Agriculture is needed for ensuring low latency steering services. Such objects can move very fast, so video analysis and decisions should be sent without high delays.

Last use case, which is worth mentioning in this Section, is MEC usage for security improvement. As it is well known, IoT devices dedicated to farms should be cheap and straightforward. Therefore their protection is sometimes on a very low level. For this reason, MEC architecture allows extending the security of sensors by providing additional protection in the form of virtual firewalls, scanners, and other security applications close to them - at the edge of the network.

Parameters for all groups are given in the Table 12 and presented graphically in Fig. 13.

K. MEC FOR THE LOGISTICS

In the Logistics vertical we are aiming mainly to things related to automotive and mobility. It includes air vehicles like drones what are very popular last time and might easily adapt some of automotive solutions.

- *V2X communication* - vehicles used in a supply chain might communicate with other objects. From MEC per-

TABLE 13. Parameters for the logistics use cases in 5G MEC

PA	(1)	(2)	(3)
LAT	10 ms [31]	10 ms [205]	50 ms [307]
REL	99.999 [205]	99.999 [205], [303]	99 [307]
PDR	100 Mb/s [307]	50 Mb/s [205]	100 Mb/s [307]
DD	up to 50 000/km^2 (cars in traffic jam, drones); more than 10 000/km^2 [303]	up to 50 000/km^2 (cars in traffic jam, drones); more than 10 000/km^2 [303]	< 1000/km^2 [307]
CAP	5000 Gb/s/km^2	2500 Gb/s/km^2	100 Gb/s/km^2
IL	C [300]	C [300]	I
TTM	C	C	E
ECU	E	E	I
AVA	99.999 [300], [307]	99.999 [300]	99.999 [307]

spective most interesting are scenarios where computing power or broad knowledge about road traffic and transportation situation available via the MEC service are used. It includes scenarios like Bird's Eye View, Vulnerable Road User discovery, or cooperative driving like cooperative collision avoidance [205]. This covers various types of communication, especially Vehicle-to-Network (V2N), Vehicle-to-Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), and V2V [294].

- *Automated vehicles* - vehicles used in logistics might become autonomous and self-driving. This use case contains scenarios like Cooperative Awareness, Cooperative Sensing, Cooperative Maneuvering [204]. The MEC application might be used as a robust third-party for data exchange and decision-making center.
- *Automated logistics* - logistics operations in port environment might be done by robots. The MEC application might control them, orchestrate the whole logistics process in the port, and provide computation power for robot's supporting solutions like image recognition for real-time video processing in autonomous manipulation of items and robot's position.

The properties of logistics use cases are given in Table 13 and presented graphically in Fig. 14.

L. MEC FOR EDUCATION, CULTURE AND SCIENCE SECTORS

When it comes to the 5G MEC, there are already plenty of applications in manufacturing, media, city management, and healthcare that will use network resources to ensure the high quality of services. Education is just scratching the surface of what is possible in the classroom. Here is what teachers and educators can expect:

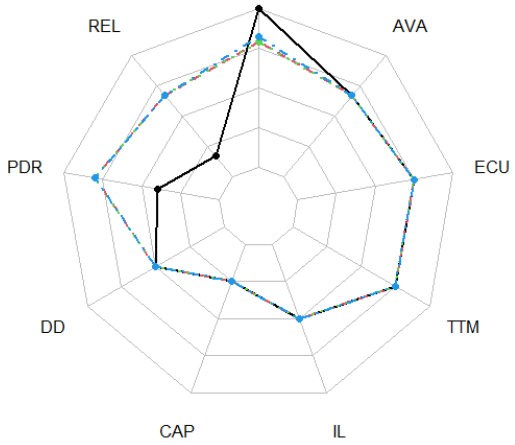

FIGURE 15. Requirements for use cases in education, culture and science ((1) black: Tactile Internet & Skillset communication; (2) red: Personalized learning; (3) green: IoT & Smart Classroom; (4) blue: VR-AR & education).

TABLE 14. Parameters for the education and culture science use cases in 5G MEC

PA	(1)	(2)	(3)	(4)
LAT	1 ms	7 ms	7 ms	5 ms
REL	95	99.9999	99.9999	99.9999
PDR	10 Mb/s	1000 Mb/s	1000 Mb/s	1000 Mb/s
DD	100 /km^2	100 /km^2	100 /km^2	100 /km^2
CAP	1 Gb/s/km^2	1 Gb/s/km^2	1 Gb/s/km^2	1 Gb/s/km^2
IL	1	1	1	1
TTM	E	E	E	E
ECU	E	E	E	E
AVA	99.9999	99.9999	99.9999	99.9999

- *Tactile Internet & Skillset communication*: Using fast and reliable data transport in the 5G MEC network, it will be possible to send tactile communication via the Internet. It will create new possibilities in Tele-teaching and Tele-mentoring, especially for manual training and skill development. The teacher will feel the learner's movement when she/he undertakes a task involving fine motor skills and correct her/him as necessary. The learner will be able to see, hear, and feel the exact movements their trainer has made, be they an engineer, pilot, or surgeon.
- *VR/AR & education*: Mixed-reality content and video require high bandwidth and low latency to perform optimally. 4G struggles to maintain the traffic required for AR and VR experiences. However, with 5G, especially 5G MEC, experiences will be seamless. Students may tour the human body or visit other planets in VR. With AR, they can explore concepts through touch, pinching, and zooming through the Earth's layers as fast as they think it.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

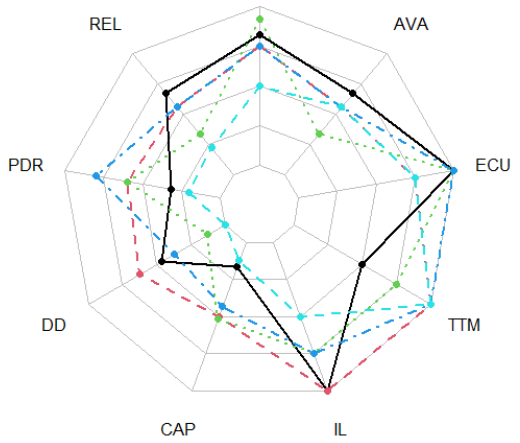

FIGURE 16. Requirements for use cases in critical infrastructure sectors ((1) black: Critical support services; (2) red: Critical communication (emergency); (3) green: High-speed wireless access; (4) blue: UHD Broadcasting; (5) light blue: Public Safety Services).

- *Walled-off, smart classroom*: Setting up devices and gathering feedback in class takes time, even when everything works perfectly. With the IoT on 5G MEC, teachers can automatically log in as soon as they enter the classroom. Menial administrative tasks will be automated, and students can deliver feedback digitally. Higher bandwidth will help signals remain strong throughout entire lectures and presentations, preventing occasional dropped connections and derailing focus.
- *Personalized learning*: Each student's learning style and ability is different. 5G MEC will help students continue their education outside the classroom, delivering the same data speeds and responsiveness in the classroom to their phones or laptops. Regardless of distance or location, 5G MEC empowers students to access the same information and exercises as their peers. Moreover, personal access to a mobile device enables to connect each learner into intelligent individualized systems that can suggest learning pathways, enable an aggregated analysis of student progress, or much better decision-making about all aspects of a students' education.

The properties of the Education, culture, and science use cases are given in Table 14 and presented graphically in Fig. 15.

M. MEC FOR CRITICAL INFRASTRUCTURE SECTORS

Critical infrastructure unifies, in fact, several use cases of different vertical industries sectors. As it was already presented in Section II-M, it is crucial for public safety and security, especially in natural hazards, disasters, social unrest, and other dangerous phenomena on a large scale. Therefore, the use of MEC technology requires strong protection of communication and data processing infrastructure on the one hand and enhances the opportunity of business continuity and disaster recovery on the other hand. To present different communication parameters requirements and possible support by MEC technology, we give five examples of the critical infrastructure vertical use case.

TABLE 15. Parameters for the critical infrastructure sectors use cases in 5G MEC, according to [53]

PA	(1)	(2)	(3)	(4)	(5)
LAT	5 ms	10 ms	2 ms	10 ms	100 ms
REL	99.9999	99.999	99.9	99.999	99
PDR	4 Mb/s	100 Mb/s	100 Mb/s	1 - 10 Gb/s	1 Mb/s
DD	50/km^2	1000/km^2	0.1	10/km^2	0.01
CAP	0.2 Gb/s/km^2	100 Gb/s/km^2	135 Gb/s/bowl	30 Gb/s/km^2	0.1 Gb/s/km^2
IL	C	C	E	E	I
TTM	I	C	E	C	C
ECU	C	E	C	C	E
AVA	99.9999	99.999	99.9	99.999	99.999

- *Critical support services*: Such a use case requires high capacity, bidirectional data communications, including automatic control signaling, often with additional requirements, like high precision location, high speed of communicating devices, with high security, reliability, and availability. MEC technology can help to satisfy these conditions, improving low latency requirements.
- *Critical communication (emergency)*: Such services require very short network traversal time, which is typical for URLLC networks. It should support compatibility with industrial automation communication, support for drone control, new medical applications, and wearables [289]. The MEC technology could support emergency services in crowded places or places with a high concentration of communicating devices (users, sensors, actuators). It can be suitable for disaster recovery in case of an incident like a fire, terrorist attack, earthquake, flood, etc.
- *High-speed wireless access*: This use case corresponds to situations with high variation of traffic/services requirements due to seasonality or unexpected events. It ranges from typical requirements of everyday stable usage to extreme hot spot-like requirements (requiring the eMBB network parameters) during the events, incidents, actions, etc. In such a case, the MEC technology can reduce network infrastructure costs in delivering services in critical places and moments.
- *UHD Broadcasting*: This use case enables transmissions supporting Virtual Reality-based services or visualization of emergency actions to local authorities in a large area. Such services are bandwidth and processing-intensive with high requirements on latency, so MEC technology can both increase network performance and localize contents distribution into cells according to dynamically changing situation.

- *Public Safety Services*: It requires a resilient network with high availability that can provide reliable communication even in the event of the destruction of part of the network because of failure or accident. Minimal communication services such as voice and text messages must be available even after a disaster. The energy consumption of both terminals and network infrastructure must be reduced. The MEC infrastructure can be suitable here to recover network functions in case of a breakdown or restore stopped safety services in another host.

The properties of Critical Infrastructure Sectors use cases are given in Table 15 and presented graphically in Fig. 16.

N. SUMMARY FOR 5G MEC VERTICALS

5G MEC is an example of fulfilling known technical requirements for low latency, high security, and high reliability and open new business opportunities enabling new services that are not possible with traditional network architecture. Vertical industries, cloud providers, and operators consider edge computing as the source of benefits related with:

- new use cases for real-time operations thanks to low latency,
- new business cases, related with services that benefit, for example from edge analytics,
- better bandwidth efficiency thanks to fewer data streams pushed through the network,
- data privacy and security with defined parameters for sensitive data processing,
- regulatory compliance related with data privacy and sovereignty.

Planning evolution of the 5G-based services to edge certain model drawbacks of MEC solution must be considered, for instance:

- initial costs for roll-out,
- need for the development of new business and operational models,
- the need to address responsibility and liability aspects in the new service chain,
- the need to ensure the physical security of MEC locations,
- fewer computing resources than in the cloud.

In this Section, the benefits and drawbacks of applying MEC technology for 5G vertical industries have been specified in more detail. The summary of our studies is presented in Table 16.

IV. IMPACT OF THREATS ON 5G MEC VERTICALS AND THEIR PARAMETERS

Analyzing risks in the verticals presented in Sections II and III and, at the same time, have a shared vision of its categorization, this Section includes a summary of threats that are present in all considered verticals. We followed a two-step approach to get a concise overview of all threats in the verticals of the 5G MEC network. First, we assessed the impact of the main threats on the quality parameters of the 5G MEC network. Then, considering the use cases of verticals discussed in Section III, we assessed the level of sensitivity of verticals depending on the 5G MEC parameters and their vulnerability to attacks. The results of our analysis are presented below.

Our analysis of threats to vertical industries done in Section II shows that many industries are vulnerable to attacks from the Internet. The following groups of attacks (see Table 2) are the most dangerous here:

- Malware,
- Denial of Service,
- Botnet,
- Insider Threat,
- Physical manipulation damage/theft/loss.

It is easy to understand why such attacks have the most destructive impact on the verticals. For instance, malware is a large group of intrusive software easily and covertly portable, adapted to each network service, and activated at unexpected moments. Therefore, if it only propagates inside the system, it can cause extensive damage. The following identified most dangerous attack is DoS. Every service can become a target for the DoS attack. There are various ways to launch this attack against the service, including distributed approach, botnet-based attack, or using 0-day vulnerability. Typically, service providers use well-known countermeasures like anti-DoS systems based on firewalls and ingress filters, build-in High Availability and Load Balancing solutions, setting proper connection limits, and request execution timeouts. The use of the MEC framework could be a remedy against such an attack. For instance, it allows the service provider to move some of the traffic to other MEC hosts to avoid service unavailability.

Some of the attacks classified by ENISA [290] have not been identified in our studies as very dangerous for the considered 5G MEC vertical industries and their use cases. However, the reason for the lack of their inclusion could be that such attacks are relatively new (e.g., [291]), rarely reported, and are not yet considered in recent research papers. For instance, cryptojacking is not on the list of the most common threats, but it is not widely known yet, making it enjoyable to indicate and discuss in the future. This attack is mining cryptocurrencies without the knowledge and approval of the computing resources' owner. The mining process might be executed in various places: in the UE, at the MEC host on any virtualization layer, and in the cloud. Each place is worthy of the attackers' interest because it provides free computing resources that can be exchanged for money.

Table 2 in Section II specifies which attacks affect the 5G MEC verticals and their use cases most. Certainly, they are destructive to the network quality and security parameters. Table 2 gives us the information on which verticals are sensitive, to some extent, to a specific threat (mark "V" in a corresponding column) and which threat is the most dangerous for all verticals (graded by the number in column "V" in Table 2).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 16. Main benefits and drawbacks introduced by the vertical industries within 5G MEC systems

Vertical	Benefits	Drawbacks
Manufacturing industry	New low latency-based services: robotic control, Augmented Reality, and video analytics. Privacy and security of manufacturing process thanks to data kept and processed locally	New business and operational models needed for Private (campus) 5G networks. Security issues with legacy industrial systems integration.
The Financial Sector	Bandwidth efficiency for serving mobile users, possible new services using edge computing capabilities Mobile-to-Insurance services for logistics and automotive sectors	High security requirements, strong regulation, and high costs of protection of sensitive data.
Healthcare	Privacy protection - processing data at the edge will ensure better user privacy than when raw data is uploaded to the cloud. Ensuring redundancy of systems and their high availability, protecting communication between patients and smart healthcare applications/services. Edge computing capabilities and 5G wireless networking technologies can provide real-time and cost-effective patient remote monitoring. Edge gateways for IoMT devices. QoS monitoring at the edge of the network for remote health care services like remote surgery.	High costs of protection of sensitive data. Relatively low computing resources.
Retail	Local treatment of the data coming from massive IoT. Specialized Artificial Intelligence bots allowing interaction with a customer in a more dynamic way. Security services at the edge of the network. More effective AR/VR services. Reduction of WAN traffic.	Need to change the operational model. The new model needs to be analyzed in terms of TCO.
Telecommunications	Openness for new service providers. Closing network traffic at the edge: fewer data sent to the core network. Improvement of QoS and QoE. Providing new customer-oriented services. E2E resources virtualization.	Need for higher protection for network APIs. Need additional protection for shared resources and isolation. Need more advanced management systems. Higher maintenance and support costs.
Authorities	Decentralization - data processing at the edge. Faster decision-making by additional computation power. Possibility to use AI and ML for analysis of regional data and customized prediction.	Privacy issues and need for additional protection for distributed computing. Need for additional integration of government IT system with other infrastructures.
Media and Entertainment	Ultra High Fidelity Media experience. On-site Live Event Experience. User and Machine Generated Content. New possible services, sharable infrastructure for events.	Protection of distributed content. Law, License, Copyright, and other aspects of content multiplication. Higher risk of a data leak.
Smart City	Additional computation power for IoT and smart sensors data collection and online processing. New services like disaster prediction, advanced traffic control, Augmented Reality, communication with other smart entities. New management features for optimization of Distributed Energy and others resources.	Privacy issues. Responsibility issues - for car accidents, lack of energy, and others. Cost of high availability and protection systems.
Agriculture and food industry	Multiple data collection and processing at the edge with real-time response. The opportunity of robotization, automation remote control. New advanced AI/ML prediction systems. Higher regional cooperation system and distribution.	Need for additional protection for IoT sensors. Cost of SIM cards, transfer, and management systems. Risk of data manipulation and leakage. Energy consumption.
Logistics	Opportunity of realization new services like Autonomic vehicles, Automated logistics, V2X communication, Vulnerable Road User discovery, cooperative collision avoidance.	Privacy issues. Responsibility issues - for car accidents, mistakes in logistics. Cost of redundant resources to avoid High Availability issues. Need for protection of sensitive data. Risk of making services dependent on telecom capabilities (country, continent).
Education, culture, and science	New low latency-based services: AR/VR services, tactile internet. Bandwidth efficiency for remote learning and cultural events. Inclusion of persons with disabilities in education and culture.	Need for protection of content and user privacy.
Critical Infrastructure Sectors	Ensuring operability in case of unavailability of a wide area network and access to cloud computing resources. Local MEC nodes can still provide critical communication and services. Protection of critical infrastructure by placement in MEC dedicated enhanced security systems. Monitoring of critical infrastructure. MEC is a distributed system that is more fault-tolerant by design.	More challenging to ensure the physical security of the MEC location. Need for strong security by design approach.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 17. Impact of threats on 5G MEC parameters. (impact factors: C-5, E-4, I-3, NE-2, N-1, N/A -0)

	Web Based Attacks	**Web Application Attacks**	**Phishing**	**Spam**	**Denial of Service**	**Botnets**	**Malware**	**Ransomware**	**Cryptojacking**	**Data Breaches**	**Information Leakage**	**Identity theft**	**Cyber Espionage**	**Insider threat**	**Physical manipulation damage/theft/ loss**
Latency	I	I	N	N	**C**	**C**	**C**	I	C	N	N	N	N	**C**	**C**
Reliability	E	E	N	N	**C**	**C**	**C**	C	C	N	N	N	N	**C**	**C**
Peak data rate	I	I	N	N	**C**	**C**	**C**	C	C	N	N	N	N	**C**	**C**
Device Density	N	N	N	N	**N**	**N**	**N**	N	N	N	N	N	N	**C**	**C**
Capacity	I	I	N	N	**C**	**C**	**C**	C	C	N	N	I	N	**C**	**C**
Isolation level	I	I	N	N	**C**	**C**	**C**	C	C	I	I	I	N	**C**	**C**
Trust to MEC platform	I	I	C	C	**C**	**C**	**C**	C	C	I	I	I	N	**C**	**C**
Edge Computing Usage	I	I	N	I	**C**	**C**	**C**	C	C	N	N	N	N	**C**	**C**
Availability	C	C	N	N	**C**	**C**	**C**	C	C	N	N	N	N	**C**	**C**

Naturally, the threats presented in Table 2 can have some degradation impact on crucial quality and security parameters of the 5G MEC network (these parameters are characterized briefly in Table 3). Table 17 contains estimated characteristics of possible threats' influence on these 5G MEC parameters. Each row includes one of five values: C (Crucial), E (Essential), I (Important), NE(Not-Essential), N (Negligible), N/A (Not Applicable). Based on this Table, it is possible to specify threats that have the greatest impact on the 5G MEC parameters in general:

- DoS,
- Botnets,
- Malware,
- Insider Threat,
- Physical manipulation damage/theft/loss.

Sometimes, we can predict the effect of the attacks on the quality parameters in an abstract use case. However, it is important to know what such an effect in a specific vertical deployment is since the parameters do not play the same important role in the functioning of a specific vertical. By compiling the average expected requirements on the verticals' parameters collected in Tables 4 - 15 for each vertical industry and the general threats' impacts on these parameters presented in Table 2 we reached the sensitivity of 12 verticals to the 5G MEC quality and security parameters. The adequate sensitivities are collected in Table 18, with the scale analogous to presented in Table 2. The last column in Table 18 summarizes the vulnerabilities to attacks for the 5G MEC parameters of all twelve verticals considered in this paper. The first 12 columns represent such vulnerabilities in all verticals of the 5G MEC. The last one is a sum of individual impacts representing each vertical expressed as the number of the range 0...5. This way, the latency can be indicated as the most sensitive parameter.

The latency considered as the primary quality parameter of 5G mobile networks and application of the edge server is indispensable to provide a high quality of the deployed solution. Thus, protection of the low latency against attacks must have priority in MEC server protection. The second vulnerable parameter is Edge Computing Usage. An attack against this parameter is the destruction of the MEC-based services, so general protection of the edge servers is the second challenge. The following two crucial aspects of the 5G MEC networks functioning are related to the traditional

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 18. Impact of threats on 5G MEC parameters in verticals. (impact factors: C-5, E-4, I-3, NE-2, N-1, N/A -0)

5G MEC parameter	Manufacturing industry	The Financial Sector	Healthcare	Retail	Telecommunications	Authorities	Media and Entertainment	Smart City	Agriculture and food industry	Logistics	Education, culture and science	Critical Infrastructure Sectors	Impact (sum of factors)
Latency	C	E	C	E	C	I	C	C	I	C	E	E	51
Reliability	I	E	C	I	C	C	E	C	I	C	E	I	48
Peak data rate	I	NE	C	I	C	I	E	NE	NE	E	I	E	41
Device Density	I	N	I	C	C	N/A	I	I	NE	E	I	N	32
Capacity	I	I	I	E	C	N/A	E	C	NE	C	I	NE	39
Isolation level	I	E	C	NE	C	E	E	C	I	C	E	E	46
Trust to MEC platform	E	I	C	NE	C	E	E	C	I	C	E	C	47
Edge Computing Usage	E	I	C	E	C	I	C	C	I	E	E	C	50
Availability	I	E	C	N/A	C	C	C	C	NE	C	C	I	47

understanding of security. The first of them is a threat related to the network's reliability/availability (which represents the A - availability in the CIA triangle), while the second one covers the CI - confidentiality and integrity, in our 9-tuple of parameters represented by the trust to MEC platform and isolation level 5G MEC parameters.

In Section V we will present a synthetic view of the impact of threats on Verticals in MEC in case of affecting crucial 5G MEC parameters considered in Section III. The general directions indicating how to minimize these threats or reduce the vulnerability of parameters will be shown.

V. CONCLUSIONS AND MAIN SECURITY RECOMMENDATIONS

In Section IV the estimation of threats influence on 5G MEC parameters was proposed (Table 17) and the sensitivity of verticals to the 5G MEC quality and security parameters degradation was derived (Table 18). Therefore, the highly impacting parameters for Verticals can be correlated with the most dangerous threats to these parameters. Table 19 presents the resulting level of sensitivity of Verticals to different threats, in the context of affecting 5G MEC parameters presented in Section III.

From this synthetic view, major threats which impact 5G MEC parameters and consequently operation of the largest number of verticals in MEC can be obtained. These are:

- Web-based Attacks and Web Application Attacks,
- Denial of Service,
- Botnets,
- Malware (and Ransomware),
- Cryptojacking,
- Insider threat,
- Physical manipulation/damage/theft/loss.

Denial of Service, botnets, malware, cryptojacking, insider threat, and physical manipulation/damage/theft/loss threats, if not adequately addressed, are the most dangerous and critical for all 5G MEC parameters presented in Section III. Consequently, they can affect the largest number of Verticals and their use cases. Also, Web-based attacks and Web Application Attacks can have a significant impact on 5G MEC parameters. Therefore, the following use cases of Verticals can be the most impacted if threats presented above are not properly addressed:

- Manufacturing Industry: robotic control, automated guided vehicle, augmented reality, quality check,
- Financial Sector: the most sensitive to InterBank, Mobile-to-Bank,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3088374, IEEE Access

TABLE 19. Impact of threats (affecting 5G MEC parameters) on verticals. (impact level: L-Low, M-medium, H-High)

5G MEC parameter	Manufacturing industry	The Financial Sector	Healthcare	Retail	Telecommunications	Authorities	Media and Entertainment	Smart City	Agriculture and food industry	Logistics	Education, culture and science	Critical Infrastructure Sectors
Web-Based Attacks	H	H	H	M	H	H	H	H	M	H	H	H
Web Application Attacks	H	H	H	M	H	H	H	H	M	H	H	H
Phishing	L	L	L	L	L	L	L	L	L	L	L	L
Spam	L	L	L	L	L	L	L	L	L	L	L	L
Denial of Service	H	H	H	H	H	H	H	H	M	H	H	H
Botnets	H	H	H	H	H	H	H	H	M	H	H	H
Malware	H	H	H	H	H	H	H	H	M	H	H	H
Ransomware	H	H	H	H	H	H	H	H	M	H	H	H
Cryptojacking	H	H	H	H	H	H	H	H	M	H	H	H
Data Breaches	L	L	L	L	L	L	L	L	L	L	L	L
Information Leakage	L	L	L	L	L	L	L	L	L	L	L	L
Identity Theft	M	M	M	L	M	L	M	M	L	M	M	L
Cyber Espionage	L	L	L	L	L	L	L	L	L	L	L	L
Insider Threat	H	H	H	M	H	M	H	H	M	H	H	H
Physical	H	H	H	M	H	M	H	H	M	H	H	H

- Healthcare: health monitoring, smarter medication, robotics,
- Retail: on-site live events,
- Telecommunications: MVNE, Full MVNO, Light MVNO,
- Authorities: Authority-to-Authority,
- Media and Entertainment: Ultra High-Fidelity Media, Immersive and Integrated Media, and Gaming, On-site live events experience,
- Smart City: smart grid, emergency situation management,
- Agriculture and Food Industry: Drones, Remote control, Agribots,
- Logistics: V2X communication, automated vehicles,
- Education, Culture and Science: Tactile Internet and Skillset communication, Personalized learning, IoT & Smart Classroom, VR-AR, and education,
- Critical Infrastructure: Critical support services, critical communication (emergency), high-speed wireless access, UHD broadcasting, public safety services.

Analysis and rating of most critical parameters concerning Vertical's needs and possible attack types resulted in identifying most dangerous attacks with the most significant impact on services of Verticals. Such analysis provides a valuable starting point for the decisions concerning secure MEC infrastructure design, MEC application design, infrastructure

deployment, application implementation, system operation, etc. Continuing analysis of the impact of the threats on Verticals can lead to further and more detailed identification of assets concerning the threats. To identify priorities, one can choose the most suitable solutions for security orchestration, security management, multilayer security, proper measures, controls, etc. For this reason, a complex holistic approach to MEC infrastructure design, orchestration, and operational security is needed. Different dimensions should be addressed to protect:

- 5G MEC quality parameters crucial for Verticals against the most dangerous threats identified in Table 19,
- Verticals against threats specific and most dangerous for them presented in Table 2 in Section II (e.g., malware, Denial of Service, botnet, insider threat, physical manipulation/ damage/ theft/ loss),
- All the MEC system's components.

The main recommendations for such an approach to security in MEC are:

- MEC infrastructure should be secured by design. In particular:
  - it should meet isolation and sovereignty requirements of hosted third parties,
  - infrastructure monitoring should be applied to ensure platform safety and resiliency,
  - the infrastructure should be built considering security requirements for external and internal interfaces, Local Data Network, internal MEC network, virtualization, Cloud and MEC platform,
  - proper access control scheme should be applied,
  - MEC applications should be secure by design and built according to appropriate security requirements,
  - it should be considered that MEC is not an isolated but rather a distributed system, with its specific location in the network and specific model of communication (access, intra-MEC, Cloud/Internet).
- Operational security architecture for the safety of MEC applications in MEC environment is needed.
  - Incident management should be dynamic and automated (as far as possible) and based on using new enablers (e.g., ML/AI-based methods for detection).
  - Dedicated Security Services addressing security needs of Verticals should be applied by proper orchestration according to appropriate security policies (protection, reaction), coherent with 5G network policy.
  - Security policy of MEC applications can contain a technical description of specific security needs of Vertical application in MEC.

It should be noticed that the possibility of compromising end devices can be a severe vulnerability of the whole MEC ecosystem. Compromised devices could be used to attack the MEC system and disrupt its operation. Therefore, the proper approach to the security of devices is crucial too.

VI. SUMMARY AND FUTURE WORK

In this paper, we have presented an overview of how in practice, the application of the MEC technology affects the functioning 5G MEC-based services. We have considered twelve representative vertical industries of 5G MEC and presented their essential characteristics of functioning, threats they undergo, and vulnerabilities. Then for each of described verticals, an additional analysis of the most needed parameters and their required level was done. According to selected parameters, we also analyzed the most frequent network attacks and their impact on different verticals' use cases. This impact is strongly correlated with the required performance of a vertical and its expected security level: the higher the requirements, the more vulnerable the sector is, and the more severe the attacks are. Our analysis, based on the dedicated contemporary literature (see Table 20), shows a well-defined picture of threats in 5G MEC networks offering services to public recipients. It allows indicating those places in which correctly applied security measures will give a protective effect the fastest and minimize potential losses.

The security of 5G mobile networks is currently the subject of extensive research. Note that the integration of an additional MEC element in the network architecture may create new vulnerabilities. The attack surface in MEC is larger than in the classical IT system since inherent MEC distributed architecture combines resource virtualization, 3rd party application hosting, and mobile network integration. On the other hand, deploying services at the edge of the network can help protect the entire mobile network by isolating potentially compromised services and locating security tools on the edge server.

In this paper, we described which vulnerabilities are the most impacting on the parameters needed for service realization for a large number of verticals. Thanks to this analysis, it is possible to prioritize protection and minimize the most dangerous threats for 5G MEC. Moreover, we suggest using Edge Computing technology to reduce them as a new opportunity for attack neutralization near the service.

In the Edge Computing paradigm, the service consists of device application, MEC application, and Cloud backend. Service providers need to have End-to-End security visibility using preferred security management systems. End-to-End security largely depends on the appropriate addressing of roles and responsibilities in delivering and managing the service. Therefore it is important to address the liability by:

- Security Service Level Agreement (SSLA) between MEC Operators and Verticals on guaranteed security metrics.
- Security Service Level Agreement (SSLA) between Operator and MEC infrastructure providers on guaranteed security metrics.
- Ability to verify the security of infrastructure used to deploy MEC platform and hosting MEC applications.

TABLE 20. Overview of 5G MEC verticals-related literature

Vertical	Characteristics	Threats and vulnerabilities	Attacks and countermeasures	Use cases	Parameters	Other issues
Manufacturing industry	[50], [66], [67]	[55]–[57], [290]	[58]–[62], [64]	[50]–[52]	[53], [54], [292], [307]	[63], [65], [68]
The Financial Sector	[69], [70]	[71], [73], [74], [290]	[75]–[77]	[295]–[298]	[292], [295], [296], [307]	[117]
Healthcare	[82]–[92], [94]–[96]	[97]–[103]	[104]–[109]	[80], [81], [182]	[3], [303], [307]	[78], [79]
Retail	[111]–[114]	[113], [115], [116]	[117]	[113], [303]	[80], [303]	[113]
Telecommunications	[123]–[125]	[135]–[139], [143]–[146]	[147]–[153]	[125]–[128], [130]–[133], [140]–[142]	[140], [154], [155]	[129], [134]
Authorities	[156], [157], [159], [163], [165]–[167]	[168]–[171], [173], [174]	[175]–[179]	[158], [161], [164]	[180], [181]	[160], [162], [172]
Media and Entertainment	[185]–[192]	[120], [121]	[122]	[183], [184]	[3], [4], [307], [308]	[193], [194]
Smart City	[206]–[209], [211]	[213], [214]	[210], [215]	[216]–[218]	[3], [4], [209], [216]	[212]
Agriculture and food industry	[220], [221], [223]–[225]	[226]–[235], [237], [238]	[231], [236], [239], [240]	[221], [222]	[220], [223], [234], [241], [309]	[236]
Logistics	[195]–[198], [206], [209]	[196], [199]	[200], [201]	[204], [205], [294], [303]	[31], [205], [300], [303], [307]	[196]
Education, culture and science	[250], [251]	[253]–[258]	[259]–[271]	[246]–[248]	[3]	[249]
Critical Infrastructure Sectors	[47], [272]–[274]	[278], [279], [290]	[278], [279], [281]–[284], [286]–[288]	[47], [272], [289]	[292], [307]	[275]–[277]

- Ability to verify the security of the MEC platform with MEC services and the Life Cycle Management implementation.

Modern advanced technologies like artificial intelligence, data mining, or machine learning can be a new inspiration to mobile network development. Those techniques could combine data and knowledge from the MEC service layer and from lower network layers (from physical to transport layer) to make better resource allocation decisions based on the broader context. The paper [23] considered this combined approach with only a single vertical (social media) for relationships between verticals and aggregated impact on the network might be a subject of future research.

Integration of network performance with artificial intelligence [310] is the milestone to transform 5G into 6G. A promising approach might be clustering, one of the machine learning methods, to divide data flows, users, and services into clusters with similar properties to manage them more effectively. Regression techniques and neural networks could also be used to obtain expected resource utilization upfront and avoid an unacceptable level of resource utilization. Moreover, active methods from the AI toolset should be considered to increase the efficiency of the ML system by providing feedback [310].

Thus, the use of MEC technology gives vast possibilities of using mobile networks in different branches of the digital economy, increasing network's quality and performance. However, it is also a new security challenge that requires detailed analysis (but it can be a subject of another detailed study).

REFERENCES

[1] *5G empowering vertical industries*, White Paper, 5G PPP, 2016. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf

[2] *View on 5G Architecture*, Ver. 3.0, 5G PPP, Feb. 2020. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2020/02/5G-PPP-5G-Architecture-White-Paper_final.pdf

[3] *Requirements definition and analysis from vertical industries and core applications*, Deliverable D1.2, 5G EVE, 2019. [Online]. Available: https://www.5g-eve.eu/wp-content/uploads/2019/11/5g-eve-d1.2-requirements-definition-analysis-vertical-industries-core-applications.pdf

[4] *Participating vertical industries planning*, Deliverable D2.6, 5G EVE, 2019. [Online]. Available: https://www.5g-eve.eu/wp-content/uploads/2019/11/5g-eve-d2.6-participating-vertical-industries-planning.pdf

[5] *Cisco 5G Vision Series: Vertical Value Creation*, White Paper, 2016. [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/ultra-services-platform/5g-vision-series-vertical-value-creation.pdf

[6] R. Vannithamby and A.C.K. Soong, (Eds), *5G Verticals: Customizing Applications, Technologies and Deployment Techniques*, New York, NY, USA: Wiley, 2020. https://doi.org/10.1002/9781119514848

[7] A. Rostami, "Private 5G Networks for Vertical Industries: Deployment and Operation Models," in *2019 IEEE 2nd 5G World Forum (5GWF)*, 2019. https://doi.org/10.1109/5GWF.2019.8911687

[8] G. Spathoulas and S. Katsikas, "Towards a Secure Industrial Internet of Things," in C. Alcaraz (Ed.), *Security and Privacy Trends in the Industrial Internet of Things*, ASTSA, Springer 2019. https://doi.org/10.1007/978-3-030-12330-7_2

[9] A.S.D. Alfoudi *et al.*, "Data Traffic Model in Machine to Machine Communications over 5G Network Slicing," in *2016 9th International Conference on Developments in e-Systems Engineering (DeSE)*, 2017. https://doi.org/10.1109/DeSE.2016.54

[10] T. Doukoglou *et al.*, "Vertical Industries Requirements Analysis and Targeted KPIs for Advanced 5G Trials," in *2019 European Conference on Networks and Communications (EuCNC)*, 2019. https://doi.org/10.1109/EuCNC.2019.8801959

[11] *Why do we need 5G?* [Online]. Available: https://www.etsi.org/technologies/5g

[12] A. Xiang, "5G Market and Industry," in W. Lei *et al.*, *5G System Design*, Springer, Cham 2020. https://doi.org/10.1007/978-3-030-22236-9_6

[13] B. Blancoa, *et al.*, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Computer Standards and Interfaces*, vol.54, no.4, pp.216-228, 2017. https://doi.org/10.1016/j.csi.2016.12.007

[14] S. Singh and R.K. Jha, "A Survey on Software Defined Networking: Architecture for Next Generation Network," *J. Netw. Syst. Manage.*, vol.25, pp.321-374, 2017. https://doi.org/10.1007/s10922-016-9393-9

[15] Q. Long *et al.*, "Software Defined 5G and 6G Networks: a Survey," *Mobile Networks and Applications*, 2019. https://doi.org/10.1007/s11036-019-01397-2

[16] R. Mijumbi *et al.*, "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Commun. Surveys Tuts.*, vol.18, no.1, pp.236-262, 2016, https://doi.org/10.1109/COMST.2015.2477041

[17] L. Chiaraviglio *et al.*, "Algorithms for the design of 5G networks with VNF-based Reusable Functional Blocks", *Ann. Telecommun.*, vol.74, pp.559-574, 2019. https://doi.org/10.1007/s12243-019-00722-w

[18] A.A. Barakabitze *et al.*, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," in *Computer Networks*, vol.167, art.106984, 2020. https://doi.org/10.1016/j.comnet.2019.106984

[19] R. Sahay, W. Meng, and Ch.D. Jensen, "The application of Software Defined Networking on securing computer networks: A survey," *J. Netw. Comp. Appl.*, vol.131, pp.89-108, 2019. https://doi.org/10.1016/j.jnca.2019.01.019

[20] F. Nife, Z. Kotulski, and O. Reyad, *New SDN-Oriented Distributed Network Security System*, *Appl. Math. Inf. Sci.*, vol.12, no.4, pp.673-683, 2018. https://doi.org/10.18576/amis/120401

[21] Y.-Ch. Hu *et al.*, *Mobile Edge Computing. A key technology towards 5G*, ETSI White Paper No. 11, First edition, September 2015

[22] *Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications*, ETSI White Paper No. 36, Jul. 2020.

[23] E. Stai, V. Karyotis and S. Papavassiliou, *Exploiting socio-physical network interactions via a utility-based framework for resource management in mobile social networks,* in IEEE Wireless Communications, vol. 21, no. 1, pp. 10-17, February 2014, https://doi.org/10.1109/MWC.2014.6757892

[24] Z. Kotulski *et al.*, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP J. Inf. Sec.*, 2018: 2, pp.1-23, (2018), https://doi.org/10.1186/s13635-018-0072-0

[25] *5G E2E Technology to Support Verticals URLLC Requirements*. NGMN Alliance, 2020.

[26] M.A. Imran, Y.A. Sambo, and Q.H. Abbasi (Eds), *Enabling 5G Communication Systems to Support Vertical Industries*, New York, NY, USA: Wiley, 2019.

[27] J. Kalliovaara *et al.*, "Designing a Testbed Infrastructure for Experimental Validation and Trialing of 5G Vertical Applications", in P. Marques *et al.* (Eds), *CROWNCOM 2017, LNICST* 228, pp. 247-263, 2018. https://doi.org/10.1007/978-3-319-76207-4_21

[28] I. Hussain, Q. Duan, and T. Zhong, "Service Performance Tests on the Mobile Edge Computing Platform: Challenges and Opportunities", in H. Yang *et al.* (Eds), *Smart Service Systems, Operations Management, and Analytics*, Springer Proceedings in Business and Economics, Springer 2020. https://doi.org/10.1007/978-3-030-30967-1_22

[29] M. Monshizadeh, V. Khatri, and I. Adam, "Security for Vertical Industries", in *Wiley 5G Ref: The Essential 5G reference*, New York, NY, USA: Wiley, 2019. https://doi.org/10.1002/9781119471509.w5GRef156

[30] S. Cheruvu *et al.*, *Demystifying Internet of Things Security Successful IoT Device/Edge and Platform Security Deployment*, Chapter 6 *IoT Vertical Applications and Associated Security Requirements*, Apress Berkeley 2020. https://doi.org/10.1007/978-1-4842-2896-8

[31] N. Hehenkamp, Ch. Facchi, and S. Neumeier, "How to Achieve Traffic Safety with LTE and Edge Computing," in K. Arai and R. Bhatia (Eds), *FICC 2019*, LNNS 69, pp. 164-176, Springer 2020. https://doi.org/10.1007/978-3-030-12388-8_12

[32] P. Krishnan, S. Duttagupta, and K. Achuthan, "SDNFV Based Threat Monitoring and Security Framework for Multi-access Edge Computing Infrastructure," *Mobile Networks and Applications*, vol.24, pp.1896-1923, 2019. https://doi.org/10.1007/s11036-019-01389-2

[33] N. Akkari and N. Dimitriou, "Mobility management solutions for 5G networks: Architecture and services", *Comput. Netw.* vol. 169, art. 107082, 2020. https://doi.org/10.1016/j.comnet.2019.107082

[34] M. Shafi, R.K. Jha, and M. Sabraj, "A survey on security issues of 5G NR: Perspective of artificial dust and artificial rain", *J. Netw. Comput. Appl.* vol. 160, art. 102597, 2020. https://doi.org/10.1016/j.jnca.2020.102597

[35] O. Yurekten and M. Demirci, "SDN-based cyber defense: A survey", *Futur. Gener. Comp. Syst.*, vol. 115, pp. 126-149, 2021. https://doi.org/10.1016/j.future.2020.09.006

[36] S. Sridharan, "A Literature Review of Network Function Virtualization (NFV) in 5G Networks", *I. J. Comput. Trends Technol.*, vol. 68 no. 10, pp. 49-55, Oct. 2020. https://doi.org/10.14445/22312803/IJCTT-V68I10P109

[37] P.P. Ray and N. Kumar, "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review", *Comput. Commun.*, vol. 169, pp. 129-153, 2021. https://doi.org/10.1016/j.comcom.2021.01.018

[38] N. Abbas *et al.*, "Mobile Edge Computing: A Survey", *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450-465, Feb 2018. https://doi.org/10.1109/JIOT.2017.2750180

[39] C. Jiang *et al.*, "Energy aware edge computing: A survey", *Comput. Commun.*, vol. 151, pp. 556-580, 2020. https://doi.org/10.1016/j.comcom.2020.01.004

[40] Quoc-Viet Pham *et al.*, "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art", *IEEE Access*, vol. 8, art. 116974, 2020. https://doi.org/10.1109/ACCESS.2020.3001277

[41] A. Zafeiropoulos *et al.*, "Enabling Vertical Industries Adoption of 5G Technologies: a Cartography of evolving solutions", *2018 European Conference on Networks and Communications (EuCNC): Network Softwarisation (NET)*, pp. 130-135, 2018. https://doi.org/10.1109/EuCNC.2018.8442656

[42] F. Spinelli and V. Mancuso, "Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility", *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, Q1 2021. https://doi.org/10.1109/COMST.2020.3037674

[43] A. Jain, E. Lopez-Aguilera, and I. Demirkol, "Are mobility management solutions ready for 5G and beyond?", *Comput. Commun.*, vol. 161, pp. 50-75, 2020. https://doi.org/10.1016/j.comcom.2020.07.016

[44] 5G Infrastructure Association web page. [Online]. Available: https://5g-ia.eu/verticals/

[45] A. Javed, *CyberSecurity Landscape in 2018 - The focus is on vertical industries,* 14 Jan. 2018. [On-

line]. Available: http://www.xorlogics.com/2018/01/14/cybersecurity-landscape-in-2018-the-focus-is-on-vertical-industries/

[46] *Great Expectations: Sizing the Opportunity for 5G in Vertical Industries. Survey Report*, Insights - Mobile World Live, 9 Mar 2020. https://www.gsma.com/iot/resources/great-expectations-sizing-the-opportunity-for-5g-in-vertical-industries/

[47] CISA Web Page. [Online]. Available: https://www.us-cert.gov/

[48] "Empowering Vertical Industries through 5G Networks - Current Status and Future Trends," Version 1.0, 5G PPP Technology Board & 5G IA Verticals Task Force, 2020. https://doi.org/10.5281/zenodo.3698113

[49] C. Campbell *et al.*, *The 5G economy: How 5G technology will contribute to the global economy*, HIS 2017. [Online]. Available: https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf

[50] *5G and the Factories of the Future*, The white paper, 5G PPP, 2015. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf

[51] M. Mueller *et al.*, "5G as Key Technology for Networked Factories: Application of Vertical-specific Network Services for Enabling Flexible Smart Manufacturing," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, 2020. https://doi.org/10.1109/INDIN41052.2019.8972305

[52] M. Karrenbauer *et al.*, "Future industrial networking: from use cases to wireless technologies to a flexible system architecture," *at-Automatisierungstechnik*, vol.67, no.7, pp.526-544, 2019. https://doi.org/10.1515/auto-2018-0141

[53] 5G PICTURE, D2.1 *5G and Vertical Services, use cases and requirements*, v.2.0, 2018.

[54] 3GPP TS 22.104, *Service requirements for cyber-physical control applications in vertical domains*, V18.0.0 (2021-03).

[55] A. Soltysik-Piorunkiewicz and M. Krysiak, "The Cyber Threats Analysis for Web Applications Security in Industry 4.0," in M. Hernes *et al.* (Eds), *Towards Industry 4.0 - Current Challenges in Information Systems*, Studies in Computational Intelligence 887, Springer 2020. https://doi.org/10.1007/978-3-030-40417-8_8

[56] *Top 10 Web Application Security Risks*. [Online]. Available: https://owasp.org/www-project-top-ten/

[57] *Top 10 Mobile Risks - Final List 2016* [Online]. Available: https://owasp.org/www-project-mobile-top-10/

[58] E. Oztemel and S. Gursev, "Literature review of Industry 4.0 and related technologies," *J. Intell. Manuf.*, vol. 31, pp. 127-182, 2020. https://doi.org/10.1007/s10845-018-1433-8

[59] *Security Standards White Paper for Sino-German Industrie 4.0/Intelligent Manufacturing*, Sino-German Industrie 4.0/Intelligent Manufacturing Standardization Sub-Working Group, April 2018.

[60] C. Rieger *et al.*, (Eds), *Industrial Control Systems Security and Resiliency. Practice and Theory*, Springer 2019. https://doi.org/10.1007/978-3-030-18214-4

[61] A. Wegner, J. Graham, and E. Ribble, *A New Approach to Cyberphysical Security in Industry 4.0*, in L. Thames and D. Schaefer (Eds), *Cybersecurity for Industry 4.0*, Springer Series in Advanced Manufacturing, Springer 2017. https://doi.org/10.1007/978-3-319-50660-9_3

[62] L. Thames and D. Schaefer, (Eds), *Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing*. Springer 2017. https://doi.org/10.1007/978-3-319-50660-9

[63] Z. Kotulski and A. Zwierko, "Security of Mobile Code," Chapter 197 in *Mobile Computing: Concepts, Methodologies, Tools, and Applications*, pp. 2583-2599, IGI Global, 2009. https://doi.org/10.4018/978-1-60566-054-7.ch197

[64] S.R. Chhetri *et al.*, "Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0," *J. Hardw. Syst. Secur.* vol.2, pp. 51-68, 2018. https://doi.org/10.1007/s41635-017-0031-0

[65] D. Perakovic *et al.*, "Identification of the Relevant Parameters for Modeling the Ecosystem Elements in Industry 4.0," in L. Knapcikova *et al.* (Eds), *4th EAI International Conference on Management of Manufacturing Systems, EAI/Springer Innovations in Communication and Computing*, Springer 2020. https://doi.org/10.1007/978-3-030-34272-2_11

[66] The OPC Foundation web page, [Online]. Available: https://opcfoundation.org/

[67] R. Khondoker *et al.*, "Addressing Industry 4.0 Security by Software-Defined Networking," in S.Y. Zhu *et al.* (Eds), *Guide to Security in SDN and NFV, Computer Communications and Networks*, Springer 2017. https://doi.org/10.1007/978-3-319-64653-4_9

[68] J. Ordonez-Lucena *et al.*, "The use of 5G Non-Public Networks to support Industry 4.0 scenarios," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, https://doi.org/10.1109/CSCN.2019.8931325

[69] S. Das, "The Cyber Security Ecosystem: Post-global Financial Crisis," Chapter 36 in S. Chatterjee *et al.* (Eds), *Managing in Recovering Markets*, Springer 2015, https://doi.org/10.1007/978-81-322-1979-8_36

[70] V. Ravi and S. Kamaruddin, "Big Data Analytics Enabled Smart Financial Services: Opportunities and Challenges," in P.K. Reddy *et al.* (Eds), *BDA 2017*, LNCS 10721, pp. 15 - 39, Springer 2017. https://doi.org/10.1007/978-3-319-72413-3_2

[71] S. Bhattacharya, "Unified Resource Descriptor over KAAS Framework. Refining Cloud Dynamics," in V.B. Aggarwal *et al.* (Eds), *Big Data Analytics, Advances in Intelligent Systems and Computing* 654, Springer 2018. https://doi.org/10.1007/978-981-10-6620-7_2

[72] S.P.V. Gollapudi *et al.*, "Promoting better financial inclusion through web page transformation - a systematic literature review," *J. Banking Financial Techn.*, vol.3, pp.131-147, 2019. https://doi.org/10.1007/s42786-019-00010-0

[73] S.S. Majeti *et al.*, *Study and Ranking of Vulnerabilities in the Indian Mobile Banking Applications Using Static Analysis and Bayes Classification*, in K.S. Raju *et al.* (Eds), *Proceedings of the Third International Conference on Computational Intelligence and Informatics*, Advances in Intelligent Systems and Computing 1090, Springer 2020. https://doi.org/10.1007/978-981-15-1480-7_5

[74] B. Streeter, *Consumers Crave More Mobile Banking Features Despite Security Concerns*, 2018. https://thefinancialbrand.com/74044/mobile-banking-features-digital-security

[75] A. Mukhopadhyay *et al.*, "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance," *Inf. Syst. Front.*, vol.21, pp.997-1018, 2019. https://doi.org/10.1007/s10796-017-9808-5

[76] R. Girasa, *Regulation of Cryptocurrencies and Blockchain Technologies. National and International Perspectives*, Springer 2018. https://doi.org/10.1007/978-3-319-78509-7

[77] U. Hacioglu, *Blockchain Economics and Financial Market Innovation Financial Innovations in the Digital Age*, Springer 2019. https://doi.org/10.1007/978-3-030-25275-5

[78] J. Portnoy, M. Waller, and T. Elliott, "Telemedicine in the Era of COVID-19," *J. Allergy Clin. Immunol.*, vol. 8, no. 5, pp. 1489-1491, 2020. https://doi.org/10.1016/j.jaip.2020.03.008

[79] J.E. Hollander and B.G. Carr, "Virtually Perfect? Telemedicine for Covid-19," *N. Engl. J. Med.*, vol.382, pp.1679-1681, 2020. https://doi.org/10.1056/NEJMp2003539

[80] *5G and e-Health*, White Paper, Sep. 2015, [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-eHealth-Vertical-Sector.pdf

[81] A. de la Oliva *et al.*, "5G-TRANSFORMER: Slicing and Orchestrating Transport Networks for Industry Verticals," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 78-84, 2018. https://doi.org/10.1109/MCOM.2018.1700990

[82] Y. Miao *et al.*, "Telesurgery Robot Based on 5G Tactile Internet," *Mobile Networks and Applications*, pp. 1645-1654, 2018. https://doi.org/10.1007/s11036-018-1110-3

[83] R. Gupta *et al.*, "Tactile-Internet-Based Telesurgery System for Healthcare 4.0: An Architecture, Research Challenges, and Future Directions," *IEEE Network*, vol. 33 no. 6, pp. 22-29, 2019. https://doi.org/10.1109/MNET.001.1900063

[84] R. Gupta *et al.*, "HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, 2019, pp. 1-5. https://doi.org/10.1109/CITS.2019.8862127

[85] S. Andreas *et al.*, "An Overview of mHealth Medical Video Communication Systems," in *Mobile Health. A Technology Road Map*, SSBN 5, pp. 609-633, Springer 2015. https://doi.org/10.1007/978-3-319-12817-7_26

[86] N.Y. Philip and I.U. Rehman, "Towards 5G Health for Medical Video Streaming over Small Cells," in *XIV Mediterranean Conference on Medical and Biological Engineering and Computing*, IFMBE Proceedings, vol 57, pp.1093-1098, Springer, Cham 2016. https://doi.org/10.1007/978-3-319-32703-7_215

[87] J. Lloret *et al.*, "An Architecture and Protocol for Smart Continuous eHealth Monitoring using 5G," *Computer Networks*, vol.129, no. 2, pp. 340-351, 2017. https://doi.org/10.1016/j.comnet.2017.05.018

[88] M. Cankar, *et al.*, "Fog and Cloud in the Transportation, Marine and eHealth Domains," in *European Conference on Parallel Processing*, pp. 292-303, 2017. https://doi.org/10.1007/978-3-319-75178-8_24

[89] S. Morosi, *et al.*, "Medical Tele-Monitoring and Tele-Assistance for Diabetics Patients by Means of 5G Cellular Networks," in *EAI International Conference on Body Area Networks*, 2019, pp. 79-88, https://doi.org/10.1007/978-3-030-34833-5_7

[90] B. Feng *et al.*, "Secure 5G Network Slicing for Elderly Care," in *International Conference on Mobile Web and Intelligent Information Systems*, pp. 202-213, 2019. https://doi.org/10.1007/978-3-030-27192-3_16

[91] S. Kyriazakos *et al.*, "eWALL: An Open-Source Cloud-Based eHealth Platform for Creating Home Caring Environments for Older Adults Living with Chronic Diseases or Frailty," *Wireless Pers. Commun.*, vol. 97, pp. 1835-1875, 2017. https://doi.org/10.1007/s11277-017-4656-7

[92] E. Kapassa *et al.*, "An Innovative eHealth System Powered By 5G Network Slicing," in *6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 7-12. https://doi.org/10.1109/IOTSMS48152.2019.8939266

[93] L. Castaldo and V. Cinque, "Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe," in *International ISCIS Security Workshop*, 2018, pp. 46-56. https://doi.org/10.1007/978-3-319-95189-8_5

[94] Bit4id: Smartlog, 2018. [Online]. Available: https://www.bit4id.com/en/secure-log-management/

[95] S. Haiba and T. Mazri, "Secure Communication in Ehealth Care Based IoT," in *Proc. 3rd International Conference on Smart City Applications*, 2019, pp. 311-323, https://doi.org/10.1007/978-3-030-37629-1_24

[96] S. Anwar and R. Prasad, "Framework for Future Telemedicine Planning and Infrastructure using 5G Technology," *Wireless Pers. Commun.*, vol. 100, pp. 193-208, 2018. https://doi.org/10.1007/s11277-018-5622-8

[97] K. Habib, A. Torjusen, and W. Leister, "Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth," in *7th International Conference on eHealth, Telemedicine, and Social Medicine, eTELEMED 2015*, pp. 73-78.

[98] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," *IEEE Wireless Comm.*, vol. 17, no. 1, pp. 51-58, 2010. https://doi.org/10.1109/MWC.2010.5416350

[99] S. Saleem, S. Ullah, and K.S. Kwak, "A Study of IEEE 802. 15.4 Security Framework for Wireless Body Area Networks," *Sensors*, vol. 11, no. 2, pp. 1383-1395, 2011. https://doi.org/10.3390/s110201383

[100] M.M. Noor and W.H. Hassan, "Wireless Networks: Developments, Threats and Countermeasures," *IJDIWC*, vol. 3, no. 1, pp. 119-134, 2013.

[101] B. Matt and C.C. Li, "A Survey of the Security and threats of the IMT-Advanced Requirements for 4G Standards," *IEEE Conference Anthology*, 1-8 Jan. 2013, pp.1-5. https://doi.org/10.1109/ANTHOLOGY.2013.6784900

[102] *Case Study, Threat Analysis of Medical Device*. [Online]. Available: http://www.ptatechnologies.com/default.htm

[103] A.B. Shahri and Z. Ismail, "A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS," *J. Inf. Sec.*, vol. 3, no. 2, pp. 169-176, 2012. https://doi.org/10.4236/jis.2012.32020

[104] *Security and Resilience in eHealth*. [Online]. Available: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-annex-a-countries2019-report

[105] *Health Insurance Portability And Accountability Act of 1996*, Public Law 104-191 Aug. 21, 1996. [Online]. Available: https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf

[106] A. Michalas and R. Dowsley, "Towards Trusted eHealth Services in the Cloud," in *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, Limassol, 2015, pp. 618-623, https://doi.org/10.1109/UCC.2015.108

[107] M. Bahrami and M. Singha, "A Dynamic Cloud Computing Platformfor eHealth Systems," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*, Boston, MA, 2015, pp. 435-438, https://doi.org/10.1109/HealthCom.2015.7454539

[108] S. Adibi and G.B. Agnew, "On The Diversity of eHealth Security Systems and Mechanisms," in *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Vancouver, BC, 2008, pp. 1478-1481, https://doi.org/10.1109/IEMBS.2008.4649447

[109] I.S. Mackenzie *et al.*, "Managing security and privacy concerns over data storage in healthcare research," *Pharmacoepidemiology and Drug Safety*, 28 Jun. 2011, pp. 885-893, https://doi.org/10.1002/pds.2170

[110] S. Richard and P. LePage, *What makes a good Progressive Web App?*. [Online]. Available: https://web.dev/pwa-checklist/

[111] M.C. Suciu and A. Petre, "The Role of 5G Technology in Sustainable Development of Smart Cities," *Annals of "Dunarea de Jos" University of Galati*, vol. 25, no. 2, pp. 39-47, 2019, https://doi.org/10.35219/eai1584040930

[112] "Impacts of 5G on productivity and economic growth", Bureau of Communications and Arts Research, Department of Communications and the Arts, Australian Government, 2018. [Online]. Available: https://www.communications.gov.au/file/35551/download?token=0MlSFttv

[113] Z. Song *et al.* "Smart e-commerce systems: current status and research challenges," *Electron Markets*, vol. 29, pp. 221-238, 2019. https://doi.org/10.1007/s12525-017-0272-3

[114] N. Kshetri, "5G in E-Commerce Activities," *IT Professional*, vol. 20, no. 4, pp. 73-77, 2018, https://doi.org/10.1109/MITP.2018.043141672

[115] G. Bella, R. Giustolisi, and S. Riccobene, "Enforcing privacy in e-commerce by balancing anonymity and trust," *Computers & Security*, vol. 30, pp. 705-718, 2011. https://doi.org/10.1016/j.cose.2011.08.005

[116] N. Kitukutha and J. Olah, "Trust and e-commerce, case study on Jumia company," *The Annals of the University of Oradea. Economic Sciences*, vol. 27, no.1, pp. 313-323, 2018. [Online]. Available: http://anale.steconomiceuoradea.ro/volume/2018/n1/31.pdf

[117] PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures*, 2018.

[118] A.M. French and J.P. Shim, "The Digital Revolution: Internet of Things, 5G, and Beyond," *Comm. Ass. Inf. Syst.*, vol. 38, art. 40, 2016. https://doi.org/10.17705/1CAIS.03840

[119] G. Lv, M. Gao, and X. Ji, "Research on Information Security of Electronic Commerce Logistics System," in *12th International Conference ICIC 2016*, Part I. https://doi.org/10.1007/978-3-319-42291-6_60

[120] M. Heitmann, "Security Risks and Business Opportunities in In-Car Entertainment," in K. Lemke, C. Paar, and M. Wolf (Eds), *Embedded Security in Cars*, pp. 233-246, Springer, Berlin 2006. https://doi.org/10.1007/3-540-28428-1_14

[121] W.B. Jaballah, M. Conti, and C.E. Palazzi, "The Position Cheating Attack on Inter-Vehicular Online Gaming," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2018, pp. 1-6. https://doi.org/10.1109/CCNC.2018.8319160

[122] *E-Safety Vehicle Intrusion Protected Applications* , 2011. [Online]. Available: https://www.evita-project.org/EVITA_factsheet.pdf

[123] T. Cottam and M. ap Darran, *MVNO Opportunities and Strategies. Part of the Service.* Provider 2020 series. https://amdocsoptima.com/wp-content/uploads/2018/04/MVNO-Opportunities-and-Strategies.pdf

[124] D. Anto and S. Nadzida, "Strategies of Mobile Virtual Network Operators in the Southeast Europe Region," *Josip Juraj Strossmayer University of Osijek, Interdisciplinary Management Research*, vol. 5, pp. 123-135, 2009.

[125] N. Dao *et al.*, "A Softwarized Paradigm for Mobile Virtual Networks: Overcoming a Lack of Access Infrastructure," *IEEE Vehicular Technology Magazine*, vol. 13, no. 4, pp. 106-115, 2018. https://doi.org/10.1109/MVT.2018.2866120

[126] C. Yacouba, K. Georges, and A. Mohammed, "Mobile Virtual Network Operator Strategy for Migration towards 4G," in *International Conference on Information and Communication Technology Research, ICTRC 2015*. https://doi.org/10.1109/ICTRC.2015.7156473

[127] K. Samdanis, X. Costa-Perez and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Comm. Mag.*, vol. 54, no. 7, pp. 32-39, 2016, https://doi.org/10.1109/MCOM.2016.7514161

[128] P. v. Anvith *et al.*, "A Survey on Network Functions Virtualization for Telecom Paradigm," in *2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW)*, Tiruchirappalli, India, 2019, pp. 302-306, https://doi.org/10.1109/IMICPW.2019.8933271

[129] R.W. Crandall, J.A. Eisenach, and R.E. Litan, "Vertical Separation of Telecommunications Networks: Evidence from Five Countries," *Federal Communications Law J.*, vol. 62, 2009. [Online]. Available: https://ssrn.com/abstract=1471960

[130] F. Alvarez *et al.*, "An Edge-to-Cloud Virtualized Multimedia Service Platform for 5G Networks," *IEEE Trans. Broad.*, vol. 65, no. 2, pp. 369-380, 2019. https://doi.org/10.1109/TBC.2019.2901400

[131] P. Quoc-Viet *et al.*, "A Survey of Multi-access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," *IEEE Access*, vol. 8, pp. 116974-117017, 2020. https://doi.org/10.1109/ACCESS.2020.3001277

[132] S. Kekki *et al.*, *MEC in 5G networks.* ETSI White Paper No. 28 (2018)

[133] T. Taleb *et al.*, "On Multi-access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657-1681, third quarter 2017, https://doi.org/10.1109/COMST.2017.2705720

[134] Q.-V. Pham *et al.*, "A Survey of Multi-access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," *CoRR*, 1906.08452, 2019. [Online]. Available: https://arxiv.org/pdf/1906.08452.pdf

[135] P. v.Anvith *et al.*, "A Survey on Network Functions Virtualization for Telecom Paradigm," in*2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW)*, Tiruchirappalli, India, 2019, pp. 302-306, https://doi.org/10.1109/IMICPW.2019.8933271

[136] F. Granelli and R. Bassoli, "Autonomic Mobile Virtual Network Operators for Future Generation Networks," *IEEE Network*, vol. 32, pp. 76-84, 2018. https://doi.org/10.1109/MNET.2018.1700455

[137] M. Monshizadeh, V. Khatri, and A. Gurtov, "NFV security considerations for cloud-based mobile virtual network operators," in *2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, 2016, pp. 1-5, https://doi.org/10.1109/SOFTCOM.2016.7772161

[138] A.U. Rehman, R.L. Aguiar, and J.P. Barraca, "Network Functions Virtualization: The Long Road to Commercial Deployments," *IEEE Access*, vol. 7, pp. 60439-60464, 2019. https://doi.org/10.1109/ACCESS.2019.2915195

[139] K. Wazir *et al.*, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219-235, 2019. https://doi.org/10.1016/j.future.2019.02.050

[140] A. Banchs *et al.*, "A 5G Mobile Network Architecture to Support Vertical Industries," *IEEE Comm. Mag.*, vol. 57, pp. 38-44, 2019. https://doi.org/10.1109/MCOM.001.1900258

[141] P. Ranaweera, A.D. Jurcut, and M. Liyanage, "Realizing Multi-access Edge Computing Feasibility: Security Perspective," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, Granada, Spain, 2019, pp. 1-7, https://doi.org/10.1109/CSCN.2019.8931357

[142] O. Jude *et al.*, *Cloud and MEC security,* in *A Comprehensive Guide to 5G Security*, John Wiley & Sons 2018. https://doi.org/10.1002/9781119293071.ch16

[143] J. Zhang *et al.*, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues," *IEEE Access*, vol. 6, pp. 18209-18237, 2018. https://doi.org/10.1109/ACCESS.2018.2820162

[144] GSMA, *Smart Port MEC Security Application Based on 5G Standalone*, China Mobile and Huawei

[145] F. Reynaud *et al.*, "Attacks against Network Functions Virtualization and Software-Defined Networking: State-of-the-art," in *Workshop on Security in Virtualized Networks (Sec-Virtnet 2016)*, workshop of 2nd IEEE Conference on Network Softwarization (NetSoft 2016), Jun 2016, Seoul, South Korea, pp.471-476. https://doi.org/10.1109/NETSOFT.2016.7502487

[146] *Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points*, ETSI GS NFV-SEC 014 V3.1.1 (Apr. 2018)

[147] M. Liyanage *et al.*, "Enhancing Security of Software Defined Mobile Networks," *IEEE Access*, vol. 5, pp. 9422-9438, 2017. https://doi.org/10.1109/ACCESS.2017.2701416

[148] C.K. Agubor, G.A. Chukwudebe, and O.C. Nosiri, "Security challenges to telecommunication networks: An overview of threats and preventive strategies," in *2015 International Conference on Cyberspace (CYBER-Abuja)*, Abuja, 2015, pp. 124-129, https://doi.org/10.1109/CYBER-Abuja.2015.7360500

[149] K. Zhu and E. Hossain, "Virtualization of 5G Cellular Networks as a Hierarchical Combinatorial Auction," *IEEE Trans. Mob. Comp.*, vol. 15, no. 10, pp. 2640-2654, 2016. https://doi.org/10.1109/TMC.2015.2506578

[150] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," *IEEE Comm. Mag.*, vol. 55, no. 8, pp. 211-217, 2017. https://doi.org/10.1109/MCOM.2017.1600899

[151] P. Ranaweera, A. D. Jurcut and M. Liyanage, "Realizing Multi-access Edge Computing Feasibility: Security Perspective," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, Granada, Spain, 2019, pp. 1-7. https://doi.org/10.1109/CSCN.2019.8931357

[152] *ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Threat assessment for the fifth generation of mobile telecommunications networks (5G)*, Nov. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[153] *ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)*, Dec. 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

[154] C. Gheorghe, D. A. Stoichescu and R. Dragomir, "Latency requirement for 5G mobile communications", 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2018, pp. 1-4, https://doi.org/10.1109/ECAI.2018.8679058

[155] Y. Benchaabene, N. Boujnah and F. Zarai, "Ultra Reliable Communication : Availability Analysis in 5G Cellular Networks," 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Gold Coast, QLD, Australia, 2019, pp. 96-102,https://doi.org/10.1109/PDCAT46702.2019.00029

[156] CISA, *A Guide to Critical Infrastructure Security and Resilience*, Nov. 2019. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

[157] *Public Summary of Sector Security and Resilience Plans*, Cabinet Office, Publication date: Feb. 2019. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[158] A.M. Radu and Z. Polkowski, "Theoretical, technical and practical aspects of e-administration," *CEJSH 2014*, 2014. [Online]. Available: http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-6386268a-bf8b-443c-bfdc-8255012119bd

[159] M. Abad *et al.*, "Administration and the e-inclusion of the elderly," *Revista Latina de Comunicacion Social*, vol. 72, pp. 197-219, 2017. https://doi.org/10.4185/RLCS-2017-1161

[160] R. Davies, "Government: Using technology to improve public services and democratic participation," EPRS | European Parliamentary Research Service, (2015) PE 565.890. [Online]. Available: https://ec.europa.eu/futurium/en/system/files/ged/eprs_ida2015565890_en.pdf

[161] T.H. AlBalushi and S. Ali, "Evaluation of the quality of E-government services: Quality trend analysis," in *2015 International Conference on Information and Communication Technology Research (ICTRC)*, Abu Dhabi, pp. 226-229, 2015. https://doi.org/10.1109/ICTRC.2015.7156463

[162] T. Grimstad and P. Myrseth, "Information governance as a basis for cross-sector e-services in public administration," in *2011 International Conference on E-Business and E-Government (ICEE)*, Shanghai, China, pp. 1-4, 2011. https://doi.org/10.1109/ICEBEG.2011.5887109

[163] K.K. Smitha, T. Thomas, and K.Chitharanjan, "Cloud Based E-Governance System: A Survey," *Procedia Engineering*, vol. 38, pp. 3816-3823, 2012. https://doi.org/10.1016/j.proeng.2012.06.437

[164] S. Dasha and S.K. Panib, "E-Governance Paradigm Using Cloud Infrastructure: Benefits and Challenges," *Procedia Computer Science*, vol. 85, pp. 843-855, 2016. https://doi.org/10.1016/j.procs.2016.05.274

[165] H. El-Bakry, "Cloud Computing in E-Government: A Survey," *IJARCST*, vol. 3, no. 2, pp. 132-139, 2015.

[166] F. Danielsen, L. Flak, and A. Ronzhyn, "Cloud Computing in eGovernment: Benefits and Challenges," in *The Thirteenth International Conference on Digital Society and eGovernments (ICDS 2019)* Athens, Greece, 2019, pp. 71-77.

[167] *Compendium of Innovative E-Government Practices Volume V*, Department of Economic and Social Affairs,Division for Public Administration and Development Management, United Nations 2013, ST/ESA/PAD/SER.E/114

[168] M. Alshehri and S.J. Drew, "E-government principles: implementation, advantages and challenges," *IJEB*, vol. 9, pp. 255-270, 2011. https://doi.org/10.1504/IJEB.2011.042545

[169] S. Shareef, " ," *J. Emerging Trends in Computing and Information Sciences*, vol. 7, no. 3, pp. 139-146, 2016.

[170] M. Serban, R.-M. Stefan, E.-I. Ionescu, "Information Protection Security, Clustering and E-governance," in *21st International Economic Conference 2014, IECS 2014*, 16-17 May 2014, Sibiu, Romania

[171] A. Bettacchi, B. Re, and A. Polzonetti, "E-government and cloud: Security implementation for services,", *4th International Conference on eDemocracy & eGovernment (ICEDEG)*, Quito, 2017, pp. 79-85. https://doi.org/10.1109/ICEDEG.2017.7962516

[172] M.P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[173] A. Fath-Allah *et al.*, "E-Government Portals Best Practices: A Comprehensive Survey," *Electronic Government an International Journal*, vol.11, pp.101-132, 2014. https://doi.org/10.1504/EG.2014.063316

[174] S. Singh, "E-Governance: Information Security Issues," in *Int. Conf. Computer Science and Information Technology (ICCSIT'2011)*, pp. 120-124, Pattaya, Dec. 2011.

[175] BSI, *Information and Cyber Challenges in the Public Sector*, Survey 2018. [Online]. Available: https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-sector-cloud.pdf

[176] L. Kumari and R. Kumar, "Impact of Cyber Security in different application of e-Governance: Case Study," in *4th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2015.

[177] R.G. Hassan and O.O. Khalifa, "E-Government - an Information Security Perspective," *International Journal of Computer Trends and Technology*, vol.36, no.1, pp. 1-9, 2016. https://doi.org/10.14445/22312803/IJCTT-V36P101

[178] L. Coppolino *et al.*, "How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project," in *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Krakow, 2018, pp. 573-578, https://doi.org/10.1109/WAINA.2018.00147

[179] E. Sogut and O. Ayhan Erdem. "A Review of Research Studies on Cyber Terror," in *Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism*, A. Sari (Ed.), IGI Global, 2019, pp.179-202. https://doi.org/10.4018/978-1-5225-8976-1.ch008

[180] D2.1-5G and Vertical Services, use cases and requirements, Deliverable from 5G Programmable Infrastructure Convergingdisaggregated network and compUte Resources Project [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b838fb48&appId=PPGMS

[181] "5G in government. The future of hyperconnected public services.", A report from the Deloitte Center for Government Insights [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/6504_CGI-5G-in-govt/DI_5G-in-government.pdf

[182] M. Condoluci *et al.*, *5G IoT Industry Verticals and Network Requirements*, Jul. 2017, https://doi.org/10.4018/978-1-5225-2799-2.ch006

[183] *5G and Media & Entertainment*, White Paper, Jan. 2016. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2016/02/5G-PPP-White-Paper-on-Media-Entertainment-Vertical-Sector.pdf

[184] G. Caruso *et al.*, "Embedding 5G solutions enabling new business scenarios in Media and Entertainment Industry," in *2019 IEEE 2nd 5G World Forum (5GWF)*, Dresden, Germany, 2019, pp. 460-464. https://doi.org/10.1109/5GWF.2019.8911735

[185] P.J. Braun *et al.*, "On the Study and Deployment of Mobile Edge Application," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2017, pp. 154-159. https://doi.org/10.1109/CCNC.2017.7983098

[186] S. Pandi *et al.*, "Demonstration of Mobile Edge Cloud for Tactile Internet using a 5G Gaming Application," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas NV, 2017, pp. 607-608, https://doi.org/10.1109/CCNC.2017.7983188

[187] S. Chen *et al.*, "Distributed Computation Offloading Based on Stochastic Game in Multi-Server Mobile Edge Computing Networks," in *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Tianjin, China, 2019, pp. 77-84. https://doi.org/10.1109/SmartIoT.2019.00021

[188] J. Park *et al.*, "Design and Implementation of Platforms for Game Streaming," in *2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS)*, Casablanca, Morocco, 2019, pp. 1-6. https://doi.org/10.1109/SysCoBIoTS48768.2019.9028019

[189] R.S. Schmoll *et al.*, "Demonstration of VR / AR offloading to Mobile EdgeCloud for low latency 5G gaming application," in *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2018, pp. 1-3. https://doi.org/10.1109/CCNC.2018.8319323

[190] J. Beyer and R. Varbelow, "Stream-A-Game: An Open-SourceMobile Cloud Gaming Platform," in *2015 International Workshop on Network and Systems Support for Games (NetGames)*, Zagreb, 2015, pp. 1-3. https://doi.org/10.1109/NetGames.2015.7383002

[191] T. Zhang and C.F. Chiasserini, "TAME: An Efficient Task Allocation Algorithm for Integrated Mobile Gaming," *IEEE Systems Journal*, vol. 13, no. 2, 2019, https://doi.org/10.1109/JSYST.2018.2829496

[192] S. Zadtootaghaj, S. Schmidt, and S. Moeller, "Modeling Gaming QoE: Towards the Impact of Frame Rate and Bit Rate on Cloud Gaming," in *2018 Tenth International Conference on Quality of Multimedia Experience (QoMEX)*, Cagliari, 2018, pp. 1-6. https://doi.org/10.1109/QoMEX.2018.8463416

[193] C.R. Storck and F. Duarte-Figueiredo, "5G V2X Ecosystem Providing Entertainment on Board using mmWave Communications," in *2018 IEEE 10th Latin-American Conference on Communications (LATINCOM)*, Guadalajara, 2018, pp. 1-6, https://doi.org/10.1109/LATINCOM.2018.8613206

[194] E. Temprado *et al.*, "In-Flight Entertainment and Connectivity in the 5G Era: the 5G ESSENCE Experimental Platform," in *2019 European Conference on Networks and Communications (EuCNC)*, Valencia, Spain, 2019, pp. 241-245. https://doi.org/10.1109/EuCNC.2019.8802039

[195] T. Malkus and S. Wawak, "Information security in logistics cooperation," *Acta Logistica*, vol. 2, no. 1, pp. 9-14, 2015. https://doi.org/10.22306/al.v2i1.32

[196] European Cyber Security Organisation, *ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea*, 2020. [Online]. Available: https://ecs-org.eu/documents/publications/5fdb2791553ac.pdf

[197] 5G-PPP Software Network Working Group, *Cloud-Native and Verticals services. 5G-PPP projects analysis,* 2019, https://doi.org/10.13140/RG.2.2.23912.21763

[198] M. Alberio and G. Parladori, "Innovation in automotive: A challenge for 5G and beyond network," in *2017 International Conference of Electrical and Electronic Technologies for Automotive*, Torino, 2017, pp. 1-6. https://doi.org/10.23919/EETA.2017.7993223

[199] V. Cempirek, P. Nachtigall, and J. Siroky, "Security in Logistics," *Open Engineering*, vol. 6, pp. 637-641, 2016. https://doi.org/10.1515/eng-2016-0082

[200] "Blockchain in logistics," DHL Customer Solutions & Innovation, 2018. [Online]. Available: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

[201] D. Pristacova, "Information logistics as mean of security of competitiveness of companies," *Acta Logistica*, vol. 3, no. 3, pp. 9-13, 2016, https://doi.org/10.22306/al.v3i3.68

[202] J. Konecny, M. Jankova, and J. Dvorak, "Modelling of Processes of Logistics in Cyberspace Security," *MATEC Web Conf.*, vol. 134, 2017. https://doi.org/10.1051/matecconf/201713400025

[203] S.K. Sharma *et al.*, "Toward Tactile Internet in Beyond 5G Era: Recent Advances, Current Issues, and Future Directions," *IEEE Access*, vol. 8, pp. 56948-56991, 2020. https://doi.org/10.1109/ACCESS.2020.2980369

[204] R. Lu *et al.*, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373-389, 2020. https://doi.org/10.1109/JPROC.2019.2948302

[205] *5G Automotive Vision,* 5G PPP, 2015. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf

[206] S.K. Rao and R. Prasad, "Impact of 5G Technologies on Smart City Implementation," *Wireless Pers Commun*, vol. 100, pp. 161-176, 2018. https://doi.org/10.1007/s11277-018-5618-4

[207] B. Dzogovic *et al.*, "Enabling Smart Home with 5G Network Slicing," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, Singapore, 2019, pp. 543-548, https://doi.org/10.1109/CCOMS.2019.8821727

[208] P. Lynggaard and K.E. Skouby, "Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences," *Wireless Pers Commun*, vol. 81, pp. 1399-1413, 2015. https://doi.org/10.1007/s11277-015-2480-5

[209] D. Marabissi *et al.*, "A Real Case of Implementation of the Future 5G City," *Future Internet*, vol. 11, no. 1, p.4, 2018, https://doi.org/10.3390/fi11010004

[210] A. AlDairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," *Procedia Computer Science*, vol. 109, pp. 1086-1091, 2017. https://doi.org/10.1016/j.procs.2017.05.391

[211] M.N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-Device Communication in 5G Cellular Networks: Challenges, Solutions, and Future Directions," *IEEE Comm. Mag.*, vol. 52, no. 2, pp. 86-92, 2014. https://doi.org/10.1109/MCOM.2014.6815897

[212] Smart Cities Information System, "The making of a smart city: policy recommendations", https://smartcities-infosystem.eu/sites/www.smartcities-infosystem.eu/files/document/the_making_of_a_smart_city_-_policy_recommendations.pdf

[213] Alliance for Internet of Things Innovation, "Smart City LSP Recommendations Report", 2015,

https://aioti.eu/wp-content/uploads/2017/03/AIOTIWG08Report2015-Smart-Cities.pdf

[214] The European Parliament, 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 (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, 2016

[215] ITU Academy, "Smart Sustainable Cities: The ICT Policy & Regulatory Context"

[216] *5G Network Slicing Enabling the Smart Grid*, China Telecom, State Grid, Huawei. [Online]. Available: http://www-file.huawei.com/-/media/CORPORATE/PDF/News/5g-network-slicing-enabling-the-smart-grid.pdf

[217] Delloite, "5G smart cities whitepaper", https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology-media-telecommunications/deloitte-cn-tmt-empowering-smart-cities-with-5g-white-paper-en-200702.pdf, June 2020

[218] L. U. Khan, I. Yaqoob, N. H. Tran et al., "Edge-Computing-Enabled Smart Cities: A Comprehensive Survey", https://arxiv.org/pdf/1909.08747.pd, 12.10.2020

[219] "Industry 4.0 in agriculture: Focus on IoT aspects," *Digital Transformation Monitor*, Jul. 2017. [Online]. Available: https://ati.ec.europa.eu/reports/technology-watch/industry-40-agriculture-focus-iot-aspects

[220] M. Ayaz *et al.*, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk," *IEEE Access*, vol. 7, pp. 129551-129583, 2019. https://doi.org/10.1109/ACCESS.2019.2932609

[221] P.P. Ray, "Internet of Things for Smart Agriculture: Technologies, Practices and Future Direction," *Journal of Ambient Intelligence and Smart Environments*, vol. 9, pp. 395-420, 2017. https://doi.org/10.3233/AIS-170440

[222] M. Grady, D. Langton, and G. O'Hare, "Edge computing: A tractable model for smart agriculture," *Artificial Intelligence in Agriculture*, vol. 3, pp. 42-51, 2019. https://doi.org/10.1016/j.aiia.2019.12.001

[223] J. Mocnej *et al.*, *Network Traffic Characteristics of the IoT Application Use Cases*, 2018. [Online]. Available: https://ecs.wgtn.ac.nz/foswiki/pub/Main/TechnicalReportSeries/IoT_network_technologies_embfonts.pdf

[224] H. Santoso and R. Delima, "Stakeholder Definition for Indonesian Integrated Agriculture Information System (IAIS)," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 185, p. 012014, 2017. https://doi.org/10.1088/1757-899X/185/1/012014

[225] A. Antonaras and A. Kostopoulos, "Stakeholder Agriculture: Innovation From Farm to Store," in *Driving Agribusiness With Technology Innovations*, IGI Global 2017. https://doi.org/10.4018/978-1-5225-2107-5.ch008

[226] "Security Features of LTE-M and NB-IoT Networks," in *Mobile IoT Security Report*, GSMA, 2019. [Online]. Available: https://www.gsma.com/iot/resources/security-features-of-ltem-nbiot/

[227] C. Smilty and J. Deepu, "Security mechanisms and Vulnerabilities in LPWAN," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 396, 012027, 2018. https://doi.org/10.1088/1757-899X/396/1/012027

[228] F. Heath, *LPWA Technology Security Comparison A White Paper from Franklin Heath Ltd.*, 2017. [Online]. Available: https://fhcouk.files.wordpress.com/2017/05/lpwa-technology-security-comparison.pdf

[229] M. Pannu *et al.*, "Investigating vulnerabilities in GSM security," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, Vancouver, BC, 2015, pp. 1-7.

[230] S. Mavoungou *et al.*, "Survey on Threats and Attacks on Mobile Networks," *IEEE Access*, vol.4, pp. 4543-4572, 2016. https://doi.org/10.1109/ACCESS.2016.2601009

[231] M. Gupta *et al.*, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564-34584, 2020. https://doi.org/10.1109/ACCESS.2020.2975142

[232] *SmartM2M; Extension to SAREF; Part 6: Smart Agriculture and Food Chain Domain*, Technical Specification, ETSI TS 103 410-6 V1.1.1 (May 2019)

[233] J. Hiller *et al.*, "Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments," in *2019 IEEE 27th International Conference on Network Protocols (ICNP)*, Chicago, IL, USA, 2019, pp. 1-12. https://doi.org/10.1109/ICNP.2019.8888033

[234] P. Varga *et al.*, "5G support for Industrial IoT Applications - Challenges, Solutions, and Research gaps," *Sensors*, vol. 20, no. 3, p. 828, 2020. https://doi.org/10.3390/s20030828

[235] O. Elijah *et al.*, "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758-3773, 2018. https://doi.org/10.1109/JIOT.2018.2844296

[236] S. Farooq *et al.*, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *IEEE Access*, vol.7, pp. 156237-156271, 2019. https://doi.org/10.1109/ACCESS.2019.2949703

[237] S. Champion *et al.*, "Threats to Precision Agriculture," *2018 Public-Private Analytic Exchange Program report*, 2020. https://doi.org/10.13140/RG.2.2.20693.37600

[238] R. Chamarajnagar and A. Ashok, "Integrity Threat Identification for Distributed IoT in Precision Agriculture," in *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, Boston, MA, USA, 2019, pp. 1-9. https://doi.org/10.1109/SAHCN.2019.8824841

[239] L. Barreto and A. Amaral, "Smart Farming: Cyber Security Challenges," in *2018 International Conference on Intelligent Systems (IS)*, Funchal - Madeira, Portugal, 2018, pp. 870-876. https://doi.org/10.1109/IS.2018.8710531

[240] S. Vashi *et al.*, "Internet of Things (IoT): A vision, architectural elements, and security issues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017, pp. 492-496. https://doi.org/10.1109/I-SMAC.2017.8058399

[241] Y. Guang *et al.*, *A Telecom Perspective on the Internet of Drones: From LTE-Advanced to 5G*, 2018.

[242] 3GPP TS 22.125, *Unmanned Aerial System (UAS) support in 3GPPP*, Rel. V17.3.0 (2021-03).

[243] S. Rose, "Medical Student Education in the Time of COVID-19," *JAMA*, vol. 323, pp. 2131-2132, 2020. https://doi.org/doi:10.1001/jama.2020.5227

[244] J. Crawford, *et al.* "COVID-19: 20 countries' higher education intra-period digital pedagogy responses," *Journal of Applied Learning & Teaching*, vol. 3, no. 1, pp. 9-28, 2020. https://doi.org/10.37074/jalt.2020.3.1.7

[245] J. Daniel, "Education and the COVID 19 pandemic," *Prospects*, vol. 49, pp. 91-96, 2020. https://doi.org/10.1007/s11125-020-09464-3

[246] E. Mirzamany *et al.*, *5G and Education*, Jisc, 2019, pp. 1-6. [Online]. Available: https://community.jisc.ac.uk/sites/default/files/Education-VM_Extended.pdf

[247] H. Leligou *et al.*, "5G technologies boosting efficient mobile learning," *MATEC Web of Conferences*, Jan. 2017. https://doi.org/10.1051/matecconf/201712503004

[248] D. K. Dake and B. Adjei, "5G Enabled Technologies for Smart Education," *IJACSA*, vol. 10, no. 12, pp. 201-206, 2019. https://doi.org/10.14569/IJACSA.2019.0101228

[249] A. Barate *et al.*, "5G Technology for Augmented and Virtual Reality in Education," in *11th annual International Conference on Education and New Learning Technologies*, 2019, pp. 512-516. https://doi.org/10.36315/2019v1end116

[250] P. Sulaj *et al.*, "Design of a Training System for Mobile E-learning with the Application of E-Technology," in *16th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Stary Smokovec, 2018, pp. 533-540. https://doi.org/10.1109/ICETA.2018.8572131

[251] A. Barate *et al.*, "5G Technologu and its Applications to Music Education," in *11th International Conference on Education and New Learning Technologies*, Jul. 2019 , pp 65-72. https://doi.org/10.33965/el2019_201909F009

[252] Y.K. Ever and A.V. Rajan, "The Role of 5G Networks in the Field of MedicalSciences Education," in *IEEE 43rd Conference on Local Computer Networks Workshops (LCN Workshops)*, Chicago, IL, USA, 2018, pp. 59-63. https://doi.org/10.1109/LCNW.2018.8628579

[253] J.A. De Guzman, K. Thailalarathna, and A. Seneviratne, "Security and Privacy Approaches in Mixed Reality: A Literature Survey," *ACM Comp. Surv.*, vol. 52, no. 6, 2019, https://doi.org/10.1145/3359626

[254] F. Roesner, T. Kohno, and D. Molnar, "Security and Privacy for Augmented Reality Systems," *Comm. ACM*, vol. 57, no. 4, 2014. https://doi.org/10.1145/2580723.2580730

[255] P. Ferreira, J. Orvalho, and F. Boavida, "Security and Privacy in a Middleware for Large Scale Mobile and Pervasive Augmented Reality," in *15th International Conference on Software, Telecommu-*

nications and Computer Networks, Split-Dubrovnik, 2007, pp. 1-5. https://doi.org/10.1109/SOFTCOM.2007.4446125

[256] K. Lebeck *et al.*, "Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users," in *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, 2018, pp. 392-408. https://doi.org/10.1109/SP.2018.00051

[257] H. Elkoubaiti and R. Mrabet, "How Are Augmented and Virtual Reality Used in Smart Classrooms?," in *ICSDE'18: Proceedings of the 2nd International Conference on Smart Digital Environment*, Oct. 2018, pp. 189-196. https://doi.org/10.1145/3289100.3289131

[258] A. Gulhane *et al.*, "Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications," in *16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2019, pp. 1-9. https://doi.org/10.1109/CCNC.2019.8651847

[259] U. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in *ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2014, pp. 1054-1067. https://doi.org/10.1145/2660267.2660348

[260] C. Gentry, *A fully homomorphic encryption scheme*, Stanford University, 2009.

[261] Y. Huang *et al.*, "Faster Secure Two-Party Computation Using Garbled Circuits," in *SEC'11: Proceedings of the 20th USENIX conference on Security*, Aug. 2011. https://www.usenix.org/legacy/event/sec11/tech/full_papers/Huang.pdf

[262] E. Zarepour *et al.*, "A context-based privacy preserving framework for wearable visual life loggers," in *IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, Sydney, NSW, 2016, pp. 1-4. https://doi.org/10.1109/PERCOMW.2016.7457057

[263] P. Szczuko, "Augmented reality for privacy-sensitive visual monitoring," in *MCSS 2014: Multimedia Communications, Services and Security*, pp. 229-241. https://doi.org/10.1007/978-3-319-07569-3_19

[264] L.S. Figueiredo *et al.*, "Prepose: Privacy, Security, and Reliability for Gesture-Based Programming," *IEEE Security & Privacy*, vol. 15, no. 2, pp. 14-23, 2017. https://doi.org/10.1109/MSP.2017.44

[265] M. Eaddy *et al.*, "My own private kiosk: Privacy-preserving public displays," in *9th International Symposium on Wearable Computers*, Arlington, VA, USA, 2004, pp. 132-135. https://doi.org/10.1109/ISWC.2004.32

[266] , A.G. Forte, "EyeDecrypt - Private interactions in plain sight," in *International Conference on Security and Cryptography for Networks*, 2014, pp. 255-276. https://doi.org/10.1007/978-3-319-10879-7_15

[267] E. Gaebe *et al.*, "Looks Good To Me: Authentication for Augmented Reality," in *TrustED'16: Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, Oct. 2016, pp. 57-67. https://doi.org/10.1145/2995289.2995295

[268] l. Aslan *et al.*, "Mid-air authentication gestures: an exploration of authentication based on palm and finger motions," in *16th International Conference on Multimodal Interaction*, ACM, 2014, pp. 311-318. https://doi.org/10.1145/2663204.2663246

[269] , C.E. Rogers *et al.*, "An approach for user identification for head-mounted displays," in *ACM International Symposium on Wearable Computers*, Sep. 2015, pp. 143-146. https://doi.org/10.1145/2802083.2808391

[270] J. Chauhan *et al.*, "BreathPrint: Breathing Acoustics-based User Authentication," in *ACM International Conference on Mobile Systems, Applications, and Services*, Niagara Falls, NY, USA, 19-06-2017, pp. 278-291. https://doi.org/10.1145/3081333.3081355

[271] M. Khamis *et al.*, "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices," in *CHI Conference Extended Abstracts on Human Factors in Computing Systems*, May 2016, pp. 2156-2164. https://doi.org/10.1145/2851581.2892314

[272] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[273] G. Baldini *et al.*, "Survey of Wireless Communication Technologies for Public Safety," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 619-641, 2014. https://doi.org/10.1109/SURV.2013.082713.00034

[274] M. Mezzavilla *et al.*, "Public Safety Communications above 6 GHz: Challenges and Opportunities," *IEEE Access*, vol. 6, pp. 316-329, 2017. https://doi.org/10.1109/ACCESS.2017.2762471

[275] J.G. Oakley, *Cybersecurity for Space: Protecting the Final Frontier*, APress 2020. https://doi.org/10.1007/978-1-4842-5732-6

[276] C. Bektas *et al.*, "Reliable Software-Defined RAN Network Slicing for Mission-Critical 5G Communication Networks," in *IEEE Globecom Workshops (GC Wkshps)*, pp. 1-6, 2020. https://doi.org/10.1109/GCWkshps45667.2019.9024677

[277] Z. Kotulski *et al.*, "On end-to-end approach for slice isolation in 5G networks. Fundamental challenges," in *The Federated Conference on Computer Science and Information Systems (FedCSIS)*, Prague, Czech Republic, Sep. 3-6, 2017. https://doi.org/10.15439/2017F228

[278] *What Is an Advanced Persistent Threat (APT)?* [Online]. Available: https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html

[279] H. Mwiki *et al.*, "Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin," in D. Gritzalis, M. Theocharidou, and G. Stergiopoulos (Eds), *Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies*, Springer 2019.

[280] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

[281] "Contribution to the NIST RFI on Developing a Framework To Improve Critical Infrastructure Cybersecurity," JTC/CS1-ICT SCRM AdHoc Working Group, 2017. [Online]. Available: https://www.nist.gov/system/files/documents/2017/06/06/040813_cs1_ict_scrm_ad_hoc.pdf

[282] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos (Eds), *Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies*, Springer 2019.

[283] R. Leszczyna, *Cybersecurity in the Electricity Sector. Managing Critical Infrastructure*, Springer Nature Switzerland AG 2019. https://doi.org/10.1007/978-3-030-19538-0

[284] T. Sage, *Killing advanced threats in their tracks: an intelligent approach to attack prevention*. SANS Institute InfoSec Reading, 2014.

[285] S. Caltagirone, A. Pendergast, and C. Betz, *The diamond model of intrusion analysis*, DTIC Document, 2013.

[286] Huang L., Chen J., Zhu Q., "A Large-Scale Markov Game Approach to Dynamic Protection of Interdependent Infrastructure Networks," in: Rass S., An B., Kiekintveld C., Fang F., Schauer S. (Eds) *Decision and Game Theory for Security. GameSec 2017*. LNCS 10575. Springer, Cham 2017. https://doi.org/10.1007/978-3-319-68711-7_19

[287] E. Barka *et al.*, "Towards a trusted unmanned aerial system using blockchain (BUAS) for the protection of critical infrastructure," *Transactions on Emerging Telecommunications Technologies,* pp. 1-10. 2019. https://doi.org/10.1002/ett.3706

[288] J. Sakhnini *et al.*, "AI and Security of Critical Infrastructure," in K.K. Choo and A. Dehghantanha, (Eds), *Handbook of Big Data Privacy,* Springer, Cham 2020. https://doi.org/10.1007/978-3-030-38557-6_2

[289] M. Hoyhtya *et al.*, "Critical Communications Over Mobile Operators' Networks: 5G Use Cases Enabled by Licensed Spectrum Sharing, Network Slicing and QoS Control", *IEEE Access* vol. 6, pp. 73572-73582, 2018. https://doi.org/10.1109/ACCESS.2018.2883787

[290] *ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends*, Final ver. 1.0, Jan. 2019.

[291] *Cloud Native Threat Report: Attacks in the Wild on Container Infrastructure*, Aqua 2020. [Online]. Available: https://info.aquasec.com/cloud-native-threats

[292] REPORT ITU-R M.2410-0 *Minimum requirements related to technical performance for IMT-2020 radio interface(s)*, ITU 2017

[293] Z. Kotulski *et al.*, "5G networks: Types of isolation and their parameters in RAN and CN slices," *Computer Networks*, vol. 171, 22 April 2020, p. 107135. https://doi.org/10.1016/j.comnet.2020.107135

[294] B. Badic *et al.*, *Rolling Out 5G: Use Cases, Applications, and Technology Solutions*, Apress 2016. https://doi.org/10.1007/978-1-4842-1506-7

[295] A. Sitek and Z. Kotulski, "POS-originated transaction traces as a source of contextual information for risk management systems in EFT transactions," *EURASIP J. Inf. Sec.*, 2018, no. 5, pp.1-16, 2018. https://doi.org/10.1186/s13635-018-0076-9

[296] A. Sitek and Z. Kotulski, "Cardholder's Reputation System for Contextual Risk Management in Payment Transactions," *MMM-ACNS-2017* , LNCS 10446, pp. 158-170, Springer 2017. https://doi.org/10.1007/978-3-319-65127-9_13

[297] R. Gellens, "Next-Generation Pan-European eCall," *RFC 8147*, IETF 2017.
[298] ITU-T Y.4119 *Requirements and capability framework for IoT-based automotive emergency response system*, ITU-T 2018
[299] Z. Kotulski *et al.*, "New security architecture of access control in 5G MEC," in *8th International Symposium on Security in Computing and Communications (SSCC'20), Oct. 14-17, 2020, Chennai, India*, CCIS 1364, Springer Nature Singapore 2021. https://doi.org/10.1007/978-981-16-0422-5_6
[300] Huawei white paper, *5G Opening up New Business Opportunities,* 2016
[301] M. Geller and P. Nair, *5G Security Innovation with Cisco,* Cisco Public Whitepaper, 2018
[302] D. Loghin *et al.*, *The Disruptions of 5G on Data-driven Technologies and Applications*. [Online]. Available: https://arxiv.org/abs/1909.08096
[303] DotEcon Ltd, Axon Partners Group *Study on Implications of 5G Deployment on Future Business Models, No BEREC/2017/02/NP3,* 2018
[304] K. Samdanis and T. Taleb, "The Road beyond 5G: A Vision and Insight of the Key Technologies," *IEEE Network*, vol. 34, no. 2, pp. 135-141, 2020. https://doi.org/10.1109/MNET.001.1900228
[305] G. Gui *et al.*, "6G: Opening New Horizons for Integration of Comfort, Security and Intelligence," *IEEE Wireless Comm.*, https://doi.org/10.1109/MWC.001.1900516
[306] A. Ksentini and P.A. Frangoudis, "Toward Slicing-Enabled Multi-access Edge Computing in 5G," *IEEE Network*, vol.34, no. 2, pp. 99-105, 2020. https://doi.org/10.1109/MNET.001.1900261
[307] 5G-Transformer, *Report on vertical requirements and use cases*. [Online]. Available: http://5g-transformer.eu/wp-content/uploads/2017/12/Report_on_vertical_requirements_and_use_cases.pdf
[308] 5G PPP, *5G PPP use cases and performance evaluation models*. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5GPPPusecasesandperformanceevaluationmodeling_v1.0.pdf
[309] J. Balendonck *et al.*, *Sensors and Wireless Sensor Networks for Irrigation Management under Deficit Conditions (FLOW-AID)*, pp. 1-19, 2008. [Online]. Available: https://edepot.wur.nl/24858
[310] J. Kaur, M. A. Khan, M. Iftikhar, M. Imran and Q. Emad Ul Haq, "Machine Learning Techniques for 5G and Beyond," in IEEE Access, vol. 9, pp. 23472-23488, 2021, https://doi.org/10.1109/ACCESS.2021.3051557.

TOMASZ W. NOWAK received B.Sc. degree in 2014 and M.Sc. degree in 2015, both in telecommunications from the Warsaw University of Technology. He also received at the same faculty B.Sc. degree in electronics in 2017. He is now Ph.D. student at the Faculty of Electronics and Information Technology. His research fields are related to 5G and 5G MEC network security, network slicing with slice isolation, and cloud solutions. He has got broad experience in software development, earned both in startups and enterprise companies.

MARIUSZ SEPCZUK received Ph.D. degree in 2018 from the Warsaw University of Technology, Poland. His research interests are: authentication, Quality of Protection, Quality of Experience and context-aware systems. Moreover, he is interested in penetration tests, Security Information and Event Management, system and network security and cryptography protocols. His current research focuses on the security aspects of 5G and 5G MEC networks and the use of mimic defense concepts to protect network resources against unknown attacks.

ZBIGNIEW KOTULSKI is a Professor at the Institute of Telecommunications of the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland. He received his M.Sc. in applied mathematics from the Warsaw University of Technology and Ph.D. and D.Sc. Degrees from the Institute of Fundamental Technological Research of the Polish Academy of Sciences. Zbigniew Kotulski is the author and co-author of 5 books and over 200 research papers on applied probability, cryptographic protocols and network security.

WOJCIECH NIEWOLSKI received the M.Sc. with honors in 2014 from the Warsaw University of Technology - Faculty of Electronics and Information Technology. From 2018 he has participate in the industrial PhD program and continue education at the same faculty as a PhD student. Since 2011, he started working at Orange Labs Research and Development Centre where currently he holds position of R&D Expert. He participated in many international research and development projects connected with security, programmable networks, machine learning, cloud and edge computing which are in the area of his interest.

RALAL ARTYCH studied telecommunications at the Warsaw University of Technology and received his M.Sc. and PhD in telecommunications in 1997 and 2003, respectively. In 2004 he joined Orange Labs Poland and worked on voice core network control evolution. He is currently a senior expert in Orange Labs Poland and is working on Internet of Things, cloud computing in telecommunications and evolution towards more open and secure networks. He represented OPL in FP7 FI-PPP projects: FINSENY and FINESCE.

KRZYSZTOF BOCIANIAK received his M.Sc. degree in telecommunications at Warsaw University of Technology, Institute of Telecommunications in 2003. In 2002 he joined Polish Telecom / Research and Development Centre, currently Orange Labs Poland, and worked on voice core network control evolution. Since 2012 he is managing security research projects. His research interest includes security for 5G and IoT, network virtualization and cloud/edge computing.

TOMASZ OSKO graduated from telecommunications at the Warsaw University of Technology and continues cooperation with the university in the areas of 5G, network slicing and edge computing security. He is also supervising PhD students pursuing industrial PhD. Works in telecommunications and ICT sector for over 20 years. Currently working as a Head of Cloud Services Skill Centre in Research and Development Centre of Polish Orange Labs. He is leading the team that is involved in several Horizon 2020 project like INSPIRE-5GPlus, 5G!Drones, 5G-DRIVE and MonB5G. Continuously works on the use of results of research projects in the implementation of operator services. Since 2012 he is realizing research projects in cybersecurity area related with cloud computing, edge computing, SDN, network slicing and E2E services security.

JEAN-PHILIPPE WARY is the Research Program Director at Orange Labs (since 2011), in charge of infrastructures security research for 5G and IoT topics. 15 years at SFR (French Mobile Operator) as Security Expert and Chief Information Security Officer for Networks and Services. 5 years at Alcatel (real time, telecom, security, electronic war). Applied Mathematic Master in Stochastic Models and Statistics (Paris-Orsay).