MEC Enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures

PASIKA RANAWEERA, University College Dublin, Ireland
ANCA JURCUT, University College Dublin, Ireland
MADHUSANKA LIYANAGE, University College Dublin, Ireland and University of Oulu, Finland

The future of mobile and internet technologies are manifesting advancements beyond the existing scope of science. The concepts of automated driving, augmented-reality, and machine-type-communication are quite sophisticated; and requires an elevation of the current mobile infrastructure for launching. The 5G mobile technology serves as the solution; though lacks a proximate networking infrastructure to satisfy the service guarantees. Multi-Access Edge Computing envisage such an edge computing platform. In this survey, we are revealing security vulnerabilities of key 5G based use cases deployed in the MEC context. Probable security flows of each case are specified, while countermeasures are proposed for mitigating them.

CCS Concepts: • **Human-centered computing** → *Ubiquitous and mobile computing*; • **Security and privacy**; • **General and reference** → **Surveys and overviews**; • **Computer systems organization** → **Cloud computing**;

Additional Key Words and Phrases: 5G, use cases, MEC, Security, ITS, V2E, AR, VR, UAV, mMTC, eMBB

ACM Reference Format:
Pasika Ranaweera, Anca Jurcut, and Madhusanka Liyanage. 2021. MEC Enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. 1, 1 (July 2021), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Moore's Law suggests the processor speed is exponentially incrementing over time [13, 88]. Hence, the number of Internet of Things (IoT) devices employed at industries serving Big Data applications are thriving with the possibility of proliferated processing capability in miniaturized devices. Moreover, improved smart device usage literacy of general public in modern era are enabling the social internet platforms to launch cumbersome bandwidth consuming applications for elevating their subscriptions with immersive Quality of Service (QoS). It is estimated that the number of mobile terminals are reaching 2.8 billion by 2019 and monthly mobile data traffic is reaching beyond 49 exabytes by 2021 according to Cisco [117]. Thus, deployments of billions of smart devices demand access capacity and bandwidth requirement from the access interfaces of mobile base stations.

The fifth-generation (5G) mobile technology is the seminal advancement explored by the Mobile Network Operators (MNOs) to reach beyond the constrictions of the prevailing network architecture. To achieve the novel requirements of enhanced performance, portability, interoperability, elasticity, reliability, spectral and energy efficiency; a network softwarization approach should be followed by the evolving mobile networks [64]. Virtualization, service migration,

Authors' addresses: Pasika Ranaweera, University College Dublin, Dublin, Ireland, pasika.ranaweera@ucdconnect.ie; Anca Jurcut, University College Dublin, Dublin, Ireland, anca.jurcut@ucd.ie; Madhusanka Liyanage, University College Dublin, Dublin, Ireland, madhusanka@ucd.ie, University of Oulu, Oulu, Finland, madhusanka.liyanage@oulu.fi.

orchestration, and service automation (as in service function chaining [50]) are the main phases of paving the path towards 5G and beyond 5G mobile paradigms[25]. As the core and backhaul portions of the emerging mobile networks are softwarized; techniques of ultra-dense networks, massive Multiple-Input-Multiple-Output (MIMO), and high-frequency communication are prominent methods for improving the wireless access network [117]. Due to these technological improvements, 5G guarantees a 1000 times enhancement of the capacity than its predecessor.

Even with the softwarized 5G core network, facilitating the diverse requirements demanded by the IoT based devices is still a predicament due to the drawbacks of existing service provisioning infrastructure[26]. Conventional cloud computing architecture fails to provision emerging myriads of services [81]. The geographically distant placement of data centres and limited access capacity contrives unintended delays and jitters that compromise the entire service infrastructure. Moreover, cloud servers are incapable of servicing billions of IoT devices ubiquitously. These limitations in cloud computing paradigm enforce vulnerabilities that can be exploitable by adversaries [130]. Moreover, privacy is a major concern with the outsourcing based cloud computing service models [43]. Most cloud service providers are violating the locational and data privacy of their consumers.

In order to overcome these constrictions in storage and processing service models, Edge Computing (EC) as a paradigm was introduced in 1990s with Content Delivery Networks (CDN) that decentralized the data centre functions [140]. Main objective of EC was to extend the functions offered from cloud computing to the edge of the mobile network [104]. With in-proximity dispensing of cloud functions at the edge, drawbacks of the cloud paradigm could be mitigated. In fact, this architectural paradigm shift is the raison d'etre for 5G and beyond 5G based concepts to achieve the guaranteed performance metrics. There are various flavours of edge concepts introduced for expanding this notion. Multi-Access Edge Computing (MEC), Fog computing, Mobile Cloud Computing (MCC), Cloudlets, and Transparent Computing (TC) are such directives followed by research communities [104, 117]. Out of these concepts however, MEC and fog computing are leading to be adopted pragmatically and in terms of standardization. In this survey, we are investigating the MEC paradigm as its standardization is much more convincing than the other concepts.

1.1 Related Surveys

There are several research studies that focus on MEC, 5G, and various approaches related to the deployment of these aspects, including security. Ren et al. in [117] explores the orchestration mechanisms within end-edge-cloud context for fog, MEC, TC, and cloudlets. Different edge flavours are contrasted with an evaluation criteria; that sets the criterion indices based on heterogeneity support, QoS requirements, elastic scalability, mobility, and interoperability. Moreover, computational offloading, caching, security, privacy, and future research directions are discussed further. In [115], a comprehensive survey is conducted on service migration scenarios for edge computing paradigms. The diversity among the existing migration schemes are highlighted while architectures, platforms, and implementations related to migration are presented further. Moreover, future research directions are presented considering the gaps identified in the literature. Li et al. in [78] reviews the edge oriented computing systems focusing on their architectural features, resource management approaches, and design objectives. Though, the investigation is more concentrated on fog computing than other EC paradigms. The adaptation of Distributed Ledger Technologies (DLTs) on IoT based applications have been studied in [157]. IoT use cases of smart home, smart transport, supply chain, smart healthcare, and smart energy are described in the applicable DLT platform context. Offloading is a vital consideration for EC scenarios. Thus, a survey is conducted on offloading algorithms in [139] for edge and cloud deployments. The surveys in [39] and [142] discuss Network Function Virtualization (NFV), Software Defined Networks (SDN), Service Function Chaining (SFC), and Network Slicing (NS) as MEC enablers; where focus on security is not comprehensive.

Ferrer et al. in [38] presents a concise comparison between MCC, Mobile Ad hoc Computing, and EC to emphasize the novel aspects of decentralized cloud approaches. Reliable resource provisioning problem with edge-cloud computing environments is addressed in [29]. More emphasis is drawn to the machine learning as a solution for workload characterization, workload prediction, component placement, system consolidation, and application elasticity aspects of prevailing resource provisioning approaches. Knowledge on IoT based communication protocols such as Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), Hypertext Transfer Protocol (HTTP), and Constrained Application Protocol (CoAP) are imperative for realizing the formation of 5G based use cases. A comprehensive survey is conducted in [27] on such IoT protocols emphasizing their characteristics, and performance issues in the context of fog and cloud computing integration.

Khan et al. in [64] addresses security and privacy advancements of 5G in the viewpoint of novel technologies of SDN, NFV, NS, and MEC. This survey has investigated the Physical Layer Security (PLS), security monitoring and management, privacy, and security standardization aspects of 5G to a comprehensive extent. Though, 5G based use cases are not considered in their scope. Ranaweera et al. in [110, 111] present a comprehensive inductive research on MEC security and privacy aspects, considering real-world MEC deployment scenarios accustoming to the ETSI standardization. Despite their holistic nature, their work does not focus on the 5G use cases that this article is introducing. The use cases of industrial automation, Intelligent Transport Systems (ITSs), Virtual Reality (VR), smart girds, e-health, and education are considered in [100] on the latency requirement perspective. Though this survey states the latency requirements of each use case, their security issues and prospects on edge computing has not been addressed.

1.2 Scope and Contribution

In this survey, we are exploring the security vulnerabilities of 5G use cases deployed in accordance to MEC based scenarios. The use cases of critical infrastructure based services, enhanced Mobile Broadband (eMBB), massive Machine Type Communication (mMTC), Autonomous driving/ Vehicle-to-Vehicle (V2V) connections, Augmented Reality (AR)/ Virtual Reality (VR)/ Mixed Reality (MR), and Unmanned Aerial Vehicles (UAVs) are investigated for security vulnerabilities. Further, prevailing security solutions are mapped as solutions and countermeasures for each use case. This is the main contribution of this research as current literature lacks the discussion of security in 5G enabled edge computing based deployments. Understanding the progress of state-of-the-art industrial and academic projects in 5G and MEC are vital to realize the adaptation of the scoped use cases. Thus, this paper presents a holistic overview of leading projects.

1.3 Paper Organization

The rest of the paper is organized into 5 sections. Section 2 presents the background on 5G, MEC, and role of MEC in 5G. Core contribution of this research is contained in Section 3, where use cases are investigated for their security issues and usable solutions. Section 4 summarizes the details on current research groups and institutions proceeding in MEC and 5G focused security developments. Insights gained from this survey are discussed in Section 5, while probable novel applications and challenges for wide adoption of 5G are presented briefly. Finally, Section 6 concludes the paper.

2 BACKGROUND

Despite that 5G and MEC can be operable independently, the integration of them would enable applications and use cases with requirements of Ultra-Reliable Low Latency Communication (URLLC) capabilities in addition to improved security and privacy aspects [39]. Thus, assimilation of 5G and MEC standardization is imperative to realize the context of this paper. The following section describes the key information on 5G, MEC, and the role of MEC in 5G.

2.1 5G

The data rates of 1 ∼ 10 Gbps, 1 ms round trip latency, enhanced capacity for plethora of connecting devices through high bandwidth channels, perceived availability of 99.999%, 100% ubiquitous connectivity, improving battery life through 90% energy reduction are major requirements for 5G in the performance perspective [2]. The softwarization of the 5G core enables the segmentation of functions to a layered architecture with its featured flexibility. The Fifth Generation Infrastructure Public Private Partnership (5G-PPP) project proposes the five layers of infrastructure, network/ control, orchestration, business, and services for forming the 5G functional architecture [42]. The orchestration layer however, is a dispersed function among other layers while services layer can be represented as an extension of the business layer [64]. The infrastructure layer represents the RAN connectivity portion of the mobile network. The Radio Access Technologies (RATs) employed in the 5G infrastructure layer are supporting Non-Orthogonal Multiple Access (NOMA), massive Multiple-Input-Multiple-Output (MIMO), Coordinated Multi-Point (CoMP) transmission, and millimeter Wave (mmWave) technologies [14, 33]. Control layer inhibits the network management function while network and business services are assigned to the business layer.

Security measures targeted for ensuring confidentiality, integrity, availability, accountability, authentication and authorization aspects were implemented with predecessor mobile networks ranging from 2G to Long Term Evolution (LTE). Though, Information Assurance (IA) policies has become most profound for 5G and beyond networks with the requisite to assure the content in processing, usage, and transmission in the cyber space [121]. Encryption is the key security mechanism to ensure security in mobile networks. Encryption schemes of A3, A5/2, A5/3, A8, Kasumi, SNOW-3G, and Evolved Packet System (EPS) Encryption Algorithm (EEA) along with EPS Integrity Algorithm (EIA) were such methods employed for confidentiality and integrity protection [64, 81]. Moreover, TS 23.122 and TS 33.210 specifications are defining the Access Stratum (AS) and Non-Access Stratum (NAS) security functions of the 3rd Generation Partnership Project (3GPP) based mobile deployments [73]. AS and NAS are functional layers of the Universal Mobile Telecommunications System (UMTS) and LTE protocol stack. Though, novel mobile network deployments require the allowance to be dynamically customized in accordance to the specifications of impending use cases and applications [3]. Thus, architectural amendments in 5G do not permit the utilization of security measures employed for pre-5G networks [61]. In addition, flash crowd network traffic demand, radio interface security, user plane integrity, roaming, Denial of Service (DoS) or saturation attacks, and signalling storms are identified as novel challenges for 5G mobile networks [4]. The heterogeneous nature of 5G enabled devices empowered with IoT technologies are envisaging massive scalability with cross-platform issues. Introducing novel services and applications are imminent to attract enormous amount of subscribers; hence contriving a flash crowd demand (unintended surge in subscribers) situation in the mobile network. Such situations are exploitable by capable adversaries to overload both application and radio interfaces that mimic a DoS effect[83]. Further, DoS or Distributed DoS (DDoS) attacks pose a service interruption risk for latency sensitive 5G applications via impeding the service with continuous malicious accessing attempts. Similar effect is expected from signalling storms, by generating massive amount of signalling traffic in the control plane; access granted by the intruder from a signalling attack perpetrated at the 5G interfaces. As 5G core network components such as User Plane Function (UPF) are deployed in line with the edge/ user level, such signalling storms could sabotage the entire mobile domain [66]. The heightened mobility with 5G devices incur roaming, handover, and migration situations more frequent. Thus, timing based interposing attacks are imminent on such control channels, channel assignments, and migration sessions [134]. In addition, malicious User Equipment (UE) and fake BSs launching masquerading attempts resulting in wormhole, or sinkhole effects are imminent in the user plane [11, 62, 111]. Thus, integrity and authenticity of the user plane is paramount for 5G. Solutions such as Host Identity Protocol (HIP) schemes, mandating global visibility for security policies, Cloud RAN (C-RAN) and EC, isolation of Virtual Network Functions (VNFs) are adaptable for meeting the security requirements [3, 82, 135]. More details on 5G security can be assimilated from [12, 30, 37, 40, 51, 81, 144].

2.2 Multi-access Edge Computing (MEC)

In contrast to other edge computing paradigms, MEC edge infrastructure is proposed to be deployed at the Radio Network Controller (RNC), or the Base Station (BS), or gNodeB (gNB) in 5G terms [104]. Thus, its reliance on MNOs service quality is higher than the other paradigms. The ETSI defined MEC architecture is formed with two levels that are deployed along with the BS and the mobile core network entities referred as the edge/ host level and the system level respectively [35]. These two levels are segmenting the functions of service registration and service provisioning for improved access and security. Isolating the orchestration function of the entire system from the edge infrastructure, mitigates the possibilities of holistic system compromise through intrusions. Moreover, an edge infrastructure operating unburdened by the service registration processes would serve with improved mobility, scalability, availability, and context awareness [119]. In addition, an edge infrastructure capable of operating standalone or with cloud connectivity, envisages a very low latency and jitter for enhanced service access [152]. These features of MEC enable the compatibility and adaptability for IoT based services facilitated with the edge domain [118]. However, these novel structures and virtualization technologies employed for deploying a dynamic service environment are creating unprecedented issues in security and privacy context.

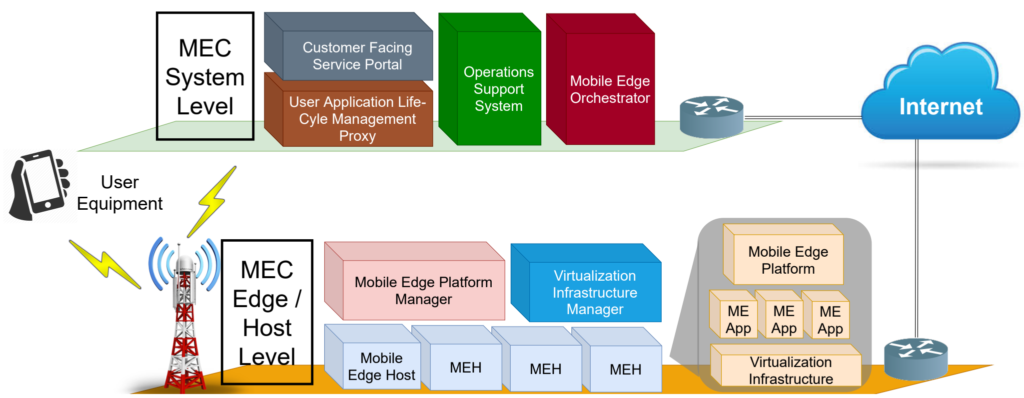

Fig. 1. MEC Operation and Structure

The MEC operational structure depicted in Fig. 1 represents the various entities defined by the ETSI for accomplishing classified tasks at the edge and the core [110]. The functions approving, rejecting, and managing service requests are handled by the entities of User Application Life-Cycle Management Proxy (UALCMP), Customer Facing Service Portal (CFSP), and Operations Support System (OSS) at the core. Mobile Edge Orchestrator (MEO) is orchestrating the entire MEC system under its domain. The edge system is governed by Mobile Edge Platform Manager (MEPM) while Virtualization Infrastructure Manager (VIM) is acting as the hypervisor for the edge environment. Mobile Edge Hosts (MEHs) are virtual entities that are configured for the subscriber service requirements; which perpetrates the actual storage and processing operations in the MEC system. Service instances instigated by the User Equipment Applications

(UE Apps) are interacting with its counterpart at a particular MEH called Mobile Edge Application (ME App). Mobile Edge Platform (MEP) is managing the resources and networking within a MEH.

MEC is built on top of the driving technologies SDN, NFV, Information Centric Networking (ICN), NS, and IoT [84, 104]. Thus, implementing security for heterogeneous services overlaid on top of the diverse driving technologies of the MEC is an intricate task. Moreover, extended access capacity at the edge with wireless channels and mobile offloading/ delegation schemes are elevating the probable penetrative and vulnerable vectors in the edge network that would be subjected for exploitation by the adversaries [52]. Thus, revealing vulnerabilities and threats in 5G based MEC deployments should be handled case-by-case for each probable use case of 5G.

2.3 Role of MEC in 5G

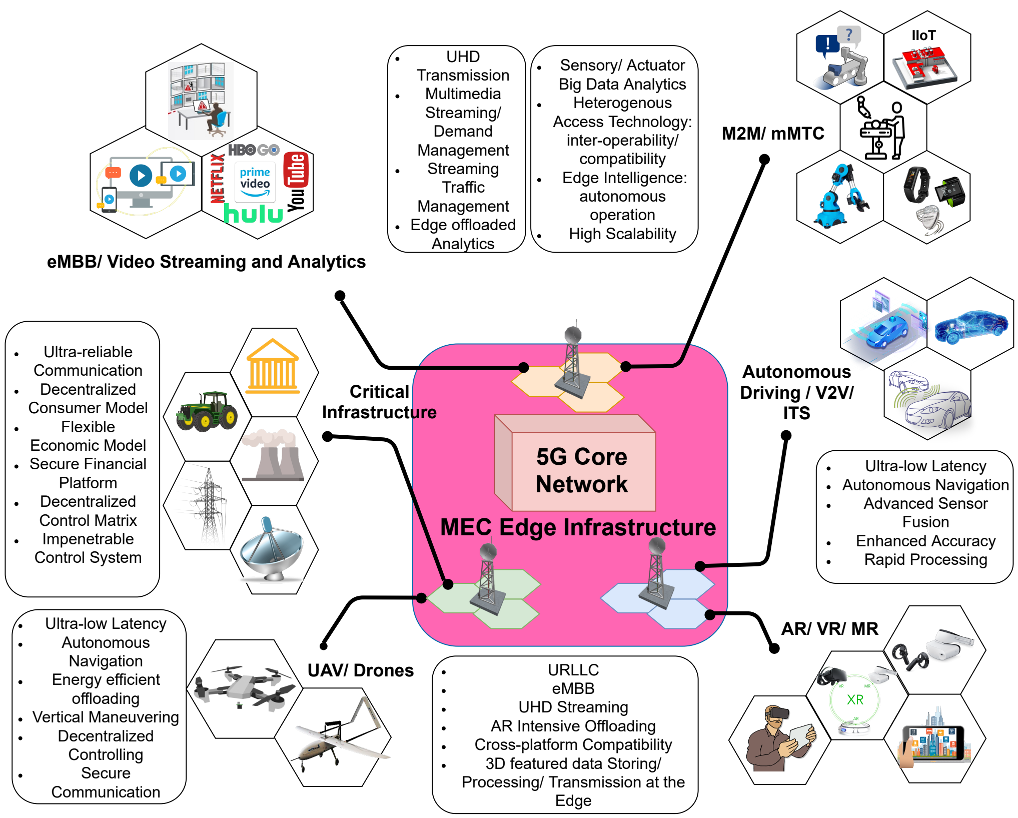

Fig. 2. MEC enabled 5G based use cases

MEC plays a key role in realizing the envisaged use cases of 5G. Six use cases, as depicted in Fig. 2, are elaborated in section 3 for stating the investigated security vulnerabilities in MEC enabled scenarios. As these use cases are offered as services to the 5G consumers, service quality in terms of QoS and Quality of Experience (QoE) are key factors for service continuity that eventually decides the pricing /charge of the particular service [22]. Thus, 5G core network deployment itself cannot ensure the required service quality from these impending applications due to limitations of access network. As discussed above, MEC and other edge computing paradigms facilitate the infrastructure for enhancing the access interfaces to cater ultra-low latency, real-time ubiquity, security, and privacy aspects of the mobile network[83]. Though, managing the diverse services that demand various requirements (i.e. low latency is critical for UAV and V2V applications while reliability, QoS, and QoE are required for eMBB and AR use cases) is a challenge for MNOs. Network Slicing is a concept identified for achieving this purpose maintaining the QoS and QoE levels specified by each service [151]. MEC supports the multi-domain globally dispersed services through sliced network deployments for heterogeneous applications and services [58]. ETSI defined MEC edge platform allows dynamic launching of service instances configurable for required specifications. Thus, network slice instances can be launched as ME Apps at MEC host level to enable multi-slice deployments.

3 SECURITY OF MEC USE CASES

In this section, use cases and applications of MEC are considered. For different MEC applications, security vulnerabilities are investigated while possible countermeasures are presented from the existing literature.

3.1 Critical Infrastructure

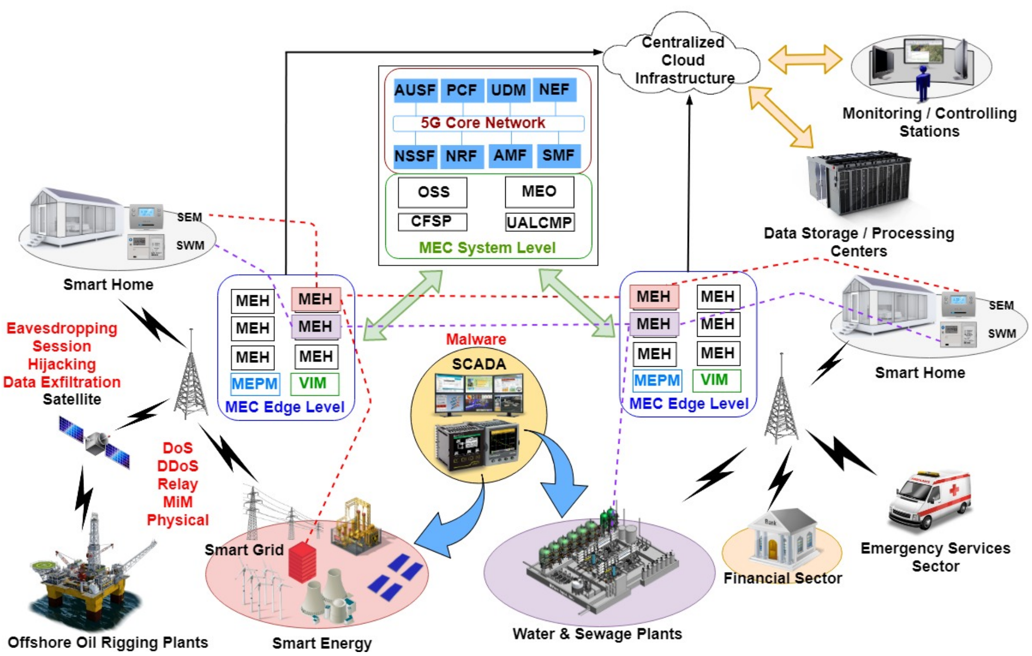

Fig. 3. Critical Infrastructure Connectivity to MEC Platform

Critical Infrastructure based services such as energy, water and sewage, offshore oil drilling rigs, financial, and emergency applications have expanded their scope through digitizing their controlling systems with IoT technology. Even industrial sectors are revolutionizing their deployments with novel technologies to cope with the rapid development[133]. Though global expansion of these services to dispersed global clusters constricts the usability of a centralized data centre for storage and processing. Thus, integrating MEC platforms for critical infrastructure services are probable and would improve the interfacing of the general public towards the services as critical customer status updating of billing, consumer usage, and service interruption notifications.

The energy sector holds the profound significance out of infrastructure services as it energizes all the other sectors and envisages a sophisticated deployment options with the evolution of smart grid technology. The integration of IoT based technologies enables the formation of Advanced Metering Infrastructure (AMI) / smart metering / net metering that overlay a monitoring framework for the smart energy solution [62]. In addition, the incorporation of renewable energy sources demands a decentralized deployment of power coordinating entities (smart grids) that enforce bi-directional energy flow through the transmission grids [8]. Thus, employing an effective power utilization scheme is an intrinsic requirement and achievable through system status analytics on consumer consumption, consistency of the generation, grid utilization and performance of the operating devices. The consumers are granted the opportunity to utilize their household utility spending by monitoring the IoT interfacing tools which facilitate the visualization of any incoherent consumption patterns. The coordinated group of European Committee for Standardization - European Committee for Electrotechnical Standardization - European Telecommunications Standards Institute (CEN-CENELEC-ETSI) proposed a Smart Grid Architectural Model (SGAM) for realizing smart energy use cases [76]. Proposed architecture formulates three dimensions that concatenate five functional interoperability layers with energy sector domains and zones which accounts for power system management. Thus, the amalgamation of IoT technologies with electro technical devices is reinforced from this proposal for achieving the ultimate integration of IoT and energy solutions. Moreover, decentralized nature of smart grids in the energy network and the requirement for minimizing the latency for critical parameter transmission demands the deployment of MEC. Subscribing MEC services for SCADA based smart grids enable the connectivity among them across the network for establishing a monitoring and awareness channel to maintain a balanced energy flow [1]. This approach is capable of alleviating the cost to improve the grid utilization. The consumer interfacing and remote activation/ deactivation of household electrical apparatus is probable from MEC based ME Apps that interconnect the smart grids to the Smart Energy Meters (SEMs).

In an era of urbanization, water and sewage treatment is a paramount necessity for achieving sustainable development facilitated through improved urban sanitation and quality of human life [147]. MEC plays a key role in optimizing the existing water governance techniques that are attributing complexities due to diversified cost structures formed by origin of water sources and environmental externalities [91]. One of the most obvious use case for MEC is the deployment of smart metering infrastructure embedded with Smart Water Meters (SWMs) resembling the AMI setup as indicated in Fig. 3. MEC edge servers or MEHs are responsible for facilitating a low latency communication platform between consumer end, water treatment plant and the central monitoring station. Moreover, sensory inclusions in an automated treatment plant act as a MTC application that is capable of calibrating the control mechanisms to achieve utilized water governance. However, current water treatment plants employ SCADA systems for controlling the fluid flow through processes such as debris removal, filtration, recarbination, flocculation, coagulation and chlorination. Enhanced MTC (eMTC) solutions to establishing communication channels are guaranteed through LTE PHY layer for SCADA deployments such as in Remote Terminal Units (RTUs) that operate at different controlling structures [24].

Petroleum extraction is a vital industry that caters the fossil fuels which generate combustible energy for energizing vehicular engines and electricity generating plants throughout the globe. The continuous extraction has led to the scarcity of natural resources that forced the petroleum industry to shift the drilling process to the offshore reservoirs where the aquatic resources are still intact [59]. Thus, offshore plants are intrinsic requisites for petroleum industry despite the precarious conditions granted to the employees. Automation is an approach to be considered for entrusting the safety of employees at offshore plants. Magnitude of the power dissipation at the heavy machinery demands the employment of SCADA systems for controlling them. Deploying MEC for expanding the scope and alleviating the latency for oil drilling services improves the probability of launching eMTC based operating infrastructure at offshore plants. This enables the remote automated operation of drilling devices which are linked through satellite communication for mitigating human casualties probable at a plant malfunctioning.

Any service infrastructure that utilizes a communication network at its formation is prone to significant security threats. In 2015, the National Cyber-security and Communication Integration Centre – Industrial Control Systems Cyber Emergency Response Team (NCCIC/ICS-CERT) witnessed that the attacks on critical infrastructure have steadily increased over the years [70]. Thus, investigating threats applicable for these application scenarios are critical. Fig. 3 depicts the various critical infrastructure based services and their connections to the MEC serviceable platform.

3.1.1 Security Vulnerabilities. If we remain with the assumption of internal connectivity of these critical infrastructure facilities are secured by design, their bi directional connectivity with the BS could be the only vector to be considered for penetration by malicious adversaries. The threats to such connectivity would resemble any intrusion based, intervention, DoS or Distributed DoS (DDoS) attacks; which are capable of ceasing ME Apps launched in the edge from accessing the relevant infrastructure services. Due to the higher scale of the applications, the MEC edge level entities should have to subscribe more than one MEH and the geo-distributed nature would link more than one MEC edge levels or system levels for a particular critical infrastructure based service. This fact improves the possibility of prone to be attacked or infected by a malicious agent through the MEC server side.

The dispersed deployment of SEMs across households in an AMI based smart grid installation encourages the adversaries to launch interposing attacks such as eavesdropping, modifying and interrupting in the wireless communication channels additionally to the physical damages effectuated in close proximity [94]. Moreover, Sleep Deprivation Torture (SDT) and Battery Exhaustion Attacks (BEA) are probable in smart grid environments [44]. Similar affect is imposed on SWM installations in a smart water governance scenario. However, the nature of attacks is dependent on the deployment scenario of the critical infrastructure application.

As the core functions of the discussed critical infrastructure based applications are facilitated through the SCADA systems, the internal security vulnerabilities are common for all cases. The isolated and disconnected nature of SCADA based systems advocated resilience against cyber-attacks in the past [18]. However, threats and vulnerabilities were detected with SCADA systems as in the case of the popular worm STUXNET that raised the probability of critical infrastructure services being vulnerable [93]. Moreover, penetration on the sewage system in Maroochi (Australia), BlackEnergy Trojan which targeted a Ukrainian power grid, HAVEX malware and command injection attack on water treatment plant in Kemuri are exemplifying the compromised SCADA systems [72, 128]. The communication of the SCADA installations is attained by Modbus, DNP3 and Profibus protocols [128]. Cyber-attacks probable on Programmable Logic Controllers (PLCs) are categorized into Reconnaissance, command injection, response injection and DoS attacks [72]. In that scenario, MEC system would be infiltrated from the critical infrastructure direction. As an example, the distributed nature of smart grids would allow an infiltrated smart grid to unbalance the energy load by feeding misleading information to the edge entities that could lead to catastrophic circumstances.

The connectivity of the critical infrastructure nodes with the BS in the proximity should be secured with extensive cryptographic means due to their criticality and inherent resources. The priority for communication protocol would be the secureness in spite of latency and bandwidth usage. Though the security measures to be adopted internally are different from one application to another.

3.1.2 Existing Solutions. Yang et al. in [147] proposed a model for a smart sewage plant operating on intelligent and picturesque SCADA system where sensory devices are employed for conveying monitoring statistics to the intelligent control systems. A high speed and reliable networking platform is formulated to maintain the connectivity between the

SCADA based control system and the sensing devices. Features such as Real time regulation for optimizing, intelligent decision making, efficient security analysis, self-healing/ correction, superior effluent quality, humanized and visualized inter-operable platform are the intended objectives of the proposed model.SWMs are used to measure the consumer water consumption while updating the central monitoring stations as illustrated in Fig. 3. As malware are definite threats to SCADA systems, the approach instated by Shirazi et al. in [128] for detecting anomalies in SCADA systems employing machine learning techniques is a prominent solution. The K-Means and Naive Bayes are configured in their supervised mode while Principle Component Analysis using Singular Value Decomposition (PCA-SVD) and Gaussian Mixture Model (GMM) techniques are configured to their unsupervised mode. The precision values of the machine learning techniques are evaluated against naive and complex response injections, malicious state/ parameter and function command injections, DoS, and reconnaissance anomalies methods in a gas pipeline simulation model[103, 131]. In addition, as Virtual Network Functions (VNFs) are imminent to be deployed in edge infrastructure in line with SCADA systems, cryptographic means to support VNF isolation and shielding for security critical function over less critical functions are important in the context of MEC [11].

Hussain et al. in [59] introduced an edge computing based resource allocation model to utilize the existing cloud data centre based latency prone systems which communicated through satellites. Task scheduling policies such as First Come First Server (FCFS) and Shortest Job First (SJF) are considered for remote operations controlled at the edge level through a VM based coordinator to minimize the reliance on onshore distant resources. Proposed heuristics are analysed for various workload conditions.

Leligou et al. in [75] proposed a framework that comprised the four layers: energy layer, telecommunication layer, VNF layer and the application layer. The framework is employing MEC as an expanded Multi Radio Access Technology (RAT) xMEC deployment for enabling offloading where blockchain based VNF Descriptors (VNFD) are acting as process tags to achieve traceability in the energy layer. However, the deployment scenario for xMEC offloading is not convincingly explicated to validate the applicability of the framework for smart grids.

Saez et al. in [122] propose a framework called System-level Manufacturing and Automation Research Test-bed (SMART) that is controlled through PLC over an IP network engaging the OPC UA protocol in diagnosing and detecting anomalies in the data extracted from the data sourcing devices: CNCs, RFID sensors, cameras, and conveyors. According to the data processing framework; data transforming, analyzing, storing and image processing tasks are conducted at the edge servers for enhancing the efficiency of the smart system. Thus, probable integrating scenarios with different PLC based technologies validate the deployment as a critical infrastructure solution.

Experimental setup was orchestrated by Oyekanlu et al. in [97] for determining channel capacity in an edge computing scenario to evaluate the performance of various IoT devices. The channel capacities in terms of SNR for edge computing use cases: smar grids (for periodic, non-periodic, and synchronized phasor management units) and IIoT are formulated assuming wired transmission channels. The results of this conduct are influential for manufacturers in spite of lesser number of loads been considered.

The blockchain model proposed by Gai et al. in [44] were focusing on energy security in smart grid environments. The intended objective of the system is to detect improper energy usage patterns to prevent probable energy related attacks such as SDT and BEA. Blockchain technique is applied to form a network resembling a Smart Grid Network (SGN) that is capable of achieving optimal resource management.

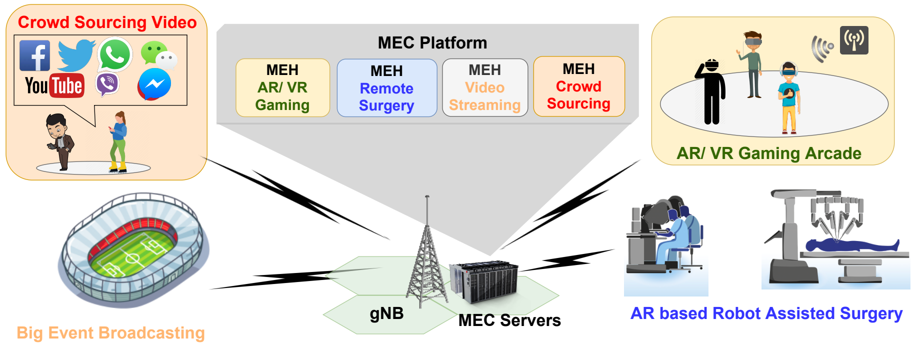

Fig. 4. AR and Video Streaming Applications with MEC

3.2 Enhanced mobile broadband channels/ Video Streaming and Analytics/ big events

Video stream analysis based applications such as vehicular license plate recognition, face recognition and domestic surveillance which require high computational complexity for their algorithms to be reliant on UHD transmissions [88][1]. Mobile gaming applications based on VR and AR integration are probable deployments for high level video streaming UHD channels that endanger the bandwidth provisioned for priority services. Cisco predicts that the share of mobile video streaming would be increased rapidly while the bandwidth saving approaches to Over the Top (OTT) streaming channels are identified as intrinsic preliminaries to form multimedia channels [87]. The crowd sourcing based media are uploaded into the servers through multimedia channels precipitately as in; 72 hours of video content uploaded to YouTube, 2.4 million pieces uploaded to Facebook, 347,000 and 216,000 images uploaded into WhatsApp and Instagram in a minute [16]. Moreover, consumer bandwidth has extended from single view to multi-view, 2D to 3D, and single source stream representation to adaptive multi-bit-rate multi-resolution representation. Thus, necessity to implement measures for utilizing the bandwidth from OTT streaming services is a manifesting predicament. There are two scenarios where the video streaming applications are deployed. Peer-to-peer (P2P) streaming traffic routed from an eNodeB serviced by a MEC edge level platform is conveyed to a UE directly that would save the backbone capacity and traffic of the network operator. In case of big event streaming, the streams are digested at a MEC host service subscribed by a local video production studio that would convey the streams to the UEs. This approach however, could be subjected to amendments by the video editors. Fig. 4 is representing various AR and video streaming based services that are capable of deploying under a MEC service infrastructure.

3.2.1 Security Vulnerabilities. A confiscated video stream is probable for embezzlement by the attackers for distilling counterfeited credentials that would violate the integrity of the content [70]. A news feed manipulations result in misleading circumstances for the viewers and would be critical depending on the entropy of the information. As most video streaming traffic are generated from crowd-sourcing applications, an infected UE poses the threat of multi-casting malicious content acting as an egress point through the video streaming channels. The majority of the social media and crowd-sourcing accounts are not equipped with strong password based credentials. Thus, phishing type attacks are capable of commandeering such accounts that violate integrity. Video streaming channels however, is encoded with an acceptable level of encryption. It makes the interposing attacks less probable. As streaming content are stored and processed in MEHs, malicious agents could be conveyed via UEs engaged in various applications mentioned above.

This type of attack results in compromising the edge infrastructure. Moreover, an infected ME App that processes the streaming content is capable of convincing the MEP and VIM to allocate unnecessary resources to exhaust the system.

3.2.2 Existing Solutions. Makinen in [87] proposed a business model for video streaming in events handling incorporating MEC service platforms. The business model is analysed in terms of service, technology, organization, and finance designs for P2P and big event streaming scenarios. Bilal et al. in [16] presented solutions for interactive multi-view streaming and gaming communities incorporating edge computing deployments. Interactive multi-view/ free-view video, video stream transcoding, and cloud gaming scenarios are considered for identifying edge technologies that involve techniques such as Muti-view Video Coding (MVC), Interactive Multi-view Video Streaming (IMVS), Content Delivery Networks (CDNs), and Adaptive Bitrate Streaming (ABR). Ren et al. in [116] investigated the latency minimization problem in a multi-user time-division multiple access Mobile Edge Computing Offloading (MECO) system. Three computation models: local compression, edge cloud compression, and partial compression offloading are formulated for optimizing video compression mechanisms analogous to video streaming deployments.

3.3 Machine to Machine (M2M) and massive Machine Type Communication (mMTC) links in IoT

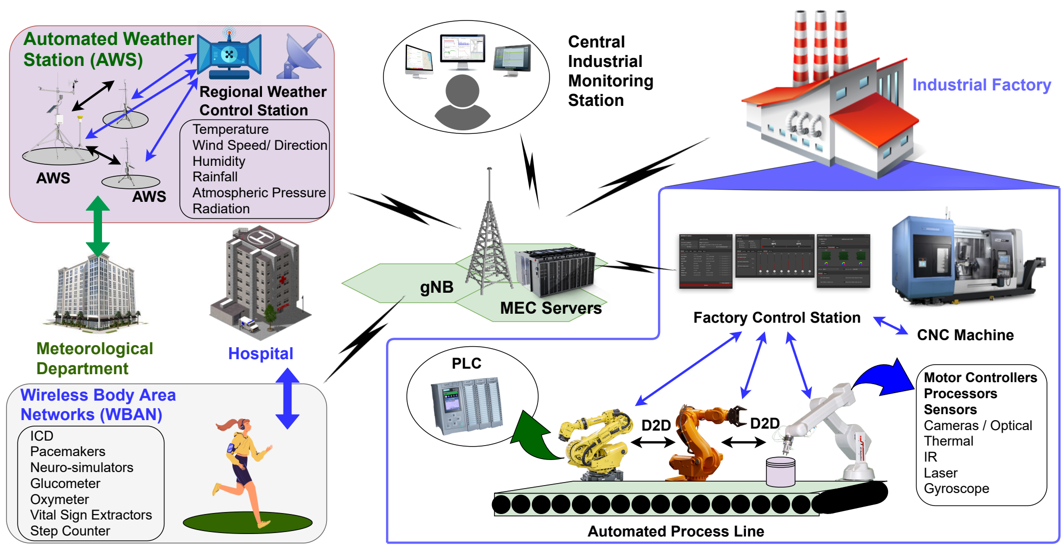

Fig. 5. MTC integration with MEC

Applications such as e-health wearables, IoT devices and entire range of machine controlled automated communication deployments are considered under this application [62]. The perception level of the majority of IoT applications is composed of sensory devices and actuators which rely on M2M communication for data transferring and conveying of control signals. The devices engaged in M2M communication are called Machine Type Communication Devices (MTCDs) by 3GPP. The access network facilitated for most MTCDs is non-cellular technologies which are Ultra Wideband (UWB), WLAN, ZigBee, Bluetooth, Low Power Wide Area (LPWA), Long Range (LoRa), Narrowband IoT (NB-IoT) or Wireless Body Area Networks (WBANs) in case of e-health applications [21],[138],[79]. The realization of IoT based services covers the extent of communication types which are ranging from Human-to-Human (H2H), Human-to- Machine (H2M) or vice versa and Machine-to-Machine (M2M) [21]. Though a typical MTC architecture instigates two communication scenarios: between MTCDs and MTC servers or inter-MTCD D2D type [28]. Healthcare applications such as health-assisting humanoid robots, remote surgeries and remote patient monitoring are plausible with MEC MTC deployments which uses WBANs for monitoring e-health statistics [104]. The types of MTCDs employed in WBANs are Implantable Cardiac Defibrillators (ICD), pacemakers, neuro-stimulators, gluco-meters, oximeters and vital sign monitors [138]. These heterogeneous bio-sensors, which are attached to different parts of the human body are communicating to the BS through a Machine Type Communication Gateways (MTCGs) using non-cellular network technologies. Fig. 5 illustrates various applications plausible for integrating into a MEC system.

3.3.1 Security Vulnerabilities. MTCDs inherit three main vulnerabilities. They are: communication media (such as wireless radio which would be subjected to eavesdropping), resource scarcity regarding power and processing. Nano-networks are limiting the usage of powerful security schemes such as X.805 and translation sequences for security protocols between wired and wireless communication networks to preserve power consumption [21],[138]. Attacks such as DoS, jamming and data tampering targeted at nano-nodes in a WBAN are plausible. An exploited WBAN or a MTCG would penetrate the BS and misinform ME Apps operated under the e-health applications in MEHs by risking the health of patients. Moreover, DoS or jamming attacks targeting a WBAN would cause service disruption of the corresponding ME Apps. Moreover, industry based MTCDs are prioritizing the longer operating time over the throughput [79]. Thus, the scarcity of computational resources in MTCDs is preventing the employment of strong security mechanisms. All these facts and diversity of communication protocols employed by MTCDs are improving the probability to penetrate the MEC system by malicious content.

3.3.2 Existing Solutions. The SMART framework proposed in [122] facilitates data extraction, transformation and load process for a plant floor data sourcing strategy. This deployment is capable of launching OPC-UA and MTConnect MTC protocols for extracting data from devices such as CNC, RFID, robots, sensors, gantry, conveyor, camera, Variable Frequency Drives (VFDs), and energy meters. Integration of edge computing utilize the storage, communication, control, configuration, measurement, and management processes while data analysis based on geometry, event, and signals are orchestrated for data reduction.

Li et al. in [79] proposed a novel framework that integrates M2M communication with MEC in a virtualized cellular network for offloading MTCD computational tasks towards the edge to utilize the energy consumption. Connectivity among the four layers: physical resource layer, NFV layer, virtual network layer, controller layer, and the application layer are established from the conjunction of Wireless Network Virtualization (WNV) and SDN technologies. The random access process is formulated employing Partially Observable Markov Decision Process (POMDP) to optimize the cost in terms of energy consumption and computation execution time. Moreover, a new technology called embedded Subscriber Identity Module (eSIM) is integrated into the MTCDs that offers the switching ability among virtual networks considering their distinct features and QoS requirements. Zhang et al. in [154] proposed a statistical delay bounded QoS provisioning scheme for two types of mobile data offloading scenarios : WiFi offloading and D2D offloading. This offloading scheme intends to be deployed on edge computing mobile wireless networks. The D2D offloading scenario is applicable to MTC deployments that require off-site processing environment due to resource scarcity in MTCDs. Th effective capacity and the optimal probability of using D2D offloading scenario is modeled mathematically to forecast a QoS guarantee for D2D based edge deployments.

Dong et al. in [28] propose an ICN approach to support anycast services in the core network through the MTC engagement at the mobile edge network located at the eNodeBs. Network softwarization is established from slicing of different service layers managed from an orchestration entity and a slice controller. A cropland monitoring use case is considered for formulating the solution where a protocol is proposed to indicate the intended message flows among the entities eNodeB, SGW, PGW, MTC server, and MTCDs. The results suggest that the bandwidth saving is higher at lower anycast update intervals times. Braeken et al. in [19] proposes an Edge Supportive Secure MAR (ESSMAR) architecture to assist doctors with additional information via MAR means to conclude the diagnosis. It is obvious that medical/healthcare information is extremely private, and should be protected against external parties. Thus, ESSMAR is included of a registration/ authentication key management scheme that was validated against MitM and replay attacks through AVISPA verification tool. The security analysis conducted among the mobile devices, edge server, cloud server, and underlying networks has given valid insights in formalizing the ESSMAR protocols.

3.4 Autonomous driving channels / connected vehicles and Vehicle to Vehicle (V2V) Connectivity

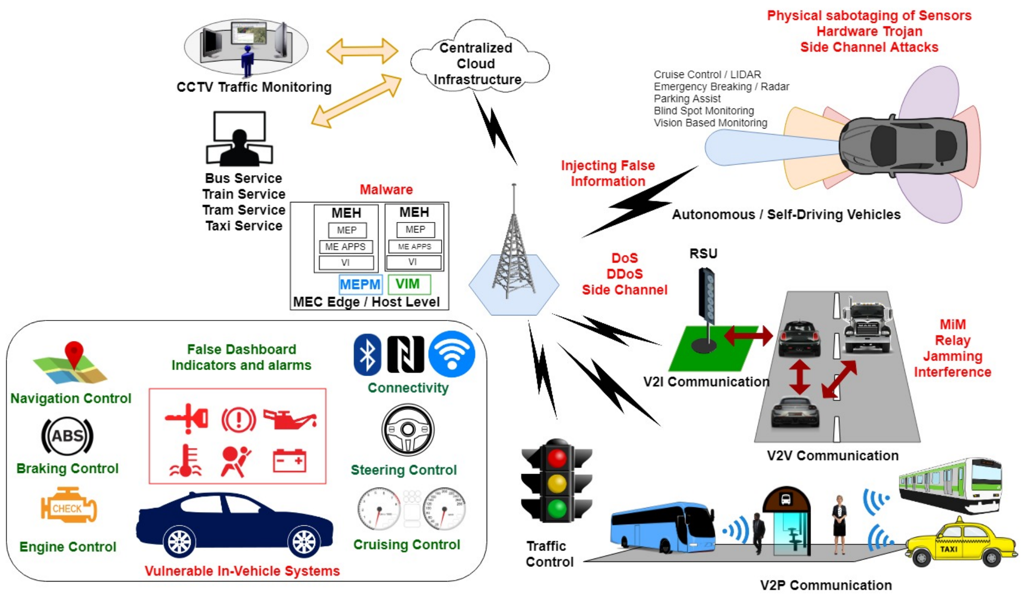

Fig. 6. ITS integration with MEC

The V2E adaptation is an initiative taken for Intelligent Transportation Systems (ITS) [102]. Vehicular Networks (VNs) that form the ITS deployments have its distinct place in 5G context [136]. Employing MEC system or any other edge paradigm for launching V2E applications is a certain fact due to its requirement of ultra-low latency and reliability [104]. The 3GPP defined connected vehicles technology is focused on enhancing safety, reducing traffic congestions, sensing vehicle behavior and servicing other vehicular value added services by offloading computational and geo-distributed services to roadside BSs or Infrastructure to enable autonomous driving with data connectivity that attribute the alleviated latency [88]. Though, with envisaged drastic development, transportation industries are becoming conspicuous cyber-targets for adversaries due to their rapidly evolving mobility structure as concluded by the report from IBM X-Force and Transport Systems Catapult [45]. The smart sensors deployed in vehicles enable the Advanced Driver Assistant Systems (ADAS), which is introduced as the preliminary stage of self-driving applications [145]. The embedded features that attribute to 100 million lines of program code and processing ability of 25 GB data per hour improves the feasibility for deployment [74]. Vehicle automation approaches are entirely reliant on sensors.

As sensors being electronic devices prone to be penetrated by adversaries, any successful malicious penetration could result in vehicle collisions, traffic congestions or damages to properties or human lives.

The connectivity between the vehicles is different from the connectivity from a vehicle to the BS. The protocols and the communication technology employed for this connectivity depends highly on the manufacturer. Though, in the United States the standard for V2V connectivity is Dedicated Short Range Communication (DSRC) technology which would transmit location, direction and speed of the vehicle to the nearby vehicle [137]. The intention of this V2V deployment is to provide early warnings to imminent accidents detected through a smart system embedded in the vehicles. Fig. 6 depicts the wide range of aspects in ITS deployments integrated with a MEC system. Further, possible attack vectors are indicated in an illustrative context.

3.4.1 Security Vulnerabilities. vehicular entities are prone to attacks which could be launched in the proximity of the targeted device as physical damage, hardware Trojans and side channel attacks. These attacks could grant access to the communication devices of the smart vehicles which are in direct connection to the Engine Control Unit (ECU) of the vehicle. The infiltration of the ECU could lead to circumvention of the safety critical systems in the vehicle [102]. Thus, influencing the ECU with false statistics in case of an autonomous or semi-autonomous driving could endanger the vehicle and the passengers travelling in it. Moreover, false information could be conveyed by an infected system to a ME App operated under a MEH for causing vehicular accidents with malfunctioning automotive processes.

The threats plausible for vehicles are mainly targeted at the different systems in a vehicular entity; such as GPS (spoofing and jamming), in-vehicle devices (malware, head unit attack), acoustic sensor (fake noises or interference), radar (jamming, repeater, chaff and smart materials), LIDAR (jamming and smart materials), Odometric sensor (magnetic or thermal), and electronic devices (EMP) [102]. Attacks such as dictionary, rainbow table and brute-force attacks to extract the passwords or keys, DoS or DDoS attacks for service disruption, protocol based attacks targeting Controller Area Network (CAN) or FlexRay and Rouge updates where the adversary targets the ECU firmware are plausible attacks on software perspective [99]. Out of those, attacks focused on in-vehicle, GPS and electronic devices are significant for MEC based connected vehicle deployments. Apart from service disruption of self-driving applications, latency precipitated from these interposing or jamming attacks would still be crucial for connected vehicle applications.

"Uconnect" is a remote monitoring and controlling in-vehicle connectivity tool that maintains a link with the internet from ECU for facilitating drivers the off-the-vehicle access. The same link with the internet is prone to exploitation for compromising vehicular controlling (brakes, steering, and lighting) and peripheral ECU / Bluetooth based infotainment systems that improve the plausibility of impregnating user mobile devices [45]. The traditional measures for protecting the vehicular systems are inviable due to the evolving softwarize infrastructure of the connected vehicle concept.

The mobility of the connected vehicles would be a major concern as their speeds and direction are changing rapidly with their movement. This mobility aspect of V2E applications are prone to threats of frequency hijacking of roamed channel, masquerading during handshake, and VM migration attacks presented in [69]. The causes of this threats could result in traffic congestions, accidents, property damages, or human casualties with the latency caused by mobility.

An infiltrated vehicular communication device is capable of injecting false information with the intention of causing accidents. A threat originated at a vehicular sub system for propagating a malicious agent to the MEC system is facilitated by the intrinsic circuitry of novel V2E deployments. As these embedded circuits are enriched with resources, connectivity and coverage for infiltration could be achieved. But the threat origination could incur at a vehicle which is not connected to the BS directly. The wireless links established between the vehicles in close proximity are vulnerable to jamming or interference attacks which disrupt the V2V communication links entirely. However, the possibility of a V2V link being subjected for intervention based attacks such as MitM and relay would be less probable due to the speeds where the vehicles are travelling.

3.4.2 Existing Solutions. To counter the security threats on ITS deployments, security procedures and algorithms have been defined in the IEEE Wireless Access for Vehicular Environments (WAVE) standard which are followed in US and Europe under ETSI [60]. This standard proposes an ECC based schema for certification and encryption where the wireless technology IEEE 802.11p is used for secure communication. An adversary is capable of exploiting even the smallest sensors inbuilt in a vehicle such as ultrasonic sensors which are used to detect the short range distances for assisting parking. Xu et al. suggested two defense strategies for vehicular sensory systems. They are; single-sensor based Physical Shift Authentication (PSA) scheme that verifies signals on the physical level and Multiple Sensor Consistency Check (MSCC) that employs multiple sensors to verify signals on the system level to overcome the probable attacks on ultrasonic sensors such as random spoofing, adaptive spoofing and jamming attacks [145].

As an initiative to achieve the efficiency guaranteed by Vehicular Delay Tolerant Networks (VDTNs), Kumar et al. in [67] proposed a system architecture which integrates the smart grid environments with MEC based hosting platform for various applications commandeered by mobile devices that are operating within the vicinity of Plug-in Hybrid Electric Vehicles (PHEVs). The architecture consists of four layers where the edge data centers responsible for data storage, file services and CA servers for legitimizing secure entities are included in the third layer. Smart charging functionality is modeled for PHEVs using the Bayesian cooperative coalition game approach in which the throughput increased by 10-15 % while 20% and 10% decrements are obtained for response time and incurred delay respectively.

Grewe et al. in [47] discussed MEC as a solution to alleviating the cost and latency associated with the resource heavy algorithms executed at the cloud in Electronic Horizon (EH) ADAS systems. The strategy involves offloading the EH instances to the Base Transceiver Station (BTS) or the Road-Side Unit (RSU). This enables mobility independent data retrieval and virtualized services with Information Centric Networking (ICN) integration. Security and privacy challenges in relation to the ICN integration are identified in the paper.

Cao et al. in [20] introduced a MEC based supporting architecture for Electrical Vehicle (EV) charging that employs RSUs as edge elements to orchestrate the operations: disseminating Charging Station (CS) availability to EVs, information mining and aggregation for EV charging reservations. A protocol for signaling is designed between the entities CS, Global Controller (GC) located in the cloud and RSU, EV operating in the edge network. A process flow for charging was introduced in use of 4 algorithms and a scenario was simulated considering an area of $4500 \times 3400\ m^2$ in Helsinki.

Aissioui et al. in [6] conceptualized the Follow Me edge-Cloud (FMeC) directive amalgamating the MEC and Follow Me Cloud (FMC) concepts that sustain the requirements of 5G automotive systems. The envisioned FMeC architecture enrolls PMIPv6 domains that serve edge cloud services and links to the vehicular entities from eNodeBs covering the domain area. Performance was evaluated from a simulation to model mobile network environment, vehicle traffic environment, and network communication model that employed the tools MONeT++, INET, SimuLTE, and Veins.

3.5 Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR)

Out of encompassed 5G service categories: enhanced Mobile Boradband (eMBB), massive Machine-Type Communication (mMTC), and Ultra-Reliable and Low-Latency Communication (URLLC); mobile VR, MR and AR are use cases of eMBB and URLLC which guarantees the ultra-reliability for the considered applications [32, 132]. As a 5G use case AR, VR, and MR are facilitating the services of providing immersive and interactive experience for: 5G hotspots, in-vehicle infotainment systems, and gaming for educating / instructing [89]. The VR refers to a 100% simulated visualization while AR and MR are differing by the extent of virtualization overlaid with digitization on visual perception [32]. A typical VR Head Mounted Display (HMD) occludes the users' field of view and positions the virtualized elements through eye and head movement tracking. In the current market, VR services are delegated to the low cost mobile devices such as Samsung Gear VR and Google Cardboard while Oculus Rift, HTC Vive or PlayStation VR are high quality streaming products with latency sensitivity. The Motion-to-Photone (MTP) latency exceeding 15 - 20 ms for image rendering causes motion sickness for users through conflicted signals precipitated on Vestibulo-Occular Reflex.

Latency < 10 ms, bandwidth > 1 Gbps and cell capacity > 500 connections are the requirements for ensuring the AR services with performance factors of screen response ≈ 2 ms, sensory extractions ≈ 1 ms, refresh rate at 120 fps ≈ 8 ms, and network RTT processing ≈ 2 ms for AR to be deployed as a 5G use case [89]. Basic function of an AR mechanism is to combine digital data generated through computed processing to the physical reality that intensifies the human experience. AR applications have adopted mobile technologies such as Layar, Junaio, Google goggles and Wikitude to enable its integration towards MEC [1]. Error diagnosing in industries and fixing, remote live supporting by the Original Equipment Manufacturer (OEM), Human-Machine-Interface (HMI) functionality for machine operation and virtual training for operators are few plausible use cases of AR and VR applications in the industries [70]. Typical AR process requires five critical components operate: video source (mobile camera), tracker (position tracker of the user), mapper (modeling of the environment), object recognizer (known object identifier) and a renderer (processing of the frames) where the components other than the locally deployable video source and the renderer could be hosted in the MEC server for computer intensive offloading [88].

An AR deployment on MEC test-bed has shown the latency and energy consumption reduction by 88% and 93% respectively through computational offloading [85]. This result is increasing the plausibility of integrating AR applications with MEC. Moreover, web-based AR (web AR) is an approach that overcomes the cross-platform and extensive provisioning limitations that are inherent with device-based and app-based AR applications. MEC is a patent deployment option for web AR that is envisioning to achieve 1 ms latency with 5G integration [105].

3.5.1 Security Vulnerabilities. The main threats plausible in AR applications are accessing and unauthorized manipulation of the video streams; where the attacker could easily distill the sensitive data of the users while manipulations of the video streams could lead to critical failures in machinery in industrial applications [70][88]. Thus, an exploited streaming channel between the MEC servers and the AR applications could confiscate the content in MEC hosts, which would infect the streaming traffic conveyed to other AR users in the proximity operated under the ME application. An infected ME App would manipulate the MEP and MEPM of the MEC servers to allocate more inessential resources for the particular application resulting service interruption of the MEC Hosts. Conversely, the privacy of both physical and virtual worlds of AR and VR users is a great concern [71]. Other than the private information such as credit card details, banking and personal passwords, virtual information composing the behavioral patterns (pulse and eye tracking enabling sensitive inferences [71]) would be a critical security concern. The interposing of any high bandwidth channel is conceivable for attacks such as MitM, impersonation, malicious node inspection, relay attacks and any attack plausible for intervening communication channels.

3.5.2 Existing Solutions. Langfinger et al. in [70] proposed a secure architecture for industrial AR applications to be compatible with Industry 4.0 standardization. In the deployment, an industrial automation device (as a Programmable Logic Controller (PLC)) is securely connected to a mobile device which would convey the camera frames into the edge server through the AR pipeline. After pose estimation, 3D registration, and rendering processes, AR output is visualized at the mobile device transferred in the same secure channel. Measures such as prohibition of parallel connections that links the UE and the edge, one directional information flow as in data diodes, using Transport Layer Security (TLS) protocol, and dynamic assignment of permissions for UE are proposed to enhance the security in this solution.

Qiao et al. proposed a framework in [105] for integrating web AR with MEC. The framework is formed from terminal, edge cloud, and remote cloud levels. The terminal level is pursuing the service scheduling and processing tasks while image capturing, image matching and 3D rendering are performed under processing operation. The edge level orchestrates the AR object deployment, destruction and support functions while the remote cloud level is provisioning generalized services in terms of resource management. A performance evaluation conducted employing Samsung Note 4, Wi-Fi and Alibaba cloud for launching the MEC framework revealed the effectiveness of edge computing compared with cloud computing.

The computational intensive and delay sensitive features of AR deployments prompt the issue of battery life time on AR devices. In order to address this predicament, Al-Shuwaili et al. in [7] formulated a model for offloading AR tasks to a cloudlet operating in the edge to alleviate the computational and communication overhead thereby utilizing the energy consumption. Successive Convex Approximation (SCA) scheme is adapted to allocate the resources in the AR process in an energy efficient manner.

Elbamby et al. in [32] investigated a use case for multiplayer immersive and interactive VR gaming scenario for assessing the URLLC performance that employs edge computing and mmWave Access Points (mmAPs). In the gaming environment, the location and orientation of VR Players (VRPs) are are tracked and mapped into the virtual space using the mmWave head-mounted displays (mmHMDs). MEC network is formed to perform the offloaded real-time computing tasks that are conveyed through the mmAPs.

Eventhough the MEC paradigm improves the network responsiveness of the VR applications through alleviated latency, saving the communication bandwidth is vital for the network to avoid congestions. Conversely, leveraging computation and caching resources in mobile VR devices are an approach of sustaining the transmission efficiency. Thus, Yang et al. in [148] proposed a communication constrained MEC framework that utilizes the consumption of resources in the mobile VR devices through the exploitation of caching mechanisms in the edge servers. Lyapunov theory was used to produce the offloading decision optimization algorithm which acts as an optimal task scheduling policy, while the task requests are modeled as a Bernoulli process among other mathematical scenarios considered.

3.6 Unmanned Aerial Vehicles (UAVs)

UAVs play an increasingly important role in various scenarios such as photography, disaster response, inspection, monitoring, precision agriculture, military, communication relaying, traffic control, and disaster relief services [88][52]. Tasks such as disaster relief efforts, detection of damaged reactors in the Fukushima nuclear power plant, real time sensing of radiation levels, and status assessment of the neutralizing program was orchestrated by UAVs during the Japans' East great earthquake [92]. Federal Aviation Administration (FAA) is predicting the amount of UAVs to be sold annually to 4.3 million by 2020 as an indication on the extent of applicability for UAVs [41]. UAV based communication deployments attribute: the Line-of-Sight (LoS) transmission attained by hovering to targeted locations, dynamic deployment ability that features robustness to climatic effects and nullified costs for site installation in case of an acting BS, and UAV-based swarm networks that facilitate ubiquitous connectivity to ground users with high flexibility and various provisioning options [77]. UAV operations are categorized as Low Altitude Platforms (LAPs) and High Altitude Platforms (HAPs) that are distinguished on altitude, computation, coverage, power, capacity and endurance capabilities. Moreover, Size, Weight and Power (SWAP) of UAVs are constraints for attaining desired performance metrics. The priority of the UAV is to conserve its battery life for flying while offloading the computational or storage content to the MEC servers for processing [104]. Thus, employing strong cryptographic primitives or prolonged security protocols would be infeasible. The controlling link to UAVs could be maintained from a ground station or by a remote station controlled through a MEC system. Fig. 7 illustrates various UAV enabled applications in addition to embedded components of a UAV plausible for exploitation and attack vectors.

3.6.1 Security Vulnerabilities. In this application, the usage of cryptographic primitives would be limited due to the requirement of preserving power (e.g. drones). Concisely, threats plausible for UAVs are categorized under Electronic / Electromagnetic, Cyber and Physical (ECP) spaces [41]. Most common type of attack plausible for drones or UAVs is the GPS spoofing attack, in which fake GPS locations are sent to the UAV for misleading or crashing the object. Approaches to bypass the cryptographic measures with electromagnetic, optical, or acoustic emanations called compromising emanations are mentioned in [41]. Apart from that attacks such as malware, key-loggers, blinding the sight of the remote pilot with laser, identity spoofing, cross-layer, multi-protocol and various DoS or DDoS attacks focused on exhausting the battery of the UAV is plausible [52, 108]. In the two methods where UAV maintains direct connectivity with the BS for controlling or computational offloading, the connectivity could be subjected to interposing attacks plausible on the air interface [110]. The threats towards the MEC system from UAV based attacks can exist with the computational offloading method where a malicious agent could be propagated to the MEH for manipulating ME Apps. Any successful attack could result in UAV crashing that cause damages to property or human lives.

3.6.2 Existing Solutions. Fouda et al. conducted a comprehensive assessment for plausible attacks on UAV Systems (UAS) focusing on Software Defined Radio (SDR) based UAS architectures [41]. Hooper et al. in [56] proposed a multi-layer security framework that integrates the Open System Interconnection (OSI) model layers with the Linux operating system kernel to secure the Parrot Bebop type UAVs from the exploits buffer overflow, DoS and Address Resolution

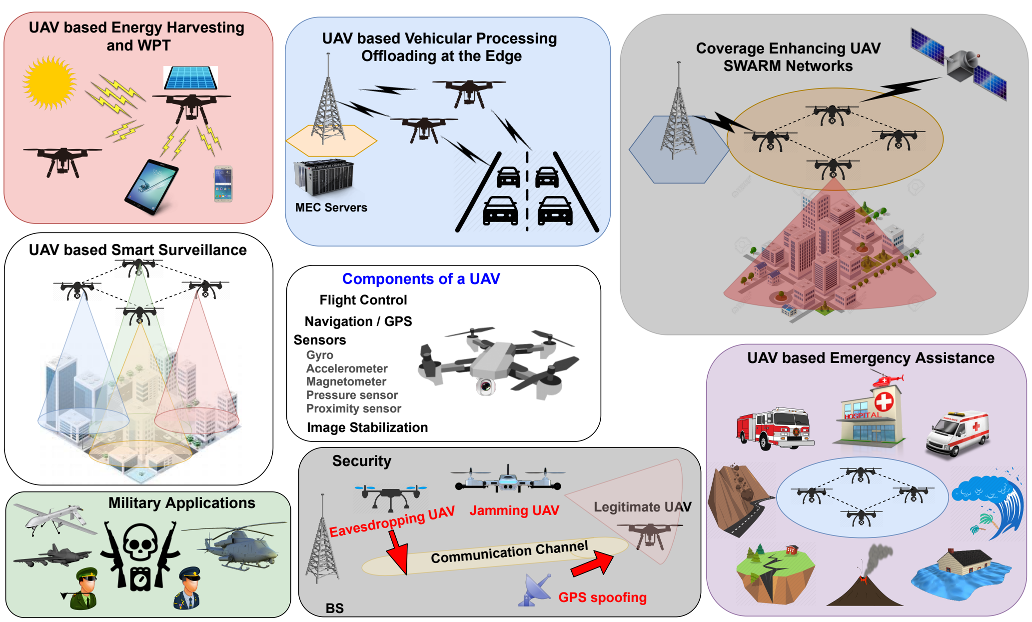

Fig. 7. Applications and Security of MEC based UAV

Protocol (ARP) cache poison attacks. Penetration tests have been undergone in addition to introducing a watchdog timer to utilize the CPU operations to the navigational processes and anti-spoofing mechanisms to the UAV access point.

Motlagh et al. in [92] proposed a crowd surveillance method adopting UAVs and face recognition techniques for detecting crimes, vandalism, and terrorist acts. In this case, MEC servers are deployed alongside a BS for offloading the surveillance processing tasks to utilize the battery life of UAVs. In the experimental setup, a hexa-copter used as the UAV is embedded with a camera, LTE modem, computing and sensory inclusions for flight controlling. The access to the MEC server is facilitated from a LTE eNodeB while the face recognition process is operated at the ground control station. Local Binary Pattern Histogram (LBPH) algorithm is employed for face detection while the results demonstrated a significant reduction in energy consumption and processing time.

Garg et al. in [45] proposed a load balancing system for vehicular edge processes where UAVs are used as intermediary hubs for transmitting information for processing and surveillance activities. The system includes the entities: vehicular entity, UAV, dispatcher, edge devices, cryptographic entity, and the aggregator. The main steps of the model are authentication, balance load distribution, data processing, encryption, decryption, aggregation of data, and decision delivery to the vehicle through the UAV. A triple-Bloom-filter is used to launch a fast service processing platform between the vehicles and UAVs for distinguishing traffic, alleviating E2E delay, and enhancing authentication mechanism. The experiments conducted in a vulnerable environment with 100 possible attack vectors concluded the improved factors: computation time complexity, time complexity, delay, and precision.

Inspired by the Wireless Power Transmission (WPT) technologies and their usability on MEC use cases, Zhou et al. in [155] introduced a novel UAV-enabled wireless powered MEC system for prolonging the operational time of the energy limited mobile devices. UAVs are transmitting wireless energy to UEs that are located in the coverage area, where the UEs are granted the ability to leverage the harvested energy to perform computations or offloading tasks. A 3D Euclidean coordinate system and Time Division Multiple Access (TDMA) protocol is adopted for formulating the model. Moreover, energy minimization, computation offloading, CPU frequency optimization, and trajectory optimization are studied employing Sequential Convex Approximation (SCA) technique and Karush-Kuhn-Tucker (KKT) conditions. The simulated results suggest a decremented total energy consumption of UAVs in the proposed scheme compared with two other schemes. The minimization however, is not significant. Security challenges for MEC based 5G use cases are specified in TABLE 1. Further, security countermeasures / best practices adoptable for MEC use cases are tabulated in TABLE 2.

4 MEC AND 5G RELATED PROJECTS

The MEC initiative is evolving around Europe as most of the companies which collaborate to standardize the concept are European institutions including the ETSI. Thus, it is conspicuous that most of the MEC based projects are formed around Europe. The European 5G Infrastructure Public Private Partnership (5G PPP) with the initiative of Horizon 2020 grants have funded a multitude of research groups in excelling their products and innovative insights on 5G related directives [104]. MEC is an underlying concept of most of such projects to achieve the guaranteed features. Therefore, in this section, MEC related projects and details of the research groups are addressed.

4.1 MEC AI (Jan 2018 - Dec 2019)

MEC AI [96] is a directive pursued under the Edge Computing Enhanced by Artificial Intelligence (EDGE AI) project conducted by University of Oulu, Finaland. The project is funded by the Technology Industries of Finland Centennial Foundation, Jane and Aatos Erkko Foundation, and 'Future Makers' award. As a pioneer in cutting edge research on 5G

Table 1. Summary of Security Challenges for MEC Integrated 5G Enabled Use Cases

Security Challenge	Description	Critical Infrastructure	eMBB Cases	M2M and mMTC	Auto Driving/ V2V	AR/ VR/ MR/ XR	UAVs
DoS/ DDoS and Jamming Threats	Maliciously intended service requests targeting 5G (radio interfaces) and MEC (UALCMP and CFSP) are created in numbers and lead to service delays and disruption.	H	M	H	M	M	H
Flaws in PLC/ SCADA/ CPS	Design flaws in these hardware entities are exposing the industrial automation systems.	H	L	H	M	L	L
Phishing/ Masquerading/ Imposter Threats and Integrity Violations	Inability to verify/ validate the UEs, access points, and 5G/ MEC interfaces are allowing the adversaries to impersonate and extract information with gained access.	M	M	H	H	M	H
Energy & Resource Depletion Threats	Attackers are targeting the exhaustion of processing, storing, and memory resources, while ultimate objective is to deplete the standalone energy of IoT devices.	L	M	H	H	M	H
Scalability	Myriads of IoT devices are demanding rapid access to MEC services; cumbersome crypto primitives are unusable.	M	M	H	L	M	M
Compatibility/ Interoperability	Technological diversification inherent with 5G and IoT is restricting integration of standardized security measures.	L	H	H	M	M	M

Low Risk   Medium Risk   High Risk

directive, researches in University of Oulu are focused on realizing the potential of employing edge computing as a means for processing data extracted from sensory and network devices to be utilized for applications such as hospitals, industry and vehicle steering. Prime objectives of this initiative are low latency and security. MEC based AI methods are developed to achieve those objectives in collaboration with the Finnish industries as Nokia. Especially, security aspects of MEC and AI integration is considered as a prime focus.

4.2 ANASTACIA [Advanced Networked Agents for Security and Trust Assessment in CPS / IoT Architectures] (Jan 2017 - December 2019)

ANASTACIA [15] is a EU H2020 funded project which integrates MEC and IoT for CPS based deployments to guarantee holistic trust and security by-design solutions. This is one of the highly functioning H2020 projects that investigate security from NFV and SDN applicability perspective. ANASTACIA achieved the goals of adaptation of security and privacy practices evident from the results of the projects that yield the technological integration of Low-Resource IoT, VNF image integrity, MEC resource geo-partitioning, NFV security best practices, anomaly based IDS, secure NFVI, network softwarization, 5G NB-IoT, Security-as-a-Service and many other novel concepts.

Table 2. Summary of Security Countermeasures/ Best Practices for MEC Use Cases / Applications

Ref. No.	Proposed Security Countermeasures / Best Practices	Critical Infrastructure	eMBB Cases	M2M and mMTC	Auto Driving/ V2V	AR/ VR/ MR/ XR	UAVs
[128]	Machine learning based anomaly detection technique for SCADA systems	✓		✓			
[75]	Utilizing blockchain based VNF descriptors for energy level tracking in RAT xMEC offloading deployment	✓		✓			
[122]	SMART framework for detecting anomalies in PLC based extracted data	✓		✓			
[44]	Blockchain model for SGNs to counter SDT and BEA, energy related attacks	✓	✓	✓			
[67]	Legitimization of PHEV entities from CA servers in the proposed architecture for MEC based smart grid vehicular charging process	✓			✓		
[47]	Security and privacy considerations in the ICN integrated MEC based offloading scenario for EH ADAS systems				✓		✓
[70]	Secure architecture for industrial AR applications that form a secure pipeline between UE and the edge servers	✓	✓			✓	
[56]	Multi-layer security framework for Parrot Bebop UAVs integrating OSI model						✓
[45]	Cryptographic means used in authentication mechanism considered for UAV based load balancing for edge processes				✓		✓
[109]	Security as a Service (SECaaS) approaches for the edge	✓	✓	✓	✓	✓	✓

4.3 SESAME [Small cEllS coordinAtion for Multi-tenancy and Edge services] (July 2015 - January 2020)

SESAME [49] is a EU H2020 project that targets the innovation of network intelligence, applications in the edge and NFV elements established through the extension of small cell concept for realizing highly dense 5G scenarios. MEC concept is studied for proposing the Cloud Enabled Small Cell (CESC) concept that forms a multi-operator configurable small cell to integrate virtualized execution platforms. SESAME targets to develop the orchestration strategy, NFV management, consumer virtualization management interfacing, self-x feature and radio access management techniques demonstrated through a prototype implementation.

4.4 SUPERFLUIDITY [A Super-Fluid, Cloud-Native, Converged Edge System] (July 2015 - March 2018)

SUPERFLUIDITY [123] project is intending to achieve super fluidity in the network by extending services to the core, aggregation, and edge partitions as in the case of zero viscosity fluids. This project is funded by the EU H2020 initiative. SUPERFLUIDITY answers the shortcoming of current networks such as impeding provisioning times, wasteful over-provisioning in variable demand, ineffective hardware, and ineffective heterogeneity support for multi-vendor components. The project developers are aiming to furnish the location, time, scale, and hardware independence benefits to the 5G networks guaranteeing telecom operators the capability to blend IT infrastructure effectively.

Developing a security framework to control the access of network processing functions is one of the project objectives of SUPERFLUIDITY. Recent directives of the project have shifted towards SDN and NFV technologies.

4.5 5G EVE [5G European Validation platform for Extensive trials] (July 2018 - July 2021)

5G EVE [36] intend to implement and test, an advanced 5G infrastructure formed by interconnecting existing European sites at Greece, Spain, France, and Italy. It is one of the three projects funded by the 5G PPP in 2018. The conceptual goal of this project is to develop a 5G end-to-end facility in Europe to validate the network Key Performance Indicators (KPIs) of the 5G prototype scenarios through experimentation. The targeted experimental subjects include advanced spectrum management, MEC, core/backhaul services, heterogeneous accessing methods, and site internetworking via multi-slice orchestration. The telecommunication operators OTE, Telefonica, Orange, and TIM are facilitating the sites at European vicinities that focus on diverse use cases as smart mobility, Industry 4.0, smart energy, smart environment, Immersive media and entertainment. Services such as URLLC, eMBB, and mMTC are dominating the deployment options.

4.6 6G FLAGSHIP (June 2018 - May 2026)

Being a project initiated by University of Oulu, Finland [95]; envisions the wireless connectivity for 2030 with data-driven and near-instant features. MEC and use cases specified in this paper are considered directives of 6g-Flagship in addition to Machine Learning (ML) and Artificial Intelligence (AI) approaches to automate the functions optimally. The goals of this project reach from finalizing the 5G adoption, to the development of the 6G enabling technologies with speeding up the digitization process. The domains of wireless connectivity, devices/circuits technology, distributed computing, and services/ applications on 6G are covered in this project. A 5G test network is already deployed in the project and deployed for developing easy to use tools for future advancements.

TABLE 3 represents the summary of MEC based projects been discussed and their targeted aspects in terms of security, privacy, trust, mobility, and interoperability.

Table 3. Summary of 5G and MEC Projects and Research Groups

Project	Main Research Focus	Security	Privacy	Trust	Mobility	Interoperability
MEC AI [96]	Ensuring low latency and security in 5G networks via MEC and AI integration	✓	✓	✓		
ANASTACIA [15]	Investigating and demonstrating a holistic trust and security by design solution for CPSs with integrated MEC and IoT concepts that employ NFV/SDN based networking infrastructure	✓	✓	✓		✓
SESAME [49]	Extending the small cell concept to achieve CESC, with the integration of MEC and NFV technologies to realize 5G dense scenarios				✓	✓
SUPERFLUID [123]	Proposes a converged cloud based 5G concept that enable mobile edge use cases by extending the service functionality to the holistic network	✓			✓	✓
5G EVE [36]	Implementing and testing an advanced 5G infrastructure extended to European sites for validating 5G services including MEC				✓	✓
6G FLAGSHIP [95]	Developing the fundamental technologies for emerging 6G with an emphasis on wireless connectivity and intelligent distributed computing	✓	✓		✓	✓

5 DISCUSSION AND FUTURE WORK

This section comprises a concise explication of assimilated insights from the survey in terms of security and privacy of MEC systems. Presented insights are aligned with the future directives proposed from emerging researches for recognizing potential of the MEC deployments. Moreover, potential applications and probable technological solutions to be integrated with MEC to enhance the security are summarized.

5.1 MEC Applications

5.1.1 *Critical Infrastructure.*

Lessons Learned: It is evident that MEC capabilities forecast the potential to realize the smart city concept. Enabling the versatility of infrastructure based servicing is the key to achieving that goal. Though assuring security for diverse infrastructure based services is an arduous task due to their heterogeneous system architectures. Offloading storage and processing functions to the MEC edge network however, guarantees that these variant technologies are operating in a complied digitized environment in the data processing phases. SCADA and PLC based operators are common in these deployments. Threats originating internally in such environments are capable of exploiting the edge system once instilled through the communication channels. Eventhough mechanisms have been studied to detect malicious entities in SCADA based systems, the security of offloading channels are not addressed significantly.

Future Directions: In terms of smart grid security, various approaches such as key distribution based on Needham-Schroeder authentication protocol, ECC, PKI, Trusted Anchor (TA), Lightweight Directory Access Protocol (LDAP) as a third party, hybrid Diffie-Hellman, AES, RSA, Tsai-Lo identity based encryption scheme and ECC based ElGamal schemes are proposed for securing the connectivity extending from the SEM to the smart grid [90, 94, 126]. Blockchain is an approach to be considered in the future to ensure the privacy of subscriber consumption statistics traversing in SGNs. Similar approaches are plausible for developing security solutions to terminal entities in other infrastructure services. Moreover, securing the offloading channels of the edge system is a critical directive for mitigating threats originated internally. In addition, outsourcing security to a trusted MEC based service as in Security as a Service (SECaaS) approaches are gaining popularity due to its optimum resource utilization in the context of critical infrastructure [109].

5.1.2 *eMBB Channels/ Video Analytics/ Big Events.*

Lessons Learned: Crowd-sourcing applications are one of the major contributors for proliferation of video streaming traffic. As these services are demanding UHD level quality in videos to facilitate ubiquitous reception at mobile devices, managing the bandwidth utilization is a conundrum for MNOs. This requisite is prominent in case of a big event coverage is undergoing. Thus, MEC in-proximity servers are capable of buffering the content prior to launching the streaming service, that enables the seamless video transmission. Advance video analytic capabilities are plausible with MEC servers that align with CCTV, face and vehicular name plate recognition techniques adapted by authorities. Most common type of security attack plausible for streaming channels is the interposing attacks conducted for altering the content for misleading the receiver which are influenced by politics, terrorist, or cyber marketing strategies. To secure the channel, an acceptable level of encryption should be employed. Though embedding security measures for video streaming channels in these scenarios are costing the bandwidth utilization. Thus, metrics should be established to retain the balance between security and bandwidth usage.

Future Directions: As trending video streaming and crowd-sourcing applications are demanding their services to mobile devices, mobility is an aspect to be considered for proposing security measures. Thus, PLS based approaches as in [143] could be utilized to ensure security from the mobile device end. Joint network coding and re-transmission is an approach to secure the video streaming channels in IoT systems as proposed in [106]. Moreover, embedding security mechanisms in the video coding protocols at the design stage with minimum bandwidth adaptation is an interesting research directive for the future.

5.1.3 mMTC links in IoT.

Lessons Learned: The mMTC applications are ranging from the personally using e-health type WBAN wearables to massive industrial applications that employ MTCDs of different scales to create an autonomous environment. MEC plays a vital role for ensuring security for wearables with attributed location and context awareness. Moreover, edge infrastructure acts as a offloading serviceable platform to the industrial mMTC applications to improve their efficiency and global reach. As MTCDs are operating with various non-cellular communication technologies, employing security mechanisms should be applied to each technology separately in accordance with their protocols and specifications. Authentication mechanisms to be adapted should vary dependent on the authenticating entity as both human and machine entities are engaging in mMTC communications. Service impeding attacks such as DoS and DDoS are causing more damages to mMTC based industrial systems due to their reliance on scheduled operations. Privacy is a considerable factor for WBAN based services that is not addressed significantly.

Future Directions: For implementing security in WBAN based on nano-technological scale, biochemical cryptography could be adopted where biological molecules such as DNA or Ribonucleic Acid (RNA) are used as a source of encryption [138]. Though, this emerging field is creating new set of challenges, a cryptographic key based on molecular configuration or chemical reaction unique to a person would grant the level of inherence required from the bio-metrics in the nano-domain. Moreover, ECC based lightweight cryptographic protocols could be employed with WBAN sensory devices which are more resourceful than nano-level devices. In [153], a Lightweight and Robust Security Aware (LRSA) D2D assisting Certificate Less Generalized SignCryption scheme is proposed for WBAN based Mobile Health (M-Health) applications that resemble the requirement. As M2M based authentication schemes are prominent in this use case, PUF based approaches would be viable for deployment. Integrating security into D2D offloading schemes is a potential research area for the future under this application. Blockchain is becoming a solid resolution for privacy protection. Thus, blockchain based solutions such as [54] for tele-health wearable privacy preservation and certificate revocation approaches for M2M links as in [53] are promising directives for the future.

5.1.4 Autonomous Driving / Vehicle to Vehicle (V2V) Communication.

Lessons Learned: This is one of the leading use cases of MEC that relies on processing capability of the edge for enabling autonomous driving to mitigate traffic congestions and accidents. Context awareness feature of the MEC is the key to deploying these services. In this use case, most probable attack vectors are emanating from the in-vehicle systems as they are prone to physical attacks. The radio based links that communicate with the MEC BSs directly are exploitable by attackers to cause accidents. In an ITS system, infrastructure based intermediary entities are located for expanding coverage. These entities are accessible for physical manipulations. Moreover, interfacing vehicular entities that engage in V2E adaptations are plausible scenarios for MEC. In that aspect, security in DSRC protocols that enable the V2V communication is a significant factor to be considered as explicated in [150].

Future Directions: Embedding adequate security measures to DSRC protocols as proposed in [80] should be considered to enhance V2E type communication channels. As vehicular offloading channels are requiring high responsiveness compared with other offloading mechanisms; an approach as Vehicular Edge Computing Network (VECN) proposed in [125] could be employed to secure the offloading channels specific to vehicular communications. According to ITS standard, vehicular entities are connecting with the edge under different scenarios of V2X. Thus, adaptive security mechanisms should be utilized as proposed in [113]. Moreover, adaptable measures to enhance the security in ECU of vehicles should be investigated to mitigate in-vehicle threats. Since all such security measures cannot be applied manually, autonomous approaches should be sought out employing AI or ML methods with novel algorithms to exploit the trade-off of security application, latency, and energy consumption [13].

5.1.5 AR/VR/MR.

Lessons Learned: AR and VR technologies are prominent for gaming and e-learning based applications that are extended from eMBB and URLLC adaptation. Latency, bandwidth, and cellular capacity are prime factors to achieve the required performance. Similar to video streaming applications, MEC facilitate a closer proximity video server for processing and storing AR scenarios. Alleviating the latency associated with image rendering and transmission is critical for the VR or AR users to avoid health issues as motion sickness. The remote surgeries, error diagnosis and maintenance in industries are viable AR deployments for the future. Thus, minimizing the delay is vital for realizing these deployments. In the perspective of security, service impeding attacks are jeopardizing such latency prone services. Attack vectors such as physical tampering, side channel attacks, malicious code injections, and hardware Trojans are applicable to AR/VR HMDs. Privacy is a key concern with AR systems, as they are extracting a higher range of sensory acquisition scope (visual strength, ocular orientation, location, and arm/leg motion tracking) that expose user sensitive credentials and behavioral statistics.

Future Directions: Developing security measures in the user devices as HMDs is imperative to ensure the privacy of users. As behavioral statistics could be gained from AR or VR based games played by the users without their awareness; legislation's should be put forward to extract user consent before enrolling with a particular game. Moreover, human health is a concerning factor for AR/VR based services that could result in ocular discomfort. Thus, proper methods should exist to notify the user regrading the timely visual quality that AR application is attributing to safeguard the user health. Though elevated number of sensory extracting apparatus embedded in AR devices are forming an opportunity to improve the existing authentication schemes and network security through visualization as patented in [124] and [10].

5.1.6 Unmanned Aerial Vehicles (UAVs).

Lessons Learned: As most UAV based services are operated with a direct connectivity maintained with the UAV from a ground station, mobility tackling and LoS control signal transmissions are factors that raise concerns over the communication aspects. The dispersed MEC servers are providing an extended coverage for UAVs to operate seamlessly. UAVs could enhance the performance by offloading the processing to MEC servers. Due to the higher mobility and eccentric reachability, UAV deployments are perceptible for surveillance activities in the future. Though battery life is the prime factor that decides their performance. Thus, UAV targeted attacks are focusing on exhausting the resources of it to terminate its life-cycle. In addition, eavesdropping scenarios are probable with intently placing of fake UAVs to induce spoofing attacks.

Future Directions: Proper measures should be explored to pursue the operation of the UAVs in instances that it fails to maintain the LOS connectivity to the operating ground station. Utilizing AI for developing an adaptive auto-pilot scheme is an approach to overcome that requirement[146]. PLS measures could be adapted as in [156] for maximizing the Intercept Probability Security Region (IPSR) to obscure the eavesdroppers through friendly jamming. Moreover, UAV enabled mobile relaying with an integrated MEC platform could be utilized for improving PLS in mobile communication environments [141]. UAVs should be embedded with self-activated security features at the manufacturing stage to counter intercepting attacks as isolation from the communication network is not an option. Similar to V2V applications, UAV requires the autonomous edge intelligence through means of AI/ML methods to improve decision making, and security management [48, 149].

5.2 Futuristic Applications

5.2.1 Rural Communication. The term 'rural' signifies an opposite meaning to an urbanized area that does not inherit adequate amount of resources to facilitate a seamless communication operation. As telecom operators are prioritizing their return on investment, developing telecommunication infrastructure extending to areas that occupy minor population is ineffective in their perspective. Moreover, pragmatic circumstances such as geological location, atmospheric conditions, LoS, and failure to acquire land to launch remote sites are plausible factors that enable rural communication. Thus, existing communication options are limited to satellite links that are accessible globally with attributed drawbacks of latency and high reliance on atmospheric conditions[23]. Rural communication is applicable for various instances where rural communities are restricted of accessing novel technologies that rely on mobile connectivity for operation [120]. Rural Smart Grids are one such instance in which an isolated facility or minor community are serviced by a low capacity grid deployment [63]. Moreover, health sector is a widely applicable rural circumstance that requires assistance from underlying communication infrastructure to handle emergency situations including ambulances [31][57]. Due to the improved capacity and coverage in mobile sites of MEC systems, servicing the rural areas are plausible with proper mobile propagation parametric adjustments. In addition, MEC enabled RAN access interfaces are capable of supporting non-3GPP communication services that are plausible for connecting the rural sites to the proximate BS. MEC based rural transmission of data endure an improved opportunity to ensure security and privacy compared with satellite communications.

5.2.2 Smart Agriculture / Farming. The rapid population growth demands excessive food production to cater humans and live stocks in farming industries. Resource depletion, pollution and scarcity for labor are elevating the arduousness of maintaining agriculture based services to cater the demand [101]. Thus, automation is an imminent option for improving the servicing of smart farms with IoT integration. IoT sensors are deployable for monitoring climatic and crop development status to automate the water and fertilizer dispersing mechanisms. These automation strategies draw insights from gathered data analytics to maximize the crop production. Adapting machine learning is such a strategy for crop selection and maximizing crop yielding rates [68]. M2M links are typically established between IoT devices that employ technologies such as BLE, NFC, or Wi-Fi. As these devices are located remotely to the main farm site, physical tampering due to intended or natural causes is plausible. Vehicular monitoring is another aspect of smart agriculture that enhances the efficiency of the outcome. UAVs are applicable to remote monitoring of crops while autonomous vehicles (tractors) are enabling precision farming [104].

Nanotechnology based bio-sensors are a trending adoption for smart farming applications to conduct accurate analysis on soil humidity, water, pesticide usage, and plant pathogens in a nano-scale [9]. Dong et al. in [28] proposed an information centric approach to achieve the anycast service in MTC with ICN (Information Centric Networking) being enabled as a slice in the future network adaptable to smart farming. The mobile edge computing at the eNodeB facilitates the anycast service to the clients with significantly less experienced latency and reduced control message overhead generated in the core network. In the MEC perspective, similar to rural communication; MEC servers remotely situated or reached via enhanced coverage of MEC enabled BSs, contribute to smart agriculture services significantly. Though achieving security is a challenging task due to wide coverage.

5.2.3 Industrial IoT (IIoT) and Industry 4.0. Industrial Internet, IIoT or "Industry 4.0" is a standard represented by the Fourth Industrial Revolution (4IR) for integrating IoT services for industrial sectors [104]. Initial intention of the Industry 4.0 standard was to integrate Cyber-Physical Systems (CPS), IoT and cloud computing based data analytics to facilitate automation for industries by assuring interoperability, information transparency, technical assistance, and decentralize decision making design principles [107]. Sensors in IIoT are optimizing the production from captured sensory data via Programmable Automation Controllers (PAC) that handle processing and communication [46, 127]. The majority of current industrial automation plants are embedded with SCADA systems. Thus, security vulnerabilities explicated under critical infrastructure based applications are adoptable for this circumstance. Moreover, IIoT could be visualized as a way of amalgamating the machine based and human based workforces for achieving a maximal outcome that benefit industrial owners and human operators. Digitized data of every aspect in the manufacturing processes offer opportunities to optimize the practices revealed through proper mechanisms. As industrial factories are large vicinities, MEC enabled BSs could be launched inside the factories for enhanced service provisioning depending on the occupied human and non-human workforce. MEC edge level launched within a factory premises could be configured for servicing specialized industrial requisites to achieve low latency and high reliability. Several edge based approaches are proposed for enhancing IIoT operation in [17, 98]. As M2M based communications are imminent, security protocols should adopt proper D2D authentication mechanisms such as PUF and PLS for mitigating exploitations.

5.2.4 Tactile Internet. The Tactile internet is considered as the next evolutionary level of the Internet that deliver real-time control, touch, sensing/actuation information via a reliable, available, responsive, secure, and intelligent connectivity that envisions a broader internetworking context capable of handling unprecedented circumstances probable with impending applications [5]. This vision preemptively coined by G. P. Fettweis in 2014, creates a plethora of opportunities and applications that provision features required for expanding IT market base [86]. It is standardized by the IEEE Tactile Internet (TI) Standards Working Group (WG) that is designated by IEEE 1918.1 [55]. The 5G mobile network concept is the raison d'etre for Tactile internet that focuses on serving the industries expanding with the Industry 4.0 standard [129]. Functional representation of the end-to-end Tactile internet architecture includes master, slave, and network domains where master and slave domains are operating at Tactile edges[5]. These deployments are mainly focused on serving CPSs, MTC, M2M, D2D, and VR applications that require 1 ms of round-trip latency. Maier et al. in [86] investigates the deployment of Tactile internet concept with Fiber-Wireless (Fi-Wi) enhanced LTE-A heterogeneous networks to be adopted in MEC considering the latency and reliability performance aspects. MEC with its attributed ultra-low latency and high reliability processing infrastructure in the edge envisage the visions of Tactile internet that enable proper security mechanisms as a significant factor.

5.2.5 Disaster Management. Environmental disasters were once believed as a means of balancing the human population from over-exhausting the resources on earth from devastation's such as landslides, earthquakes, avalanches, tsunamis, volcanic eruptions, flooding, forest-fire, and lightning. Though current disasters are prone to be emanated by human intervention as in massive explosions resulted from industrial malfunctions that extend to nuclear level or extremist acts resulted from terrorism. In spite of the origination of disasters, the damage and casualties associated with them are unpredictable. Unprecedented nature of the affected scope by geographical and atmospheric means are exacerbating the circumstances for evacuation procedures conducted by the authorities. Thus, scientists are focusing on integrating IoT for disaster management and relieving scenarios that contribute to early warning, notification, data analytics, knowledge aggregation, remote monitoring, real-time analytics, and victim localization functions [114].

Deployment of IoT sensors for measuring the environmental statistics (such as atmospheric, seismic, volcanic, radiation, and ocean level) is paramount to forecasting disasters and their magnitude. Maintaining the communication links without been overloaded is a prime requisite for telecommunication service providers perspective in a disaster situation. MEC is a paradigm introduced to improve the standards of current telecommunication infrastructure in terms of service provisioning and access capacity. Thus, Disaster management services extended through WSNs could be operated by a MEC edge level in a certain geographical coverage area, enabling the disaster mitigation functions mentioned above. Proliferated responsiveness of the MEC RF based access interfaces, attribute the potential to improve the evacuation procedures and notification schemes with the integration of crowd-sourcing applications [112]. As Ray et al. in [114] presents various IoT based state-of-the-art solutions applicable to disaster management situations; proposed cloud based IoT systems as RESCUE by Khan et al. in [65] are extensible for MEC platforms. Leveraging UAVs for disaster relief missions specialized in crowd localization is an effective use case that MEC can contribute for enhancing the performance [34].

5.3 Challenges for Wide Adaptation of 5G

The wide adaptation of 5G for IoT realization is imminent. The networking infrastructure standardized for 5G is different from LTE based deployments in both access and core network formation. Thus, following aspects can be presented as major challenges for 5G realization.

URLLC capabilities are burdening the security engineers in applying appropriate level of security for communication protocols and payload overheads. Thus, novel cryptographic means should be investigated to minimize the overhead drastically. **Massive IoT applications** are creating issues for resource utilization at the edge in terms of processing, communication, and networking aspects with the proliferated IoT devices. Managing security is evidently arduous in such circumstances. **Energy efficiency** of both UEs and intermediary resource constrained edge nodes are quite vital for the service continuity. Thus, energy saving mechanisms (i.e. hibernation), energy harvesting techniques, and energy optimum processing are quite crucial for 5G deployments.

Service migration is becoming an imminent aspect of edge computing; and with local 5G operator based gNBs. Security concerns associated with migration process in terms of virtualization technologies, MNO domains, and handover handling should be investigated thoroughly. **Scalable security** requirements are vital for 5G based deployments where security and latency have a clear trade-off. Thus, security features/ mechanisms should be applied in accordance to the requisites from the application and its priority level. **Orchestration** is the most researched aspect in virtualization domain; which requires complete autonomous control embedded with intelligence in case of edge computing. Security is a vital function under orchestration, and should be standardized for autonomous operation.

6 CONCLUSION

Security and Privacy are vital requirements for upcoming digital services that holds similar significance to performance metrics. Therefore, robustness of a particular application against cyber-intrusions is a demanding factor for raising its selectivity among consumers. However, security flaws should be investigated according to a deployment scenario for accurate identification of vulnerabilities and mapping existing security solutions to mitigate them. In this paper, we stated various vulnerabilities and attacks that range through cyber and physical space. The standardized MEC architecture has aided us to specify the flaws unique to each use case. Novel security solutions that are proposed for cyber-physical systems, ICN, NFV, and other impending technologies are mapped for each use case in the MEC context. The excessive discussion on assimilated facts and future directives are reinforcing our proposals with comprehension. As this survey focus on multiple use cases, it is our hope that, scientists working on these novel areas will find the presented insights valuable.

ACKNOWLEDGEMENT

This work is partly supported by the Academy of Finland under the 6Genesis (grant no. 318927) project.

REFERENCES

[1] Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie. 2018. Mobile Edge Computing: A Survey. IEEE Internet of Things Journal 5, 1 (2018), 450–465.

[2] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. 2016. Next generation 5G wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials 18, 3 (2016), 1617–1655.

[3] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 2017. 5G security: Analysis of threats and solutions. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 193–199.

[4] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 2018. Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine 2, 1 (2018), 36–43.

[5] Adnan Aijaz and Mahesh Sooriyabandara. 2019. The Tactile Internet for Industries: A Review. Proc. IEEE 107, 2 (2019), 414–435.

[6] Abdelkader Aissioui, Adlen Ksentini, Abdelhak Mourad Gueroui, and Tarik Taleb. 2018. On Enabling 5G Automotive Systems Using Follow Me Edge-Cloud Concept. IEEE Transactions on Vehicular Technology 67, 6 (2018), 5302–5316.

[7] Ali Al-Shuwaili and Osvaldo Simeone. 2017. Energy-efficient Resource Allocation for Mobile Edge Computing-based Augmented Reality Applications. IEEE Wireless Communications Letters 6, 3 (2017), 398–401.

[8] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. Internet of Things Security: A Survey. Journal of Network and Computer Applications 88 (2017), 10–28.

[9] Amina Antonacci, Fabiana Arduini, Danila Moscone, Giuseppe Palleschi, and Viviana Scognamiglio. 2018. Nanostructured (Bio) Sensors for Smart Agriculture. TrAC Trends in Analytical Chemistry 98 (2018), 95–103.

[10] Axelle Apvrille. 2019. Augmented Reality Visualization Device for Network Security. US Patent App. 10/178,130.

[11] Michael Bartock, Jeffrey Cichonski, and Murugiah Souppaya. 2020. 5G Cybersecurity: Preparing a Secure Evolution to 5G. Technical Report. National Institute of Standards and Technology.

[12] Jordi Mongay Batalla, Elzbieta Andrukiewicz, German Peinado Gomez, Piotr Sapiecha, Constandinos X Mavromoustakis, George Mastorakis, Jerzy Zurek, and Muhammad Imran. 2020. Security risk assessment for 5G networks: National perspective. IEEE Wireless Communications 27, 4 (2020), 16–22.

[13] Pete Beckman, Charlie Catlett, Moinuddin Ahmed, Mohammed Alawad, Linquan Bai, Prasanna Balaprakash, Kevin Barker, Pete Beckman, Randall Berry, Arup Bhuyan, et al. 2020. 5G Enabled Energy Innovation: Advanced Wireless Networks for Science, Workshop Report. Technical Report. USDOE Office of Science (SC)(United States).

[14] Vimal Bhatia, Pragya Swami, Sanjeev Sharma, and Rangeet Mitra. 2020. Non-orthogonal multiple access: an enabler for massive connectivity. Journal of the Indian Institute of Science 100, 2 (2020), 337–348.

[15] Stefano bianchi. 2017. ANASTACIA Project - Advanced Networked Agents for Security and Trust Assessment in CPS / IoT Architectures. http://www.anastacia-h2020.eu/ last accessed May 16, 2019.

[16] Kashif Bilal and Aiman Erbad. 2017. Edge Computing for Interactive Media and Video Streaming. In 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 68–73.

[17] Bartosz Boguslawski, Matthieu Boujonnier, Loryne Bissuel-Beauvais, Fahd Saghir, Rajesh D Sharma, et al. 2018. IIoT Edge Analytics: Deploying Machine Learning at the Wellhead to Identify Rod Pump Failure. In SPE Middle East Artificial Lift Conference and Exhibition. Society of Petroleum Engineers.

[18] Mohammad Borhani, Madhusanka Liyanage, Ali Hassan Sodhro, Pardeep Kumar, Anca Delia Jurcut, and Andrei Gurtov. 2020. Secure and resilient communications in the industrial internet. In Guide to Disaster-Resilient Communication Networks. Springer, 219–242.

[19] An Braeken, Pawani Porambage, Amirthan Puvaneswaran, and Madhusanka Liyanage. 2020. ESSMAR: Edge Supportive Secure Mobile Augmented Reality Architecture for Healthcare. In 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech). IEEE, 1–7.

[20] Yue Cao, Omprakash Kaiwartya, Yuan Zhuang, Naveed Ahmad, Yan Sun, and Jaime Lloret. 2018. A Decentralized Deadline-driven Electric Vehicle Charging Recommendation. IEEE Systems Journal 99 (2018), 1–12.

[21] Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, Weixiao Meng, and Jiamin Liu. 2017. Machine-to-Machine Communications in Ultra-Dense Networks—-A Survey. IEEE Communications Surveys & Tutorials 19, 3 (2017), 1478–1503.

[22] Xi Chen, Zonghang Li, Yupeng Zhang, Ruiming Long, Hongfang Yu, Xiaojiang Du, and Mohsen Guizani. 2018. Reinforcement learning–based QoS/QoE-aware service function chaining in software-driven 5G slices. Transactions on Emerging Telecommunications Technologies 29, 11 (2018), e3477.

[23] Edgar Lemos Cid, Manuel Garcia Sanchez, and Ana Vazquez Alejos. 2016. Wideband Analysis of the Satellite Communication Channel at KU and X-bands. IEEE Transactions on Vehicular Technology 65, 4 (2016), 2787–2790.

[24] Mirsad Cosovic, Achilleas Tsitsimelis, Dejan Vukobratovic, Javier Matamoros, and Carles Anton-Haro. 2017. 5G Mobile Cellular Networks: Enabling Distributed State Estimation for Smart Grids. IEEE Communications Magazine 55, 10 (2017), 62–69.

[25] Jose Costa-Requena. 2014. SDN integration in LTE mobile backhaul networks. In The International Conference on Information Networking 2014 (ICOIN2014). IEEE, 264–269.

[26] Chamitha De Alwis, Anshuman Kalla, Quoc-Viet Pham, Pardeep Kumar, Kapal Dev, Won-Joo Hwang, and Madhusanka Liyanage. 2021. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. IEEE Open Journal of the Communications Society (2021).

[27] Jasenka Dizdarević, Francisco Carpio, Admela Jukan, and Xavi Masip-Bruin. 2019. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Computing Surveys (CSUR) 51, 6 (2019), 116.

[28] Lijun Dong and Guoqiang Wang. 2017. Information Centric Approach in Achieving Anycast Service in Machine Type Communications. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 157–162.

[29] Thang Le Duc, Rafael García Leiva, Paolo Casari, and Per-Olov Östberg. 2019. Machine learning methods for reliable resource provisioning in edge-cloud computing: A survey. ACM Computing Surveys (CSUR) 52, 5 (2019), 94.

[30] Ashutosh Dutta and Eman Hammad. 2020. 5G Security Challenges and Opportunities: A System Approach. In 2020 IEEE 3rd 5G World Forum (5GWF). IEEE, 109–114.

[31] Leila Eadie, Alasdair Mort, Luke Regan, Ashish S MacAden, and Philip Wilson. 2016. Remotely Supported Prehospital Ultrasound: Real-time Communication for Diagnosis in Remote and Rural Communities. In Proceedings of the 3rd European Workshop on Practical Aspects of Health Informatics. CEUR-WS.

[32] Mohammed S Elbamby, Cristina Perfecto, Mehdi Bennis, and Klaus Doppler. 2018. Toward Low-latency and Ultra-reliable Virtual Reality. IEEE Network 32, 2 (2018), 78–84.

[33] Mohammed Elbayoumi, Mahmoud Kamel, Walaa Hamouda, and Amr Youssef. 2020. NOMA-assisted machine-type communications in UDN: State-of-the-art and challenges. IEEE Communications Surveys & Tutorials 22, 2 (2020), 1276–1304.

[34] Milan Erdelj, Enrico Natalizio, Kaushik R Chowdhury, and Ian F Akyildiz. 2017. Help from the Sky: Leveraging UAVs for Disaster Management. IEEE Pervasive Computing 16, 1 (2017), 24–32.

[35] ETSI. 2016. Mobile Edge Computing (MEC) Framework and Reference Architecture. ETSI White Paper #3 (2016). https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf Last accessed 16 May 2019.

[36] EU-H2020. 2018. 5G-EVE. https://www.5g-eve.eu/ last accessed May 16, 2019.

[37] Dongfeng Fang and Yi Qian. 2020. 5G wireless security and privacy: Architecture and flexible mechanisms. IEEE Vehicular Technology Magazine 15, 2 (2020), 58–64.

[38] Ana Juan Ferrer, Joan Manuel Marquès, and Josep Jorba. 2019. Towards the Decentralised Cloud: Survey on Approaches and Challenges for Mobile, Ad hoc, and Edge Computing. ACM Computing Surveys (CSUR) 51, 6 (2019), 111.

[39] Abderrahime Filali, Amine Abouaomar, Soumaya Cherkaoui, Abdellatif Kobbane, and Mohsen Guizani. 2020. Multi-access edge computing: A survey. IEEE Access 8 (2020), 197017–197046.

[40] Shane Fonyi. 2020. Overview of 5G security and vulnerabilities. The Cyber Defense Review 5, 1 (2020), 117–134.

[41] Reham M Fouda. 2018. Security Vulnerabilities of Cyberphysical Unmanned Aircraft Systems. IEEE Aerospace and Electronic Systems Magazine 33, 9 (2018), 4–17.

[42] Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K Marina. 2017. Network slicing in 5G: Survey and challenges. IEEE Communications Magazine 55, 5 (2017), 94–100.

[43] Keke Gai, Meikang Qiu, Hui Zhao, and Jian Xiong. 2016. Privacy-aware adaptive data encryption strategy of big data in cloud computing. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE, 273–278.

[44] Keke Gai, Yulu Wu, Liehuang Zhu, Lei Xu, and Yan Zhang. 2019. Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks. IEEE Internet of Things Journal (2019).

[45] Sahil Garg, Amritpal Singh, Shalini Batra, Neeraj Kumar, and Laurence T Yang. 2018. UAV-empowered Edge Computing Environment for Cyber-threat Detection in Smart Vehicles. IEEE Network 32, 3 (2018), 42–51.

[46] Kuntal Gaur, Anshuman Kalla, Jyoti Grover, Mohammad Borhani, Andrei Gurtov, and Madhusanka Liyanage. 2021. A survey of Virtual Private LAN Services (VPLS): Past, present and future. Computer Networks (2021), 108245.

[47] Dennis Grewe, Marco Wagner, Mayutan Arumaithurai, Ioannis Psaras, and Dirk Kutscher. 2017. Information-Centric Mobile Edge Computing for Connected Vehicle Environments: Challenges and Research Directions. In Proceedings of the Workshop on Mobile Edge Communications. ACM, 7–12.

[48] Rajesh Gupta, Dakshita Reebadiya, and Sudeep Tanwar. 2021. 6G-enabled Edge Intelligence for Ultra-Reliable Low Latency Applications: Vision and Mission. Computer Standards & Interfaces 77 (2021), 103521.

[49] H2020. 2015. Small Cells Coordination for Multi-tenancy and Edge Services. http://www.sesame-h2020-5g-ppp.eu/Home.aspx last accessed May 16, 2019.

[50] Hajar Hantouti, Nabil Benamar, Tarik Taleb, and Abdelquoddous Laghrissi. 2018. Traffic Steering for Service Function Chaining. IEEE Communications Surveys & Tutorials (2018).

[51] Rémy Harel and Steve Babbage. 2016. 5G Security Recommendations Package 2: Network Slicing. https://www.ngmn.org/fileadmin/user_upload/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf Last accessed 16 May 2019.

[52] Daojing He, Sammy Chan, and Mohsen Guizani. 2018. Security in the Internet of Things Supported by Mobile Edge Computing. IEEE Communications Magazine 56, 8 (2018), 56–61.

[53] Tharaka Hewa, An Bracken, Mika Ylianttila, and Madhusanka Liyanage. 2020. Blockchain-based Automated Certificate Revocation for 5G IoT. In ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 1–7.

[54] Tharaka Hewa, An Braeken, Mika Ylianttila, and Madhusanka Liyanage. 2020. Multi-Access Edge Computing and Blockchain-based Secure Telehealth System Connected with 5G and IoT. In The 8th IEEE International Conference on Communications and Networking (IEEE ComNet'2020).

[55] Oliver Holland, Eckehard Steinbach, R Venkatesha Prasad, Qian Liu, Zaher Dawy, Adnan Aijaz, Nikolaos Pappas, Kishor Chandra, Vijay S Rao, Sharief Oteafy, et al. 2019. The IEEE 1918.1 "Tactile Internet" Standards Working Group and its Standards. Proc. IEEE 107, 2 (2019), 256–279.

[56] Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P Lauf, Lanier Watkins, William H Robinson, and Wlajimir Alexis. 2016. Securing Commercial Wifi-based UAVs from Common Security Attacks. In Military Communications Conference, MILCOM 2016. IEEE, 1213–1218.

[57] Mohammad Hosseini, Yu Jiang, Ali Yekkehkhany, Richard R Berlin, and Lui Sha. 2017. A Mobile Geo-communication Dataset for Physiology-aware Dash in Rural Ambulance Transport. In Proceedings of the 8th ACM on Multimedia Systems Conference. ACM, 158–163.

[58] Syed Husain, Andreas Kunz, Athul Prasad, Konstantinos Samdanis, and JaeSeung Song. 2018. Mobile edge computing with network resource slicing for internet-of-things. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 1–6.

[59] Razin Farhan Hussain, Mohsen Amini Salehi, Anna Kovalenko, Saeed Salehi, and Omid Semiari. 2018. Robust Resource Allocation Using Edge Computing for Smart Oil Fields. In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA). The Steering Committee of The World Congress in Computer Science, Computer …, 204–210.

[60] Muhammad Javed, Elyes Ben Hamida, Ala Al-Fuqaha, and Bharat Bhargava. 2017. Adaptive Security for Intelligent Transport System Applications. IEEE Intelligent Transportation Systems Magazine 10, 2 (2017), 110 – 120.

[61] Dushantha Nalin K Jayakody, Kathiravan Srinivasan, and Vishal Sharma. 2019. 5G Enabled Secure Wireless Networks. Springer.

[62] Anca D Jurcut, Pasika Ranaweera, and Lina Xu. 2020. Introduction to IoT security. IoT Security: Advances in Authentication (2020), 27–64.

[63] Fahad Khan, Atiq ur Rehman, Muhammad Arif, Muhammad Aftab, and Baber Khan Jadoon. 2016. A Survey of Communication Technologies for Smart Grid Connectivity. In 2016 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube). IEEE, 256–261.

[64] Rabia Khan, Pardeep Kumar, Dushantha Nalin K Jayakody, and Madhusanka Liyanage. 2019. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions. IEEE Communications Surveys & Tutorials (2019).

[65] Taher Khan, Saptarshi Ghosh, Muddesar Iqbal, George Ubakanma, and Tasos Dagiuklas. 2018. RESCUE: A Resilient Cloud Based IoT System for Emergency and Disaster Recovery. In 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 1043–1047.

[66] Adlen Ksentini and Pantelis A Frangoudis. 2020. Toward slicing-enabled multi-access edge computing in 5g. IEEE Network 34, 2 (2020), 99–105.

[67] Neeraj Kumar, Sherali Zeadally, and Joel JPC Rodrigues. 2016. Vehicular Delay-tolerant Networks for Smart Grid Data Management Using Mobile Edge Computing. IEEE Communications Magazine 54, 10 (2016), 60–66.

[68] Rakesh Kumar, MP Singh, Prabhat Kumar, and JP Singh. 2015. Crop Selection Method to Maximize Crop Yield Rate Using Machine Learning Technique. In 2015 international conference on smart technologies and management for computing, communication, controls, energy and materials (ICSTM). IEEE, 138–145.

[69] Shankar Lal, Tarik Taleb, and Ashutosh Dutta. 2017. NFV: Security Threats and Best Practices. IEEE Communications Magazine 55, 8 (2017), 211–217.

[70] Michael Langfinger, Michael Schneider, Didier Stricker, and Hans D Schotten. 2017. Addressing Security Challenges in Industrial Augmented Reality Systems. In Industrial Informatics (INDIN), 15th International Conference on. IEEE, 299–304.

[71] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. In 2018 IEEE Symposium on Security and Privacy (SP). IEEE.

[72] Chiking Lee. 2018. Discovering Cyber Vulnerabilities in SCADA Control System via Examination of Water Treatment Plant in Laboratory Environment. The UNSW Canberra at ADFA Journal of Undergraduate Engineering Research 9, 1 (2018).

[73] Craig Lee and Andrea Fumagalli. 2019. Internet of Things Security-Multilayered Method For End to End Data Communications Over Cellular Networks. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 24–28.

[74] Jong-Hyouk Lee and Hyoungshick Kim. 2017. Security and Privacy Challenges in the Internet of Things [Security and Privacy Matters]. IEEE Consumer Electronics Magazine 6, 3 (2017), 134–136.

[75] Helen C Leligou, Theodore Zahariadis, Lambros Sarakis, Eleftherios Tsampasis, Artemis Voulkidis, and Terpsichori E Velivassaki. 2018. Smart Grid: A Demanding Use Case for 5G Technologies. In 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 215–220.

[76] A Leonardi, K Mathioudakis, A Wiesmaier, and F Zeiger. 2014. Towards the Smart Grid: Substation Automation Architecture and Technologies. Advances in Electrical Engineering 2014 (2014).

[77] Bin Li, Zesong Fei, and Yan Zhang. 2018. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. IEEE Internet of Things Journal (2018).

[78] Chao Li, Yushu Xue, Jing Wang, Weigong Zhang, and Tao Li. 2018. Edge-oriented computing paradigms: A survey on architecture design and system management. ACM Computing Surveys (CSUR) 51, 2 (2018), 39.

[79] Meng Li, Richard Yu, Pengbo Si, and Yanhua Zhang. 2018. Energy-efficient Machine-to-Machine (M2M) Communications in Virtualized Cellular Networks with Mobile Edge Computing (MEC). IEEE Transactions on Mobile Computing (2018).

[80] Chung-Wei Lin and Alberto Sangiovanni-Vincentelli. 2017. Security-Aware Design for V2V Communication. In Security-Aware Design for Cyber-Physical Systems. Springer, 77–86.

[81] Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila. 2018. A comprehensive guide to 5G security. Wiley Online Library.

[82] Madhusanka Liyanage, Ijaz Ahmed, Mika Ylianttila, Jesus Llorente Santos, Raimo Kantola, Oscar Lopez Perez, Mikel Uriarte Itzazelaia, Edgardo Montes De Oca, Asier Valtierra, and Carlos Jimenez. 2015. Security for future software defined mobile networks. In 2015 9th international conference on next generation mobile applications, services and technologies. IEEE, 256–264.

[83] Madhusanka Liyanage, An Braeken, Pardeep Kumar, and Mika Ylianttila. 2020. IoT security: Advances in authentication. John Wiley & Sons.

[84] Madhusanka Liyanage, Pawani Porambage, Aaron Yi Ding, and Anshuman Kalla. 2021. Driving Forces for Multi-Access Edge Computing (MEC) IoT Integration in 5G. ICT Express (2021).

[85] Pavel Mach and Zdenek Becvar. 2017. Mobile Edge Computing: A Survey on Architecture and Computation Offloading. IEEE Communications Surveys & Tutorials 19, 3 (2017), 1628–1656.

[86] Martin Maier, Mahfuzulhoq Chowdhury, Bhaskar Prasad Rimal, and Dung Pham Van. 2016. The Tactile Internet: Vision, Recent Progress, and Open Challenges. IEEE Communications Magazine 54, 5 (2016), 138–145.

[87] Olli Mäkinen. 2015. Streaming at the Edge: Local Service Concepts Utilizing Mobile Edge Computing. In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies. IEEE, 1–6.

[88] Yuyi Mao, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B Letaief. 2017. A Survey on Mobile Edge Computing: The Communication Pserspective. IEEE Communications Surveys & Tutorials 19, 4 (2017), 2322–2358.

[89] Jeremy Mitchell, David Soldani, and Malcolm Shore. 2018. The Path to 5G in Australia: Architecture Evolution from 4G to 5G. http://huaweihub.com.au/wp-content/uploads/2018/07/The-path-to-5G-in-Australia-03-August-2018-2.pdf Last accessed 16 May 2019.

[90] Amin Mohammadali, Mohammad Sayad Haghighi, Mohammad Hesam Tadayon, and Alireza Mohammadi-Nodooshan. 2018. A Novel Identity-based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. IEEE Transactions on Smart Grid 9, 4 (2018), 2834–2842.

[91] Andrés Molina. 2018. Water Governance in the Smart City. WIT Transactions on The Built Environment 179, 1 (2018), 13–22.

[92] Naser Hossein Motlagh, Miloud Bagaa, and Tarik Taleb. 2017. UAV-based IoT Platform: A Crowd Surveillance Use Case. IEEE Communications Magazine 55, 2 (2017), 128–134.

[93] Arash Nourian and Stuart Madnick. 2018. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. IEEE Transactions on Dependable and Secure Computing 15, 1 (2018), 2–13.

[94] Vanga Odelu, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti. 2018. Provably Secure Authenticated Key Agreement Scheme for Smart Grid. IEEE Transactions on Smart Grid 9, 3 (2018), 1900–1910.

[95] University of Oulu. 2020. 6G-FLAGSHIP. https://www.oulu.fi/6gflagship/ last accessed April 30, 2021.

[96] Oulu. 2018. Multi-Access Edge Computing (MEC) Artificial Intelligence (AI). http://www.edgeai.info/project/mec-ai/ last accessed May 16, 2019.

[97] Emmanuel Oyekanlu, Charles Nelatury, Alfred O Fatade, Olumuyiwa Alaba, and Ola Abass. 2017. Edge Computing for Industrial IoT and the Smart Grid: Channel Capacity for M2M Communication Over the Power Line. In 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON). IEEE, 1–11.

[98] Christoph Pallasch, Stephan Wein, Nicolai Hoffmann, Markus Obdenbusch, Tilman Buchner, Josef Waltl, and Christian Brecher. 2018. Edge Powered Industrial Control: Concept for Combining Cloud and Automation Technologies. In 2018 IEEE International Conference on Edge Computing (EDGE). IEEE, 130–134.

[99] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. 2017. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems 18, 11 (2017), 2898–2915.

[100] Imtiaz Parvez, Ali Rahmati, Ismail Guvenc, Arif I Sarwat, and Huaiyu Dai. 2018. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. IEEE Communications Surveys & Tutorials 20, 4 (2018), 3098–3130.

[101] Charith Perera, Chi Harold Liu, and Srimal Jayawardena. 2015. The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey. IEEE Transactions on Emerging Topics in Computing 3, 4 (2015), 585–598.

[102] Jonathan Petit and Steven E Shladover. 2015. Potential Cyberattacks on Automated Vehicles. IEEE Trans. Intelligent Transportation Systems 16, 2 (2015), 546–556.

[103] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. 2021. The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society 2 (2021), 1094–1122.

[104] Pawani Porambage, Jude Okwuibe, Madhusanka Liyanage, Mika Ylianttila, and Tarik Taleb. 2018. Survey on Multi-Access Edge Computing for Internet of Things Realization. IEEE Communications Surveys & Tutorials 20, 4 (2018), 2961–2991.

[105] Xiuquan Qiao, Pei Ren, Schahram Dustdar, and Junliang Chen. 2018. A New Era for Web AR with Mobile Edge Computing. IEEE Internet Computing 22, 4 (2018), 46–55.

[106] Pengxiang Qin, Pinyi Ren, Qinghe Du, and Li Sun. 2018. Security Enhancement for IoT Video Streaming via Joint Network Coding and Retransmission Design. In International Conference on Internet of Things as a Service. Springer, 40–47.

[107] Hamed Rahimi, Ali Zibaeenejad, and Ali Akbar Safavi. 2018. A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 81–88.

[108] Archana Rajakaruna, Ahsan Manzoor, Pawani Porambage, Madhusanka Liyanage, Mika Ylianttila, and Andrei Gurtov. 2019. Enabling end-to-end secure connectivity for low-power iot devices with uavs. In 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW). IEEE, 1–6.

[109] Pasika Ranaweera, Vashish N Imrith, Madhusanka Liyanag, and Anca Delia Jurcut. 2020. Security as a service platform leveraging multi-access edge computing infrastructure provisions. In ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 1–6.

[110] Pasika Ranaweera, Anca Delia Jurcut, and Madhusanka Liyanage. 2019. Realizing Multi-Access Edge Computing Feasibility: Security Perspective. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 1–7.

[111] Pasika Ranaweera, Anca Delia Jurcut, and Madhusanka Liyanage. 2021. Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials (2021).

[112] Ashish Rauniyar, Paal Engelstad, Boning Feng, et al. 2016. Crowdsourcing-based Disaster Management using Fog Computing in Internet of Things Paradigm. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). IEEE, 490–494.

[113] Danda B Rawat and Chandra Bajracharya. 2016. Vehicular Cyber Physical Systems: Adaptive Connectivity and Security. Springer.

[114] Partha Pratim Ray, Mithun Mukherjee, and Lei Shu. 2017. Internet of Things for Disaster Management: State-of-the-art and Prospects. IEEE Access 5 (2017), 18818–18835.

[115] Zeineb Rejiba, Xavier Masip-Bruin, and Eva Marín-Tordera. 2019. A survey on mobility-induced service migration in the fog, edge, and related computing paradigms. ACM Computing Surveys (CSUR) 52, 5 (2019), 90.

[116] Jinke Ren, Guanding Yu, Yunlong Cai, and Yinghui He. 2018. Latency Optimization for Resource Allocation in Mobile-Edge Computation Offloading. IEEE Transactions on Wireless Communications 17, 8 (2018), 5506–5519.

[117] Ju Ren, Deyu Zhang, Shiwen He, Yaoxue Zhang, and Tao Li. 2019. A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet. ACM Computing Surveys (CSUR) 52, 6 (2019), 125.

[118] Alex Reznik, Yonggang Fang, and Saad Ullah. 2018. MEC in an Enterprise Setting : A Solution Outline. ETSI White Paper #30 2, 30 (2018). https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_FINAL.pdf Last accessed 16 May 2019.

[119] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. 2018. Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. Future Generation Computer Systems 78 (2018), 680–698.

[120] Harri Saarnisaari, Sudhir Dixit, Mohamed-Slim Alouini, Abdelaali Chaoub, Marco Giordani, Adrian Kliks, Marja Matinmikko-Blue, Nan Zhang, Anuj Agrawal, Mats Andersson, et al. 2020. A 6G white paper on connectivity for remote areas. arXiv preprint arXiv:2004.14699 (2020).

[121] Matthew NO Sadiku, Shumon Alam, and Sarhan M Musa. 2017. Information assurance benefits and challenges: An introduction. Information & Security 36, 1 (2017), 1–5.

[122] Miguel Saez, Steven Lengieza, Francisco Maturana, Kira Barton, and Dawn Tilbury. 2018. A Data Transformation Adapter for Smart Manufacturing Systems with Edge and Cloud Computing Capabilities. In 2018 IEEE International Conference on Electro/Information Technology (EIT). IEEE, 0519–0524.

[123] S Salsano. 2015. Superfluidity: A Super-fluid, Cloud-native, Converged Edge System. http://superfluidity.eu/ last accessed May 16, 2019.

[124] Mike Scavezze, Jason Scott, Jonathan Steed, Ian McIntyre, Aaron Krauss, Daniel McCulloch, Stephen Latta, Kevin Geisner, and Brian Mount. 2015. User Authentication on Augmented Reality Display Device. US Patent 9,092,600.

[125] Hichem Sedjelmaci, Ines Ben Jemaa, Makhlouf Hadji, and Arnaud Kaiser. 2018. Security Framework for Vehicular Edge Computing Network Based on Behavioral Game. In 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 1–6.

[126] Vahe Seferian, Rouwaida Kanj, Ali Chehab, and Ayman Kayssi. 2018. Identity based Key Distribution Framework for Link Layer Security of AMI Networks. IEEE Transactions on Smart Grid 9, 4 (2018), 3166–3179.

[127] Syed Noorulhassan Shirazi, Antonios Gouglidis, Arsham Farshad, and David Hutchison. 2017. The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective. IEEE Journal on Selected Areas in Communications 35, 11 (2017), 2586–2595.

[128] Syed Noorulhassan Shirazi, Antonios Gouglidis, Kanza Noor Syeda, Steven Simpson, Andreas Mauthe, Ioannis M Stephanakis, and David Hutchison. 2016. Evaluation of Anomaly Detection Techniques for SCADA Communication Resilience. In 2016 Resilience Week (RWS). IEEE, 140–145.

[129] Meryem Simsek, Adnan Aijaz, Mischa Dohler, Joachim Sachs, and Gerhard Fettweis. 2016. 5G-enabled Tactile Internet. IEEE Journal on Selected Areas in Communications 34, 3 (2016), 460–473.

[130] Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. 2016. A survey on cloud computing security: Issues, threats, and solutions. Journal of Network and Computer Applications 75 (2016), 200–222.

[131] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. 2021. AI and 6G security: Opportunities and challenges. In Proc. IEEE Joint Eur. Conf. Netw. Commun.(EuCNC) 6G Summit. 1–6.

[132] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylinattila. 2021. A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications and technical aspects. IEEE Communications Surveys & Tutorials (2021).

[133] Yushan Siriwardhana, Pawani Porambage, Mika Ylianttila, and Madhusanka Liyanage. 2020. Performance Analysis of Local 5G Operator Architectures for Industrial Internet. IEEE Internet of Things Journal 7, 12 (2020), 11559–11575.

[134] Prakash Suthar, Vivek Agarwal, Rajaneesh Sudhakar Shetty, and Anil Jangam. 2020. Migration and Interworking between 4G and 5G. In 2020 IEEE 3rd 5G World Forum (5GWF). IEEE, 401–406.

[135] Rahim Tafazolli, Chin-Liang Wang, Periklis Chatzimisios, and Madhusanka Liyanage. 2021. The Wiley 5G REF: Security,. Wiley Online Library.

[136] Irina Tal and Gabriel-Miro Muntean. 2018. Towards reasoning vehicles: A survey of fuzzy logic-based solutions in vehicular networks. ACM Computing Surveys (CSUR) 50, 6 (2018), 80.

[137] Elisabeth Uhlemann. 2017. The US and Europe Advances V2V Deployment [Connected Vehicles]. IEEE Vehicular Technology Magazine 12, 2 (2017), 18–22.

[138] Muhammad Usman, Muhammad Rizwan Asghar, Imran Shafique Ansari, and Marwa Qaraqe. 2018. Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. IEEE Access 6 (2018), 58064–58074.

[139] Jianyu Wang, Jianli Pan, Flavio Esposito, Prasad Calyam, Zhicheng Yang, and Prasant Mohapatra. 2019. Edge cloud offloading algorithms: Issues, methods, and perspectives. ACM Computing Surveys (CSUR) 52, 1 (2019), 2.

[140] Meisong Wang, Prem Prakash Jayaraman, Rajiv Ranjan, Karan Mitra, Miranda Zhang, Eddie Li, Samee Khan, Mukkaddim Pathan, and Dimitrios Georgeakopoulos. 2015. An Overview of Cloud based Content Delivery Networks: Research Dimensions and State-of-the-art. In Transactions on Large-Scale Data-and Knowledge-Centered Systems XX. Springer, 131–158.

[141] Qian Wang, Zhi Chen, Weidong Mei, and Jun Fang. 2017. Improving Physical Layer Security Using UAV-enabled Mobile Relaying. IEEE Wireless Communications Letters 6, 3 (2017), 310–313.

[142] Shalitha Wijethilaka and Madhusanka Liyanage. 2021. Survey on network slicing for internet of things realization in 5g networks. IEEE Communications Surveys & Tutorials (2021).

[143] Lin Xiang, Derrick Wing Kwan Ng, Robert Schober, and Vincent WS Wong. 2018. Cache-enabled Physical Layer Security for Video Streaming in Backhaul-limited Cellular Networks. IEEE Transactions on Wireless Communications 17, 2 (2018), 736–751.

[144] L. Xu, A. D. Jurcut, and H. Ahmadi. 2019. Emerging Challenges and Requirements for Internet of Things in 5G. In 5G-Enabled Internet of Things. CRC Press.

[145] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. 2018. Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles. IEEE Internet of Things Journal 5, 6 (2018), 5015–5029.

[146] Anil Kumar Yadav and Prerna Gaur. 2014. AI-based Adaptive Control and Design of Autopilot System for Nonlinear UAV. Sadhana 39, 4 (2014), 765–783.

[147] Shan-Shan Yang, Ji-Wei Pang, Xiao-Man Jin, Zhong-Yang Wu, Xiao-Yin Yang, Wan-Qian Guo, Zhi-Qing Zhao, and Nan-Qi Ren. 2018. Let a Sewage Plant Running Smart. In IOP Conference Series: Earth and Environmental Science, Vol. 127. IOP Publishing, 012013.

[148] Xiao Yang, Zhiyong Chen, Kuikui Li, Yaping Sun, Ning Liu, Weiliang Xie, and Yong Zhao. 2018. Communication-constrained Mobile Edge Computing Systems for Wireless Virtual Reality: Scheduling and Tradeoff. IEEE Access 6 (2018), 16665–16677.

[149] Zhong Yang, Mingzhe Chen, Xiao Liu, Yuanwei Liu, Yue Chen, Shuguang Cui, and H Vincent Poor. 2021. Artificial Intelligence Driven UAV-NOMA-MEC in Next Generation Wireless Networks. arXiv preprint arXiv:2101.11681 (2021).

[150] E Yeh, Junil Choi, N Prelcic, C Bhat, and R Heath. 2016. Security in Automotive Radar and Vehicular Networks. Microwave Journal (2016).

[151] Faqir Zarrar Yousaf, Marco Gramaglia, Vasilis Friderikos, Borislava Gajic, Dirk von Hugo, Bessem Sayadi, Vincenzo Sciancalepore, and Marcos Rates Crippa. 2017. Network slicing with flexible mobility and QoS/QoE support for 5G Networks. In 2017 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 1195–1201.

[152] Ashkan Yousefpour, Caleb Fung, Tam Nguyen, Krishna Kadiyala, Fatemeh Jalali, Amirreza Niakanlahiji, Jian Kong, and Jason P Jue. 2019. All One Needs to Know About Fog Computing and Related Edge Computing Paradigms: A Complete Survey. Journal of Systems Architecture (2019).

[153] Aiqing Zhang, Lei Wang, Xinrong Ye, and Xiaodong Lin. 2017. Light-weight and Robust Security-aware D2D-assist Data Transmission Protocol for Mobile-health Systems. IEEE Transactions on Information Forensics and Security 12, 3 (2017), 662–675.

[154] Xi Zhang and Qixuan Zhu. 2017. Statistical Quality of Service Provisioning Over Edge Computing Mobile Wireless Networks. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 412–417.

[155] Fuhui Zhou, Yongpeng Wu, Haijian Sun, and Zheng Chu. 2018. UAV-enabled Mobile Edge Computing: Offloading Optimization and Trajectory Design. In 2018 IEEE International Conference on Communications (ICC). IEEE, 1–6.

[156] Yi Zhou, Phee Lep Yeoh, He Chen, Yonghui Li, Robert Schober, Li Zhuo, and Branka Vucetic. 2018. Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location. IEEE Transactions on Vehicular Technology 67, 11 (2018), 11280–11284.

[157] Qingyi Zhu, Seng W Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. 2019. Applications of Distributed Ledger Technologies to the Internet of Things: A Survey. ACM Computing Surveys (CSUR) 52, 6 (2019), 120.