Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges

Pietro Tedeschi and Savio Sciancalepore
Division of Information and Computing Technology (ICT)
College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar
e-mail: ptedeschi@mail.hbku.edu.qa, ssciancalepore@hbku.edu.qa

***Abstract*— The increasing integration of information and communication technologies has undoubtedly boosted the efficiency of Critical Infrastructures (CI). However, the first wave of IoT devices, together with the management of enormous amount of data generated by modern CIs, has created serious architectural issues. While the emerging Fog and Multi-Access Edge Computing (FMEC) paradigms can provide a viable solution, they also bring inherent security issues, that can cause dire consequences in the context of CIs.**

In this paper, we analyze the applications of FMEC solutions in the context of CIs, with a specific focus on related security issues and threats for the specific while broad scenarios: a smart airport, a smart port, and a smart offshore oil and gas extraction field. Leveraging these scenarios, a set of general security requirements for FMEC is derived, together with crucial research challenges whose further investigation is cornerstone for a successful adoption of FMEC in CIs.

I. Introduction

Fully automated computer systems nowadays manage and monitor civil and military Critical Infrastructures (CIs), including airports, ports, water treatment facilities, power plants, electricity grids, and oil and gas extraction fields [1]. Indeed, mobile technologies, embedded systems, smart devices, wireless communications, and the widespread diffusion of the Internet are facilitating the deployment of powerful and reliable solutions, ideal to be integrated in scenarios where a system failure can lead to catastrophic consequences [2].

In this context, Internet of Things (IoT) and Cloud Computing (CC) are key enabling technologies. Smart IoT devices equipped with sensing and actuation capabilities are spread in the CI area, with the task of monitoring the most important physical parameters, including temperature, light conditions, sudden acceleration or pressure changes [3]. These data are gathered on the Cloud, where they could be processed, e.g., via powerful Machine Learning (ML) techniques, to predict failures, identify intrusions and conceive adequate countermeasures to face sudden changes in the environment [4].

Despite the glaring advantages, when dealing with large networks and a huge amount of data — a typical CIs scenario — such solutions suffer from severe limitations. IoT devices are typically constrained, thus not being able to process a large amount of data. At the same time, the CC paradigm is based on pool of servers deployed in convenient physical locations, often very far from where data are originated [5]. These lead to large delays in data reporting, as well as significant latencies in the application of corrective actions.

To overcome these limitations, innovative solutions have been designed, leading to the emergence of the Edge Computing (EC) and Fog Computing (FC) architectural paradigms. Despite resorting to different strategies, these emerging architectural solutions bring the Cloud and the IoT access network close to each other, enabling real-time applications and processing of data in the local network [6].

Recent contributions successfully integrated the emerging Fog and Mobile Edge Computing (FMEC) computing paradigms in the IoT, with significant advantages in terms of reduced response times and energy consumption [7]-[10]. In the context of CIs, where the size of the networks scales up to thousands of devices, FMEC paradigms can provide substantial gains, especially from the monetary perspectives. Being operated typically also thanks to public funds, the economic sustainability of CIs is often a particularly sensitive topic. This is one of the reasons motivating the strong appeal that FMEC have for CIs deployments, as confirmed by recent investments of the major companies [11]-[15]. For instance, according to Deloitte, by 2019, 45% of IoT-created data in oil and gas extraction fields will be stored, processed, analyzed and acted upon close to or at the edge of the network [16].

Motivated by these efforts, in this paper we provide a thorough analysis of the applications and the threats emerging from the integration of FMEC technologies in next-generation smart CIs. Our analysis tackles three reference use-cases, including a smart airport, a smart port, and a smart offshore oil and gas extraction field. With reference to these scenarios, we analyze the motivations attracting the major companies toward the evolution of legacy CC technologies in FMEC architectures. In addition, we identified how the vulnerabilities and potential weaknesses inherent of FMEC architectures map to the identified scenarios, pointing out the major threats for each reference use-case. Our study results in a set of security requirements to be fulfilled by any FMEC solution deployed in a CI, as well as in a set of topical research challenges required to assure a dependable deployment.

The rest of the paper is organized as follows. Sec. II introduces our reference scenarios, while Sec. III describes the emerging FMEC paradigms and general security issues.

Sec. IV details the adoption of FMEC architectures in CIs, while Sec. V highlights the issues arising from FMEC in CIs. Sec. VI draws the possible future research directions, while Sec. VII presents the conclusions.

II. Smart Critical Infrastructures

Optimizing and protecting CI elements is becoming, even more, a cornerstone challenge for any modern country. Indeed, shortening processing times, reducing costs and guaranteeing the reliability and robustness of the whole management chain are crucial requirements to maintain the well-being of the country and maximize the revenues. In the following, we review three use-cases of CIs where digitization and computerization are indeed a reality.

A. Smart Airports

In recent years, the booming of the global civil aviation industry has witnessed continuous and rapid increases in passenger traffic and airline revenues. According to the latest statistics of the International Air Transport Association (IATA), global demand for air travel is grown by 7.0% in 2018, and the total number of air passengers is expected to soar to 4.36 billion [17].

The reports by aviation authorities and involved companies show that global airport ICT investments are mostly focused on upgrading passenger service items, travel safety, mobile commerce, and new technologies. Indeed, airports are undergoing a digital transformation toward smart operations and development, paying even greater attention to business continuity, reliability, and stability. This is where IoT and Cloud-based solutions could definitively find a suitable application scenario.

The key idea of a smart airport is to deploy a capillary IoT network, integrated and managed via a Cloud-based smart IoT platform, to both support passenger needs and improve airports efficiency [18]. The IoT cloud-based platform allows managing several types of data, leveraging advanced analytics, artificial intelligence and machine learning techniques. The data will be collected from airlines, drone inspections, passengers, incident reports and IoT devices spread in the airport, to provide optimal experiences for the passengers.

From the user perspective, an IoT platform in a smart airport could be compared to a personal assistant. It is characterized by omnipresence capabilities and pervasive powers, advising on the best possible options at each step of the user journey, based on real-time data. In this sense, the smart usage of several data sources in an airport can provide multiple advantages to the passenger, i.e., reducing queues at check-in, improving the management and the control, suggesting best routes to the gates, suggesting shopping solutions based on the users' preferences, suggesting connections with other transportation solutions, and minimizing lost luggages events. On the airport side, deploying a capillary IoT network has the potential of improving the efficiency in the personnel usage, as well as the reduction of planes taxing, fueling and boarding times. At the same time, the deployment of sensing and actuation capabilities have also the potential of increasing safety, as hazardous situations (dangerous chemical substances, explosive materials and dangerous intrusion, such as drones) could be timely detected, located and neutralized, minimizing their impact on the airport operation and reducing the economic losses. Indeed, the environmental impact of airport operations on the ecosystem surrounding the area of operations could be also reduced, as the optimal path is suggested to the airplanes and empty parking spots are adequately indicated to the passengers, reducing fuel emissions.

Nowadays, with the proliferation of the number of passengers, the management of large amounts of data is definitively one of the main challenges of the airport sector. The adoption of IoT and ML technologies is allowing to improve the services, but require a persistent connection to powerful Cloud services. In this context, operators such as Huawei has already started the deployment of smart and connected airports, integrating IoT and Cloud-based solutions [19].

B. Smart Ports

Ports represent an increasingly important junction for any country, hosting several hundreds of vessels and thousands of containers every day. A regular port of a medium-size city is fully equipped for docking of vessels of different sizes, stopping and repairing ships. It allows also the loading and unloading of cargo ships and the embarkation/disembarkation of people.

Such a wide area needs efficient, capillary and smart monitoring techniques. Indeed, containers arriving from ships docking at the port needs to be (i) recognized, (ii) indexed, (iii) their travel path and management chain should be attested, and (iv) they need to be stored in appropriate locations. At the same time, specific requirements for goods inside the containers need to be absolutely fulfilled. For instance, refrigerated containers should be placed in strategic locations, where the light and heat of the sun would not affect their operation. In addition, containers transporting sensitive chemical items should be isolated and constantly surveilled, to avoid unintended leakages and contaminations. Furthermore, manual operations at the port should be constantly monitored to avoid any kind of misuse and hazard. Containers transporting materials not allowed in a specific country should be seized and surveilled all the time to avoid unauthorized movements. At the same time, computing and storage systems archiving all the history of containers passing the port should be appropriately secured against any unauthorized access and handling of files.

A real example of a port using smart computing and advanced technologies to provide enhanced services is the Port of Rotterdam, in the Netherlands, usually considered as one of the smartest ports in the world [14]. The full area of the port, approximately 42 squares km, is equipped with IoT technologies and Cloud-based solutions. Thanks to the deployed IoT network, the operators have created a *digital twin* of the port, i.e., an exact digital replica of the operations in the port. It mirrors all available resources, including the infrastructure, weather, geographical and water depth data.

Artificial Intelligence (AI) and smart weather data are orchestrated in the Cloud to measure important metrics, including the availability of berths and other vital statistics. For instance, accurate water and weather data allow shipping companies to predict the best time to enter the port, by identifying the most favorable conditions. This is possible thanks to the coordination between the pervasive IoT network and the powerful Cloud infrastructure. IoT sensors spread all around the port, including also water, allow to access data about air temperature, wind speed, (relative) humidity, turbidity, and salinity of the water, water flow intensity and levels, tides and currents, and many others. On the Cloud, these data are integrated and processed to better predict the visibility on a given day, as well as to calculate clearance heights for ships. In addition, by predicting water conditions, wind direction and speed, the docking personnel is able to determine how smooth a ship can enter into the port. Furthermore, machine learning is applied in the Cloud to learn the patterns from sensed data, so that port operators could be able to rely on accurate, real-time data about the port's infrastructure.

Overall, such an efficient CI has a significant positive economic impact on shipping costs. Calm water and weather conditions allow for lower fuel consumption rates, facilitate cost-effective per-ship payloads and help ensure the safe arrival of cargo, maximizing revenues for the port operators. Finally, it is worth noting that a precisely-controlled ship could reduce at minimum the environmental impact of human operations on the coastal landscape, enhancing the touristic attraction of the area.

C. Smart Offshore Oil and Gas Extraction Sites

Valued at $103 billion in the U.S. in 2018, the oil and gas industry is definitively one of the main pillars of any modern country, as a well as a core element of the CI of a nation [20]. Compared to the other CIs, oil, and gas extraction sites are usually located in remote and hard-to-reach areas, with few population and Internet connection facilities in the nearby, mainly because of environmental and safety factors.

Providing high-speed internet connection and cloud facilities in such a hostile environment is indeed a challenge. As a matter of fact, a dedicated infrastructure, such as a satellite connection, should be deployed to allow the whole site to be connected and reachable via Internet. At the same time, the sensitivity of the extraction operations and the equipment used for these activities impose very tight timing and latency requirements.

Once an issue on the extraction equipment is identified, the operations need to be immediately suspended, and corrective action must be taken immediately. However, the speed at which the countermeasures are applied can be severely impacted by the speed at which they can be applied in the field. This is where tank level forecasting, via predictive maintenance, could help. Indeed, the integration among IoT devices, sensors and machine learning algorithms applied on the Cloud, could manage and abate the aforementioned issues, identifying problems in time and applying a quick remediation. To provide a glaring example, one of the most prominent problems affecting production in gas wells is liquid loading, which is the inability of gas to remove liquids being produced in the wellbore. The extraction process of the gas requires a hole to be physically drilled in the ground, for the purpose of exploration and extraction of natural resources. The issue of liquid loading occurs when the speed of the gas in its ascending move drops below a *critical speed*. The produced liquid accumulates in the well, creating a static column of liquid. The liquid creates a back pressure against formation pressure that forms within the pores of a formation rock, increasing until the well ceases production. In this case, early prediction of gas slow-down is vital to prevent huge economic losses, as well to reduce at minimum the environmental impact of extraction operations.

To address the above issues, oil and gas companies today increasingly combine the IoT, ML and the CC technologies to achieve a pervasive and ubiquitous management of remote facilities. Specifically, predictive maintenance algorithms are continuously applied, so that the companies can act in real-time as safety and regulatory issues arise, minimizing economic losses.

Indeed, the IoT and Cloud computing technology add tremendous benefits to the way oil and gas extraction activities are conducted. Smart IoT platforms, such as the one provided by Losant[1], Link-Labs[2] and Biz4Intellia[3] technologies, to name a few, help transforming raw data acquired from sensors and coming from mines, pumps, or job sites into cost savings and more efficient operations. Sensors and actuators deployed in the extraction sites and remotely controlled via the Cloud precisely monitor pumps, synchronize data from multiple systems, and empower site operators to make business decisions based on real-time information. In addition, by retrofitting or manufacturing the equipment with connected IoT sensors, it is possible to monitor the condition of machines in the field, to offer low-cost condition-based maintenance solutions to customers.

III. Edge and Fog Computing Paradigms

Starting from a brief overview of the main limitations of the CC paradigm, this section introduces the emerging FMEC technologies, highlighting also the general security issues associated with their adoption.

A. Cloud Computing: Benefits and Limitations

Since its introduction, the CC concept has attracted the interest of network designers as well as application developers. Thanks to the possibility of outsourcing data to powerful pools of configurable computing resources via a regular data connection, CC enabled ubiquitous, convenient and on-demand services [21]. At the same time, the requirements on the users' devices are minimal, if compared to the advantages. Indeed, individuals, developers, and organizations could finally get

[1]Losant Enterprise IoT Platform - https://www.losant.com/

[2]Link Labs - https://www.link-labs.com/

[3]Biz4intellia - https://www.biz4intellia.com/

rid of instantiating, configuring and managing powerful and critical servers, gaining time and resources.

The undoubted business perspectives of the Cloud Computing paradigm did not go unnoticed to the major IT companies. Thus, Amazon, Google, Microsoft, eBay, and many others invested billions of dollars in developing and providing powerful cloud infrastructures for the provision of their services to the users.

In the context of CIs, the advent of the cloud has finally released the full potential of the IoT. Before the introduction of the CC, the benefits of IoT devices in terms of pervasiveness and penetration in wild environments have been often mitigated by the limited processing capabilities and storage resources available on-board. With the CC, instead, the enormous amount of data gathered by constrained devices are entrusted to the Cloud, where storage and processing are not limited. In addition, in the context of CIs, the CC drastically reduces costs, as there is no need for skilled personnel in charge of the setup, installation, and maintenance of crucial servers. This is a very important factor, as CIs are often maintained via public funds, often scarce and subject to tight regulations.

Despite the wide range of benefits, CC brings also several drawbacks. They include:

- **Increased Delay in Data Reporting.** By offloading computationally and time intensive tasks, data need to be stored on the Cloud before any operation can take place. This increases the end-to-end delay between data acquisition and processing. For real-time tasks, very frequent especially in CIs monitoring, this further delay could be an issue.
- **Increased Latency in Accessing the User Network**. If the interfaces providing access to the IoT devices are hosted on the cloud, any data coming from the user and directed to the IoT network needs to be processed on the Cloud. This adds an extra delay, that could be an issue in case of hard-time tuning operations.
- **Limited Customization**. Applications and services hosted on the Cloud are associated with an agreed service level, namely, a Service Level Agreement (SLA) between the provider and the customer. In case further customizations are needed, e.g., prioritization of a given process rather than another type of traffic, this is quite hard to be achieved in short time.
- **Increased Reliance on the External Network.** Besides the cost of the service negotiated with the provided via the SLA, the user has to face the issue of the increased volume of traffic directed to the external network. In the best case, this implies an extra cost derived from the subscription of a plan with the Internet Service Provider (ISP), allowing for more data to be uploaded to the Cloud. In the worst case, the reliance on persistent Internet connection could be an issue, especially when the network could not be connected to the Internet for physical limitations.
- **Data Privacy**. Focusing on security issues, entrusting data and computation to the Cloud poses serious privacy issues. A malicious cloud service provider could not only access the data but also manipulate them and sell them to other parties. In addition, outsourced data could be also lost or deleted intentionally [22], [23].

B. Fog and Edge Computing in a Nutshell

The FC and EC paradigm arise leveraging the weaknesses of the CC architectures. Without loss of generality, these technologies often named as *Extended Cloud*, get resources for processing and storage closer to the user. The way this move is achieved is at the basis of their difference. The EC solution envisions sensors, actuators, and mobile devices to take a crucial role in processing, storage, and computation task, processing data locally rather than sending them towards the Cloud. The FC paradigm, instead, moves resources from the cloud closer to the source of data, typically to the gateway of the local network or to the next hop [24]. A qualitative architectural overview is depicted in Fig. 1.

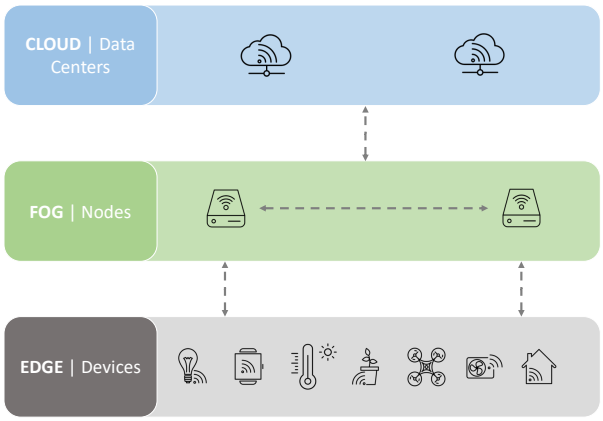

Figure 1. Fog and Edge Computing Architecture.

These architectural shifts provide evident benefits in the quality of provided services, as they result in a consistent reduction of delays in reporting data and latency in accessing information [25]. These improvements are particularly important especially in the context of the future 5G systems, where there are stringent requirements on the need to provide a customized and advanced user-centric value at an affordable price, the enabling of context-aware proximity services and advanced multimedia-centric services in crowd areas [26].

Further advantages can be achieved. Relying on dedicated nodes in the proximity, users can offload computations to more powerful devices without worrying about too high processing times, as data are processed in an ultra-low latency environment, with high bandwidth and real-time access to radio and network analytics. Moreover, location-aware services could be provided, enabling location-based caching services and content distribution. Furthermore, end-users could use dedicated resources available on site for processing and computations, without relying necessarily on a fixed infrastructure on the

Cloud. Finally, a consistent less amount of data is entrusted to the Cloud, reducing the risk of privacy leakages due to the Cloud operators snooping.

EC and FC have a parallel but independent evolution. EC was initially conceived in the context of mobile networks, especially cellular. Thus, it was immediately known as Mobile Edge Computing. In an effort to give a precise characterization and to standardize functions and procedures, European Telecommunications Standards Institute (ETSI) launched an Industry Specification Group (ISG) on purpose in December 2014, namely ISG MEC, resulting in a number of documents describing specifications and a reference architecture [27]. However, the technology experts involved in the group soon realized that the initial definition left out several access points, whose processing capabilities may also construct the edge of a network. Thus, since September 2016, ETSI has changed the official name of the group to *Multi-Access Edge Computing*, to reflect that the edge includes also other fixed-access technologies, including WiFi.

FC, instead, was introduced by Cisco Systems in 2012. Indeed, it was initially considered as an extension of the CC paradigm providing computation, storage, and networking services between end devices and traditional cloud servers [6]. Since that, several contributions reviewed and expanded the concept along several directions, including also resource-constrained and more powerful servers in the definition of a *Fog* node. At this time, the FC architecture is being further developed in the OpenFog Consortium, which started in 2015 and entered the stage of standardization end of 2017 [28].

Because of their similar objectives, FC and EC are often referred as *Extended Cloud*. In the following, we will use the terminology FMEC to indicate concepts associated with both FC and EC. Instead, we will detail the specific technology in case a particular notion involves one rather than the other.

An overview of the main differences between EC, FC and CC is provided in the following Tab. I.

C. Security Issues

Despite the evident advantages, FMEC are still in their early deployment phase, and a number of issues are quickly arising as the technology is adapted on the particular scenario. In this context, security issues stem in a prominent position, and mainly inherit weaknesses from the enabling technologies, such as IoT and CC.

Specifically, the following security issues are often associated with the design and deployment of FMEC-based solutions:

- **Location exposure**. The FMEC paradigms entrust local computations to constrained devices and local servers. Despite the numerous advantages, this offers to the attackers a clear indication of the location of the devices to be targeted to break the system. Indeed, an attacker could target the portion of the network closer to the physical location of the target to achieve its objective.
- **Traffic Analysis**. With the CC, the management traffic among distributed computational entities was exchanged between servers in the Cloud or within single devices. With the upcoming FMEC technologies, the geographical distribution of the computational network is widely increased, thanks to the participation of Fog servers and Edge IoT devices. Thus, the management traffic becomes exposed and subject to traffic analysis. Without the necessary modifications, clear-text flows become fully exposed to the adversary, while encrypted traffic could be subject to analysis based on traffic features, such as the packet size and interarrival times.
- **Privacy**. Involving Edge but constrained IoT devices in local computations undoubtedly create potential vulnerabilities. Indeed, IoT devices could be associated to different vendors, being not fully trusted. At the same time, they could have access to a wide range of information regarding the network, including data gathered from the physical environment and information about interacting devices. If a malware or a backdoor is injected, intentionally or unintentionally, sensitive information could be leaked.
- **Virtualization Issues**. With specific reference to the FC paradigm, virtualization is the main enabling technology [29]. With a so high degree of geographical distribution, virtualized images should be delivered via web, as well as they could be installed in servers located in untrusted physical locations. There are high chances of distribution of compromised images, as well as cloning of images.
- **Denial of Service (DoS)**. Classic DoS attacks based on resource exhaustion over CC architectures, either based on bandwidth congestion or processing capabilities saturation, are quite complex to achieve, given that they require the knowledge of the physical location of the servers, as well as huge resources to saturate powerful geographically distributed servers. With the shift to FMEC architectures, a consistent less amount of resources are needed to cause a DoS, both because IoT Edge devices and Fog Servers are less powerful than CC units, and because their location can be easily guessed.
- **Jamming**. The FMEC paradigm enables wireless technologies to be part of the Extended Cloud. Indeed, edge devices and machines in charge of processing-hungry operations could use also WiFi and Cellular links to communicate with neighboring components. Despite providing evident advantages, compared with CC-oriented architectures, the adoption of FMEC architectures is exposed to the possibility that an adversary disrupts the operation of critical computation points via wireless jamming.
- **Availability (Weak Elasticity)**. One of the main strengths of the CC paradigm was indeed the possibility of dynamically allocating the processing load through multiple distributed machines. With the move of processing capabilities closer to the user, the overall network architecture loses any dynamic capacity of meeting workload demands, dynamic provisioning and de-provisioning of resources, as well as the capacity to meet unpredictable

Table I
COMPARISON BETWEEN FMEC AND CC PARADIGMS.

	Edge Computing	**Fog Computing**	**Cloud Computing**
Latency in Accessing Data	Low	Medium	High
Delay in Reporting Data	Low	Medium	High
Processing and Storage Location	IoT devices	IoT gateway or one-hop away	Distributed over the Internet
Reliance on Local Network	High	Medium	Low
Geographical Network Distribution	Low	Medium	High
Customization of Services	High	Medium	Low

resource demands, operational, software and hardware failures, being subject to the well-known single-point-of-failure issue.

- **Trusting Edge Devices**. CC technologies were usually managed by single owners. Thus, an implicit trust between servers and computing devices could be safely assumed. This is not true anymore for FMEC solutions, where edge IoT devices and Fog elements from different vendors should collaborate and exchange information. Thus, effective authentication solutions, as well as reliable access control techniques, implemented at a higher layer of the network architecture, are indeed necessary.

IV. MOVING CRITICAL INFRASTRUCTURES TO THE EDGE

In smart CIs, the speed of data analysis and the predictions on these data can improve the efficiency of a decision-making system, thus emerging as key points to guarantee a reactive service. In the following, the benefits derived from the integration of FMEC solutions in each of the reference CIs are discussed.

Smart Airports. A large amount of data collected by IoT devices in a smart airport are regularly sent to the Cloud, in order to be processed and analyzed. Indeed, the huge amount of traffic generated by IoT devices currently pose several challenges, including the enormous bandwidth required to manage persistent connections, network delays and latencies issues, as well as response times [30]. This is exactly where fog and edge computing play a crucial role.

Instead of entrusting any computation to the Cloud-based IoT platform, edge IoT devices spread in the airport area could take part of the computations. For instance, IoT devices spread in the internals of the airport could collaborate to take local decisions, such as regulating the temperature close to a terminal because of people concentration, indicating to the passengers the best route towards its terminal, and suggesting to the user the most suitable shops according to its preferences.

Within the operational area of the airport, fully local automatic systems based on RFID scanning and IoT devices could guide the baggage towards the right and optimal path towards the location of the airplane, minimizing lost baggage episodes, as well as long delays in the delivering of the baggage. For local computations, edge IoT devices could be used, without involving communications with the Cloud. This could also have a parallel privacy enhancement since cloud servers could avoid managing sensitive data about passengers.

At the same time, airplanes in the landing phase could be driven by IoT sensors towards the best path to their hangar, leveraging only local operations. Such an innovative technique requires very stringent delays and minimum latencies in the communication between IoT devices on the runway and the devices on the airplanes, that could not be achieved if communication with far Cloud servers is involved. Instead, by deploying computational units in the proximity of the runway, the latencies can be minimized and an effective guide of the airplanes could be achieved, also avoiding sudden obstacles and other airplanes on the path.

Many providers, such as SITA [11] and Huawei[12], are already deploying combined IoT and FMEC solutions to improve services in the airports, with the Athens International Airport and the Hong Kong Airport being between the most important play area of this capillary deployment.

Smart Ports. In a smart port, tens of thousands of containers, transportation equipment, instruments, cameras, and personnel frequently exchange data with each other through wireless networks. Despite smart technologies such as the IoT have penetrated in the port scenario, many terminal operators still lack a reliable and dedicated wireless connectivity infrastructure that can ensure operational efficiency for cargo handling, employee safety, and data security.

Thus, moving processing power and facilities close to the port location could provide several enhancements in the network architectures. Summarizing, the following main advantages can be identified: (i) sensors reporting time reduction, (ii) equipment control optimization, (iii) real-time access to video surveillance, and (iv) customized applications deployment.

A pervasive sensor network such as the one deployed in the Port of Rotterdam generates a very high amount of data, requiring a consistent amount of computational resources to be processed. For instance, modeling and tracking ship movements, weather data, geographical insights, and water depth data with extreme accuracy require the application of computationally intensive ML algorithms. In addition, such algorithms could be even more accurate, as data is continuously and timely filled in the processing. Thanks to edge computing devices, the data gathered from the sensors do not need to travel the core network anymore, but they can be processed locally and almost in real-time. This provides a reduction in the sensors reporting time, as well as increased control over actuation systems deployed in the port. Indeed, modifications issued manually or automatically could reach the involved equipment in almost real-time. As a consequence,

it enhances the efficacy of the deployed solutions, bringing consistent monetary gains both to vessels and port operators.

With thousands of cameras monitoring every corner of the port in real time, employees could be able to inspect their operations through their hand-held mobile terminals. When a regular Cloud-based solution is deployed, network latency wildly fluctuates and video playback often stalls, severely affecting work efficiency. But, thanks to local edge servers, video data could be distributed locally to the closest edge processing server, so delays could be significantly reduced and video playback is much smoother.

In addition, a FMEC solution can integrate third-party applications related to video optimization, as well as dedicated firewalls, directly on EC devices. Also, the CC center of the smart port is moved to the edge Cloud, greatly improving the user experience.

Many providers, including Huawei and Nokia, are already working on bringing the FMEC benefits into smart port deployments [13].

Smart Offshore Oil and Gas Extraction. In the context of oil and gas extraction, the FMEC paradigms have the potential to be a disruptive cost-cutting solution [31]. As highlighted in Sec. II-C, the IoT deployment in offshore oil and gas extraction sites allows the devices used in exploration to gather data and to forward it to the Cloud, where they can be quickly analyzed and assessed from a central location. Undoubtedly, this process generates a very large amount of data, requiring at the same time very fast processing, as a decision made on them could result in operational time and cost savings.

Indeed, the following main advantages can be achieved by adapting Multi-access Edge Computing (MEC) principles in a Smart Offshore Oil and Gas Extraction: (i) processing time reduction, (ii) exploration systems uptime increase, (iii) higher productivity, and (iv) reduced energy consumption.

A huge advantage is the possibility to place processing power into remote locations. Undoubtedly, this allows a consistent less amount of traffic to be delivered to the Cloud server via dedicated satellite connections, as the raw data gathered from the extraction equipment no longer needs to be moved across long distances. This also translates in a consistent cost reduction, as the dedicated network could be sized to manage a consistent less amount of data.

A second benefit is the increase in exploration systems uptime. Greater processing power available directly at the edge translates into the possibility to immediately analyze data coming from the oil and gas wells. This allows to spot equipment difficulties or failures sooner with respect to a classic cloud-based approach and to schedule a fix before unanticipated downtime occurs. As for the previous case, this minimizes services interruption time and allows to gain up to a million dollars per hour depending upon the nature of the operation.

Finally, higher productivity and reduced energy consumption can be achieved together, as local processing power is available to fine-tune exploration well operations. Indeed, to ensure efficient equipment operations, pumping devices require constant monitoring and parameters tuning. In these operations, minimum latency is essential: as soon as a change in the structure of the underlying ground is detected, a change in the power and direction used by the equipment is immediately needed to avoid leakages or, in the worst case, more severe consequences on the environment. Thanks to FMEC devices located very close to the remote site, very fast reporting and reaction times can be achieved, reducing the power when necessary and maintaining optimal productivity levels.

Companies such as Petrolytics are at the forefront to push the integration of edge computing in oil and gas extraction fields [15].

V. Fog and Edge Computing in Critical Infrastructures: Threats and Risks

The security issues discussed in Sec. III-C can have devastating consequences when contextualized in the complex operations of Critical Infrastructures. Indeed, services offered by CIs are directly connected with the environmental health and safety management system. While improving the service can provide a clear step ahead in their protection and efficiency, vast and distributed cyber-attacks are often simplified to the attackers, with possible dreadful consequences.

Without loss of generality, three main threats can be identified when contextualizing the security issues of Fog and Multi-Access Edge Computing in CIs. They include: (i) service interruption, (ii) data leakage, and (iii) data integrity. Tab. II highlights the main threats, while a detailed discussion is provided in the following.

A. Service Interruption

Indeed, the main weakness derived from the integration of FMEC paradigms in the context of the deployment of CIs is the location exposure. When the CC paradigm is involved, attackers could only target specific IP addresses of servers frequently involved in communication between the local IoT devices and the IoT platform. However, because of the intrinsic nature of the CC paradigm, shutting down a single server could not assure to the attacker that the specific physical area using that server was without service. Indeed, this is not true for the FMEC paradigm, anymore. Thanks to the nature of the service, it is enough for the attacker to focus on edge and fog devices that are located physically closer to the CI, to have high chances of a successful attack. These attacks can be performed in many ways. The simplest option is to recur to a wide-area and geographically distributed jamming of the wireless connections, including WiFi and cellular. However, a service interruption can be also achieved by saturating the bandwidth and the processing capabilities of edge and fog devices. Given that computations and traffic management in FMEC architectures are performed on closer but less powerful devices, exhausting their resources could be achieved with substantial less effort.

In a smart airport managed via a FMEC architecture, an attacker could focus on servers and routers operating within

the airport to completely shutdown the wireless connectivity to the users and the airport personnel, and to block all automatized operations. As some computations are performed locally and then delivered to Cloud servers via wireless connections, the airport could be unable to access data about the position of the passengers in the airport area, as well as data regarding the position and the internal route of the airplanes, losing the connection with them and causing serious safety issues to people on-board.

In a smart port, losing the connection could have serious risks, especially for the companies and the port operator. Indeed, the ships could not be guided to the most feasible location anymore, using more fuel than the necessary to find a right spot. Without connection, a ship could also decide to move on a part of the port that could not host it, because of too high weight or size. This can cause the ship to be stranded, causing the block of the operations also for several days. Without connection, containers could not be positioned in optimal locations. This can lead to a quick degradation of the transported items, because of an inadequate storage.

The consequences of a connection freeze on an offshore oil and gas extraction platform can be devastating, specifically from an environmental perspective. Indeed, without connectivity to main processing sources, human operators have to rely only on their experience and to raw data from the wired sensors to extract the raw materials from the ground. Without the intelligence of distributed computing algorithms, leakages can occur, leading to huge economic losses for the company involved in the operation. At the same time, raw materials can pour into the sea, causing incalculable damages to the coastal environment, as well as to the surrounding flora and fauna.

B. Data Leakage

With the CC paradigm, all the data gathered by IoT devices were reported to the Cloud, for further processing. With the transition to FMEC architecture, the aggregation of the data takes place closer to the location where they are produced. While this speeds up the processing and the eventual detection of intrusions and failures, it also offers to the attacker a great opportunity to access them in a one-shot, without looking for traffic patterns on the web. In the context of CIs, this implies that personal and secret data passing through the sensors, gateways, and fog computing devices could be leaked to third-parties, with consequences on the large-scale.

The video data streams generated by IP-enabled cameras and camera-equipped sensors in ports and airports are delivered to the respective FMEC nodes, for temporary storage and further processing. The privacy of the streams should be carefully protected, as they include visual and audio data that can be used by third-parties to extract valuable and sensitive information.

In a smart airport, threats for people using the services are coupled with threats experienced by smart CIs operators. Sensitive conversations between people about personal and business operations could be leaked, potentially revealing industrial secrets or personal sensitive information. In addition, information about the transit of a person could be leaked, enabling unauthorized tracking of a person and access to personal preferences, including the visited shops and places. Overall, this causes a serious privacy issue, and it could have consequences also on the legal plane if the smart airport operator is indicated as a guilt for the negligence.

In a smart port, instead, not only current real-time information but also the full history of vessels and containers could be leaked. This could reveal information about the path of a vessel, to be further used by attackers for malicious purposes in further journeys of the same vessel. In addition, it could reveal the nature of the goods transported by specific containers, pointing thieves right to the containers transporting the goods of their interest. Furthermore, data about the specific conditions in which transported goods should be conserved could be leaked, and then further used by attackers to compromise them.

Similarly, in an offshore oil and gas extraction platform, leakage of the data could lead to the disclosure of industrial secrets related to the algorithms and the nature of data gathered by smart extraction devices. In turn, these could lead to huge economic losses, as unauthorized third-parties can sell these data to competitor companies, able to extract more value and infer further information.

C. Data Integrity

The involvement of IoT devices and gateways in the collection and processing of local information makes them attractive targets for an attacker aiming at altering the correct operation of CIs. Exploiting poor practices in the management of access control and weak authentication techniques originating from an implicit trust between the components of the system, attackers could modify or delete information. In the deployment of smart CIs, modifying data could have devastating consequences on people, companies and the environment.

In a smart airport, modifications to the data can cause issues on people safety and companies. Indeed, airplanes taxiing on the runway could be diverted on purpose out from their intended route, possibly blocking the traffic of the whole airport and attempting at the safety of the people on-board.

In a smart port, readings of the water level sensors could be modified on purpose to drive the ships towards not suitable areas, where they can remain stalled also for days. This would cause the stop of the operation, leading to consistent economic losses. In addition, attackers could modify the information related to the containers, e.g., the current readings of the temperature sensors within the containers, the values of the accelerometers and the location data reported by location receivers. Thus, the food in the container could rot without any detection. Moreover, the oscillations of the container because of a bad placement or intentional movements can be undetected, leading to the fall of the container and the loss of any goods stored therein. Furthermore, containers could be moved and stolen without any detection mechanism in place. Overall, these threats would cause huge economic losses to the company managing the smart port, as well as further legal

actions against them, because of direct or indirect negligence on surveillance tasks.

In smart offshore oil and gas extraction sites, attackers could modify stored information about the pressure and the nature of the ground or could delete information leading the early identification of a fault on the extraction equipment. Combining these attacks, devastating consequences can occur. In the best case, the fault of an extraction device would lead to the temporary stop of the production, until the fix or the replacement of the device, with waiting times up to weeks. In the worst case, the ground can be drilled in wrong places or using erroneous speed and techniques, leading to the leakage of the raw materials in the surrounding environment. Besides the huge environmental damages, consequences on the monetary plane would be catastrophic, considering the loss of money derived from the spill of the raw material and from the pollution and the irrecoverable damages to the environment.

D. Security Requirements for a Smart Critical Infrastructure

With a look at the threats derived in previous subsections, a set of security requirements to be achieved by any smart CI are provided in the following.

- **Physical Devices Security**. Edge devices physical security is a compelling requirement. While in regular IoT networks the constrained devices managed limited and not critical tasks, in the FMEC paradigms they are important nervous point of the network. Indeed, if an attacker gains access to an edge device, it could gain access to a higher architectural level of the network, causing serious issues on the variety of devices trusting higher-layers network elements.
- **Authentication of Edge Devices**. Differently, from the CC paradigm, smart devices working at the edge of smart CIs cannot be automatically trusted anymore. Indeed, they are exposed to direct contact with people and users, thus being at high risk of being compromised.
- **Access Control at the Edge**. Despite being authenticated, edge devices deployed in the CIs could be easily hacked or either cloned, thus trying to read or modify data that they should not be able to touch, neither for reading nor for modifications. Thus, lightweight access control solutions must be in place at the edge of the network, to ensure authorized access to resources between FMEC elements of the network.
- **Privacy-preserving Information Management**. The privacy issue of the CC paradigm is not solved, but only moved to FMEC devices, that are more exposed than Cloud servers to intrusions. Thus, privacy-preserving solutions should be applied also at the edge of the network.
- **Availability**. While in an industrial scenario a temporary stop to wireless activities could be disruptive only for the economy of the single company, stopping services of CIs has devastating consequences also on people and environment, likely stopping a whole nation and its international connections. Thus, a FMEC-enabled CI should be able to detect timely DoS and Jamming Attacks, and promptly switching to alternative paths able to guarantee continuous availability. In this sense, Intrusion Detection System (IDS) should work at the edge to ensure the continuous connection of the CI to essential functions.
- **Resilience**. A resilient framework, able to detect failures, as well as safely and quickly rolling back to safe recovery points is a requirement for every CI. In turn, this requires smart and efficient solutions able to establish the most feasible time instant where images of the system should be taken, as well as smart storage of such images.

VI. Research Challenges

Despite the integration of FMEC computing paradigms in the context of CIs has been already triggered, still, several security challenges need to be addressed. They include:

- **Scalable Authentication Solutions for Edge Devices**. The authentication processes involving edge devices must require minimum execution times and fast re-keying procedures. Indeed, long key exchange procedures, e.g. via online consulting of Public Key Infrastructure (PKI) or mutual sharing of Public Key Certificates, would lead to high delays, eliminating any performance gain introduced by FMEC paradigms.
- **Access Control in Heterogeneous Environments**. Managing authorization between non-trusted domains is a challenge toward the secure deployment of FMEC elements in smart CIs. For instance, in a smart offshore oil and gas extraction field, an IoT device monitoring and regulating the pressure of extraction equipment should receive data coming from one or more fog devices positioned in nearby cellular base-stations, possibly owned by different Mobile Network Operators (MNOs). In such a context, negotiating the agreement with single communicating parties would not scale up with the size of the network, as every different manufacturer of IoT devices would setup a different access control logic with the fog device. Possible winning solutions could leverage the federation of different ecosystems across shared and trusted attributes, requiring minimal access latencies.
- **Privacy-Preserving FMEC deployment**. Guaranteeing minimal data losses and privacy leakages when dealing with compromised devices is indeed a topical research challenge. Emerging technologies, such as Homomorphic and Searchable Encryption have indeed the potential to offload data to untrusted entities, without allowing them to access their content, alleviating these concerns. However, scalable and lightweight solutions, possibly leveraging offloading strategies, are still needed.
- **Advanced IDS.** To guarantee the availability, CIs requires effective IDSs, based on powerful ML solutions, able to immediately identify events leading to a DoS. However, designing and tuning an IDS that can work in a large-scale, geo-distributed, and heterogeneous mobile environment is still a challenge.
- **Backup Solutions.** At the detection time, the system should be able to switch the architectural context, possi-

Table II
THREATS ON FMEC-ENABLED CIS

Use Case	Threats		
	Service Interruption	*Data Leakage*	*Data Integrity*
Airports	No dedicated user experience On board safety of people Airplanes connection loss	People sensitive data leakage People tracking Companies industrial secrets	Airline path deviation Low-quality services to passengers Passengers data tampering
Ports	Transported items degradation No ships navigation control No port area surveillance	Containers path leakage Containers tracking Port secrets disclosure	Ships hijacking Intentional goods degradation Containers theft
Oil and Gas Extraction Sites	Manual equipment control Manual area exploration Human-driven raw materials extraction	Industrial secrets disclosure Manufacturing process leakage Extraction points revelation	Undetected equipment degradation Extraction data compromise Undetected raw materials leakage

bly rolling back to a Cloud-based architecture. Designing and orchestrating such a complex system is indeed a challenge, and has to deal with likely increase of costs.

VII. CONCLUSIONS

The increasing adoption of FMEC technologies in modern CIs brings undeniable improvements in terms of latencies and delays. However, these very same technologies expose the CIs to unforeseen threats, requiring innovative solutions to tackle the upcoming security challenges. In this context, dependable solutions are highly needed to trigger the adoption of FMEC concepts in CIs, paving the way to pervasive applications at the service of users, companies, and the natural ecosystem.

ACKNOWLEDGEMENTS

This publication was partially supported by awards NPRP-S-11-0109-180242, UREP23-065-1-014, and NPRP X-063-1-014 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF.

REFERENCES

[1] L. Cazorla, C. Alcaraz, and J. Lopez, "Cyber Stealth Attacks in Critical Information Infrastructures," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1778–1792, June 2018.

[2] A. Carelli, A. Vallero, and S. Di Carlo, "Performance Monitor Counters: interplay between safety and security in complex Cyber-Physical Systems," *IEEE Trans. on Device and Materials Reliability*, 2019.

[3] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3453–3495, Oct. 2018.

[4] Z. Zohrevand, U. Glässer, M. A. Tayebi, H. Y. Shahir, M. Shirmaleki, and A. Y. Shahir, "Deep Learning Based Forecasting of Critical Infrastructure Data," in *Proceedings of the ACM on Conference on Information and Knowledge Management*, ser. CIKM '17, 2017, pp. 1129–1138.

[5] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, Feb 2018.

[6] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[7] H. Li, K. Ota, and M. Dong, "Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, Jan. 2018.

[8] M. Palattella, R. Soua, K. Abdelmajid, and T. Engel, "Fog Computing as the Key for Seamless Connectivity Handover in Future Vehicular Networks," in *34th ACM Symposium On Applied Computing (SAC)*, 2019.

[9] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia, and G. Bianchi, "On the Design of a Decentralized and Multiauthority Access Control Scheme in Federated and Cloud-Assisted Cyber-Physical Systems," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5190–5204, Dec 2018.

[10] R. Roman, R. Rios, J. A. Onieva, and J. Lopez, "Immune System for the Internet of Things using Edge Technologies," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[11] Sita-Aero, https://www.sita.aero/air-transport-it-review/articles/iot-crucial-to-smart-airport, 2018, accessed: 2019-03-06.

[12] Huawei, https://www.airport-technology.com/news/huawei-rolls-smart-airport-2-0-solution/, 2018, accessed: 2019-03-06.

[13] Equiniz Blog, "China Unicom and Huawei Jointly Launch Industry-First 5G Edge-Cloud Smart Port ," Technical Report, Apr. 2017.

[14] IBM, "Turning Rotterdam into the "World's Smartest Port" with IBM Cloud & IoT," Technical Report, Jan. 2018.

[15] S. Hill, https://iot.eetimes.com/iot-ai-and-edge-computing-are-transforming-the-oil-industry/, 2018, accessed: 2019-03-06.

[16] A. Hand, https://www.automationworld.com/oil-and-gas-edge, 2017, accessed: 2019-03-06.

[17] IATA, https://www.iata.org/pressroom/pr/Pages/2018-11-06-02.aspx, 2018, accessed: 2019-03-06.

[18] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience," in *Global Internet of Things Summit (GIoTS)*, Jun. 2018, pp. 1–6.

[19] Huawei, https://www.huawei.com/en/press-events/news/2018/6/Huawei-Smart-Airport-2-Solution, 2018, accessed: 2019-03-06.

[20] Equiniz Blog, "How the Oil and Gas Industry is Powered by the IoT, Machine Learning and Cloud," Technical Report, Dec. 2017.

[21] NIST, "The NIST definition of cloud computing," Technical Report, 2011.

[22] F. Lombardi and R. Di Pietro, *Security for Cloud Computing*. Springer Science & Business Media, 2015, vol. 38.

[23] R. Di Pietro and A. Sorniotti, "Proof of ownership for deduplication systems: a secure, scalable, and efficient solution," *Computer Communications*, vol. 82, pp. 71–82, 2016.

[24] K. Munir, *Advancing Consumer-Centric Fog Computing Architectures*. IGI Global, 2018.

[25] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," *IEEE Journ. on Sel. Areas in Communications*, vol. 35, no. 11, pp. 2586–2595, Nov 2017.

[26] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Communications Surveys Tutorials*, vol. 19, no. 3, pp. 1657–1681, Jul. 2017.

[27] ETSI GS MEC, "Mobile Edge Computing (MEC) Terminology; v1.1.1," Standard 001, Mar. 2016.

[28] OpenFog Consortium, https://www.openfogconsortium.org/, 2015, accessed: 2019-03-06.

[29] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of network and computer applications*, vol. 34, no. 4, pp. 1113–1122, 2011.

[30] S. Bouyakoub, A. Belkhir, F. M. Bouyakoub, and W. Guebli, "Smart Airport: An IoT-based Airport Management System," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, ser. ICFNDS '17, 2017, pp. 45:1–45:7.

[31] R. F. Hussain, M. Salehi, A. Kovalenko, S. Salehi, and O. Semiari, "Robust Resource Allocation Using Edge Computing for Smart Oil Fields," in *Proceedings of the International Conference on Parallel and Distributed Processing Techniques & Applications*, Jul. 2018.