Wireless Personal Communications (2021) 120:2409–2426
https://doi.org/10.1007/s11277-021-08554-5

Security Threat Analysis of the 5G ESSENCE Platform

Ioannis P. Chochliouros[1] · Anastasia S. Spiliopoulou[1] · Alexandros Kostopoulos[1] · Michail-Alexandros Kourtis[2] · Pavlos I. Lazaridis[3] · Zaharias D. Zaharis[4] · Neeli R. Prasad[5]

Accepted: 26 April 2021 / Published online: 9 May 2021

Abstract
The present paper discusses several security requirements coming from assessment of the use cases developed within the context of the original 5G-PPP "5G ESSENCE" project. Following to a concrete introduction to the project's main innovative features and the description of all selected use cases coming directly from the vertical markets, we have separately assessed each one among them towards identifying security threats affecting the development of associated virtualised services within the broader 5G scope. Once our analysis has been performed, we propose options for potential service implementation, to ensure specific security requests.

Keywords 5G · Edge cloud computing · Network functions virtualisation (NFV) · Network management · Security · Small cell (SC) · Network softwarisation · Telemetry and analytics · Virtual Network function (VNF)

1 Introduction

The 5th Generation of Mobile and Wireless Communications (also called as 5G) represents a complete revolution of mobile networks for accommodating the over-growing demands of users, services and applications [1]. Among other features, modern 5G networks represent a "shift" in networking paradigms, purely implicating to a transition from today's "network of entities" to a sort of "network of functions". Indeed, this "network of (virtual) functions" resulting in some cases in the decomposition of current monolithic network

✉ Pavlos I. Lazaridis
p.lazaridis@hud.ac.uk

[1] Hellenic Telecommunications Organization, Deutsche Telekom Group of Companies, 15122 Athens, Greece

[2] National Centre for Scientific Research "Demokritos", 15310 Athens, Greece

[3] University of Huddersfield, Huddersfield HD1 3DH, UK

[4] Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece

[5] International Technology University (ITU), San Francisco Bay Area, USA

entities can be a pillar for constituting the unit of networking for next generation systems [2].

The 5G ESSENCE [3] is a Leading Edge Project focused on the innovation of Edge Cloud computing and Small Cell as-a-Service (SCaaS) paradigms by exploiting the drivers and removing the backstops in the Small Cell (SC) market, expected to grow at a significant pace up to 2020 and beyond and to play an essential role in the 5G ecosystem. The progressive 5G ESSENCE context focuses upon structuring an efficient ecosystem, capable of creating new business models and revenue streams by generating a "neutral" host market and also by reducing both CAPEX and OPEX.

The 5G ESSENCE provides a highly flexible and scalable platform, capable of supporting new business models and revenue streams, by providing new opportunities for ownership, deployment, operation and amortisation. The project enhances the processing capabilities for data that have immediate value beyond locality; it also addresses the processing-intensive small cell management functions, such as Radio Resource Management (RRM)/Self Organising Network (SON) and, it culminates with real-life demonstrations. For all the above, the project suggests clear breakthroughs in the research fields of wireless access, network virtualisation and end-to-end (E2E) service delivery. The 5G ESSENCE project targets providing a concrete solution for modern business use cases directly relevant to vertical markets, as well as about introducing innovation in the fields of network softwarisation, virtualisation and cognitive network management, so that to jointly operate different radio nodes and radio access technologies, abstracting the available radio resources in an edge Data Center (DC). Within this Edge Cloud or Edge Data Center concept the corresponding, by the proposed architecture, centralised Software-Defined Radio Access Network Controller (cSD-RAN Controller) is in charge of managing the RAN infrastructure, the required resource abstraction framework and the virtualisation capabilities for introducing network slicing into existing legacy RAN deployments. This turns into providing a multi-connectivity framework to the end-user, seamlessly using the optimal RAT (Radio Access Technology) combination for fulfilling the Quality of Service (QoS) requirements of the service, operator- or terminal-type. Moreover, this entity also enables the support of Control Plane and User Plane Separation in legacy networks, by means of defining a centralised RRM that unifies the Control Plane functions for different RATs. The cSD-RAN Controller also implements a critical concept of the 5G ESSENCE solution architecture, laying the foundation of a cost-efficient and easy-to-deploy 5G system architecture, being as well completely aligned with the ongoing standardisation work developed in 3GPP, in ITU-R and in other standards bodies.

2 Basic Architectural Approach and Use Cases

The proposed and already developed 5G ESSENCE architecture [4] allows multiple network operators (i.e., tenants) to provide services to their users through a set of Cloud-Enabled Small Cells (CESCs) potentially deployed, owned and managed by a "third party" (i.e., the CESC provider) [5]. These are devices that include both the processing power platform and the SC unit. CESCs can be deployed at low and medium scale venues and support multiple network operators (multitenancy) and further, network services and applications at the edge of the network. In this way, operators can significantly extend the capacity of their own 5G RAN in areas where the deployment of their own infrastructure could be expensive and/or inefficient, as it would be the case of, *for example,* highly dense areas

where massive numbers of SCs would be needed to provide expected services [6]. More specifically, the 5G ESSENCE platform is equipped with a two-tier virtualised execution environment, materialised in the form of the Edge DC that allows also the provision of Multi-access Edge Computing (MEC) capabilities to the mobile operators for enhancing the user experience and the agility in the service delivery. One among the 5G ESSENCE major innovations is the efficient deployment of RAN and cloud infrastructure slices over a common physical infrastructure, so that to fulfil the requirements defined by the vertical use cases and the mobile broadband services, both assessed in parallel. In this scope, the 5G ESSENCE architectural approach also provides further innovative features about extending experiences upon (1) advanced and efficient virtualisation platforms, (2) dynamic telemetry and analytics based resource monitoring [7], and (3) development of the orchestration of distributed E2E services [8, 9]. In particular, 5G ESSENCE's common orchestration of radio, network and cloud resources is expected to contribute significantly to the fulfilment of the requirements defined by the entirety of the respective use cases. The 5G ESSENCE platform brings new mechanisms to share both radio and edge computing capabilities in localised/temporary network deployments between telco operators and market users. The challenge consists of allocating radio, network and cloud resources to the critical actors efficiently and by guaranteeing a certain QoS level. By definition, the project has prioritised high-quality services and demonstrates RAN/Edge DC features in three distinct Use Cases (UCs) listed as follows:

2.1 UC1: 5G Edge Network Acceleration for a Stadium

This scenario provides the logic for distributing the live video feeds received from the local production room to local spectators in a highly efficient manner. The municipal football stadium "Stavros Mavrothalasitis" (in the Municipality of Egaleo in the city of Athens, Greece) is covered with a cluster of multitenant evolved Multimedia Broadcast Multicast Services- (eMBMS) enabled CESCs and, together with the CESC Manager (CESCM) and the Main DC, they can be connected to the core network(s) of one or more telecom operators. The video content from cameras is sent for processing locally at the Edge DC. Then, the video streams are broadcasted locally by using the CESCs and so the involved spectators are able to dynamically select between different offered streams. The data traffic will not impact the backhaul connection since it is produced, processed and consumed locally.

2.2 UC2: Mission-Critical (MC) Communications for Public Safety (PS)

Use Case 2 focuses on two different public safety services, that is: (1) Mission Critical Push-To-Talk (MCPTT), and; (2) mission-critical messaging and localisation service. The MCPTT and Chat & Localisation services allow the secure communication such as, voice calls, chats and localisation tacking between pairs and/or groups of first responders. It should be specified that for different emergency situations each service is deployed in an isolated network slice and the necessary available resources will be allocated to ensure the functionality, connectivity and even the needed QoS. UC2 involves one or more PS communications providers that can use the resources offered by a deployed 5G ESSENCE platform for the delivery of communication services to PS organisations in a certain region or country. The 5G ESSENCE platform can be owned by a mobile (potentially virtual) network operator, or even by a venue owner, such as in UC1. In the MC use case, the infrastructure owner exploits the corresponding system capabilities by providing the required

network/cloud slicing capabilities with dedicated Service Level Agreements (SLAs) to different types of tenants, however by prioritising the PS communications providers.

2.3 UC3: Next Generation integrated In-Flight Entertainment and Connectivity (IFEC)

In UC3, the expected goal is to validate the multitenancy-enabled network solution for passenger connectivity and wireless broadband experience on-board. UC3 leverages integrated access points, being deployed on-board for hosting airborne applications (such as video player and files that can be made available for in-flight streaming) and caches (a version of the in-flight portal gateway with which passengers can connect to). In particular, UC3 enables multitenancy in the aircraft network hosting multiple operators and service providers by embracing the concept of "neutral host", thus supporting market competitiveness between "actors" aiming to offer advanced services on-board to a wide range of end-users' terminals of different types and capabilities. The multi-RAT CESCs can be implemented as a set of integrated SCs and Wi-Fi access points, deployed on-board. Afterwards, since IFEC has to consider the explosive growth of multi-screen content consumption, the related 5G ESSENCE CESCs will stream on demand multi-screen video content from on-board 5G Edge DC servers to the wireless devices thus demonstrating, *inter-alia*, multicast, transcoding and caching solutions.

All proposed 5G ESSENCE UCs are strongly relevant to current market needs and implicate for high dynamism and opportunities for growth and development in the related vertical industries. However, their intended deployment as well as their potential impact may be drastically affected by several security concerns. As security is also a critical factor for the ongoing and future 5G advances, the core of the actual work assesses related security threats, identified for each one of the selected UCs.

3 Security Threat Assessment

Security threat assessment is a necessary enabler towards building an effective security architecture in modern 5G networks. There are various documents from different standardisation bodies addressing the issues of threat and risk assessment and for mitigation in computer or telecommunication networks. Within the 5G ESSENCE framework, the methodology adopted for conducting the threat assessment is in line with the methodology introduced in the ISO/IEC 27005 standard [10]. The proposed risk assessment process has three main parts, namely risk identification, risk analysis and risk evaluation. This means that one has first to identify valuable assets, then consider the threats that could compromise those assets and finally perform a risk assessment in order to effectively estimate the damage that the realisation of any threat could pose to these assets. In any case, threats do play a key role in defining the risk assessment, especially when considering the components of risks. More specifically, ISO/IEC 27005 defines that risks emerge when "threats abuse vulnerabilities of assets to generate harm for the involved legal entity".

The asset identification process does follow the high level asset categories defined in ENISA Threat Landscape for SDN/5G [11], extended with assets that are specific to the 5G ESSENCE architecture (e.g., the case of the CESCM). On the other hand, the threat identification and categorisation process is based on available threat catalogues such as the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service,

Elevation of privilege) threat classification model [12] or the threat taxonomy provided by ENISA (as in [11]) or by ITU-T in Recommendation X.805 [13]. Our approach can finally "output" the level of risk as determined by the combination of threat likelihood and impact in the form of a relevant Risk Matrix. However, computing the risk likelihood and impact for 5G assets is quite challenging. Three main approaches can be used for this purpose: (1) qualitative analysis; (2) semi-quantitative analysis where values are assigned to the scales used in the qualitative assessment, based on existing literature and estimations performed for 4G systems as well as by evaluations provided by experts present in the various 5G-PPP projects [14], and; (3) quantitative analysis where numerical values are assigned to both impact and likelihood. As a result of the above, each approach is examined by the 5G ESSENCE and a clear risk assessment methodology can be proposed. It is under consideration for future work to support the detection of relevant risks, by using analytical and Machine Learning (ML) approaches. ML approaches are being adopted to improve detection and remediation of complex cyber-attacks. These methods typically require that an algorithm is trained by using normal traffic data to provide a baseline of normal system operation. Anomalies can then be detected, based on traffic patterns that are unusual or atypical for this system. Apache Spot [15] is an example of an open and scalable ML-based cybersecurity framework that may be used in the context of the 5G ESSENCE. Spot's goal is to "expedite threat detection, investigation and remediation via ML and consolidate all enterprise security data into a comprehensive IT telemetry hub based on open data models".

The overall analysis can also be supported by the 5G-SAT tool [16]. This is an open-source software hosted on GitHub under the MIT license, and can be used to facilitate the security analysis of 5G systems. It is based on the Electron [17] JavaScript framework and Cytoscape.js [18] library for front-end visualisation of the models. The components of the 5G ESSENCE system can be represented as graph nodes while their relationships can be represented as edges. At its core, the 5G-SAT tool uses an asset-centric modelling language, meaning that the concept of Threat can only target the concept of Asset. If a component of the system is not an Asset, it cannot be targeted by a Threat. Besides the visualisation of models, the application also offers additional functionalities (such as search capabilities, pattern identification, model validation and threat verification).

3.1 Security Analysis for Use Case 1

Within pilot UC1, the 5G ESSENCE project focuses on the demonstration of a combined 5G-based video production and video distribution scenario towards delivering benefits to both media producers and (mobile) operators involved. The production/distribution of locally generated content through the 5G ESSENCE platform, coupled with value-added services and rich user context, does enable secure, high-quality and resilient transmission, in real-time and with minimal latency.

Figure 1a illustrates the hardware architecture of the related stadium's 5G deployment. The 5G ESSENCE project uses its architecture to provide two different classifications of streams. The first stream is provided to spectators and/or to world viewers (i.e., people that watch the event from their homes or other social gatherings). The second stream is dynamically generated for each spectator in the stadium. Each stream uses a different Light DC as a host. The first stream (world feed) is hosted on the Local Production Light DC, while the second stream is hosted on the Spectator Control Light DC. The Main DC is responsible for the data processing of the data generated from the

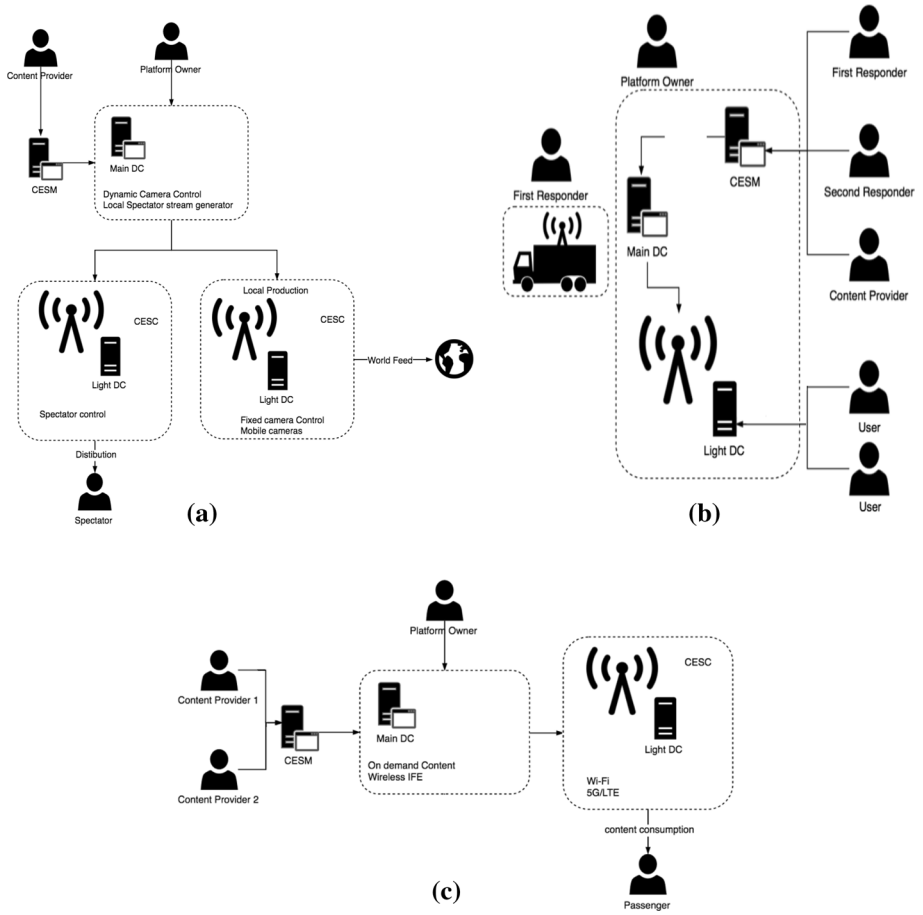


Fig. 1 Hardware architecture of: **a** stadium UC; **b** PS scenario, and; **c** in-flight scenario

Light DCs. Moreover, the Main DC provides additional functions. It acts as an interface between the spectator and the dynamic camera selection. The content provider manages the properties of the system using the interface of the CESM. The participating stadium spectators become able to dynamically select, among different offered broadcast streams. Among the supported services are: (1) Multicast Video Delivery in multi/single view; (2) User Equipment (UE) View Switching during the video delivery; (3) Video Delivery with handover, *and*; (4) Unicast *vs.* Multicast Video Delivery. Then, Table 1 provides a detailed list of already identified security requirements relevant to the above UC1. We define the security requirements of the system based on the security considerations of the system's stakeholders. For the context of the present analysis, the identified security requirements apply to the localised Light DC that is operated by the platform owner as well as external components of the system. In order to proactively assess the implicated threats, we propose suitable counter-measures or potential responding actions for each requirement, aiming to assure the proper fulfilling of a certain correlated objective (such as integrity, authentication, authorisation, availability and confidentiality). The proposed desctiption affects and improves the defined

Table 1 Stadium scenario security requirements

Security requirements	Objective	Description
The system should provide real-time telemetry and analytics data	Integrity	Telemetry data and analytics data are a general requirement of the system, which can be used to provide additional security. Analytics data can be leveraged to identify and fend off denial of Service (DoS) attacks. Telemetry data can improve the auditability of the system and demonstrate security to local regulators, which is another generic requirement of the system
Allow usage of the provided services only to authenticated "local" spectators	Authentication	The system must be able to determine that a spectator is eligible for "local" services. It should be able to determine the actual location of a spectator without the spectator being able to "spoof" his/her location
Prevent spectators from retransmitting the provided content	Authorisation	"Local" spectators can use their additional function to illegally stream local-only content to non-authorised spectators. The system must not only ensure that the provided services can only be used by authenticated and authorised spectators, but those spectators cannot tamper with the services. A very common attack vector in similar scenarios is location spoofing. Malicious actors can digitally alter the perceived location of their devices, in such a manner that stadium services will identify them as "local" users. The purpose of such an attack would be to leak exclusive content
Ensure availability of services to spectators accessing the world stream	Availability	Spectators accessing the world stream have specific availability requirements. In order to view the stream, a number of delivery actors need to communicate effectively
Ensure the availability of services to spectators accessing the local stream	Availability	The delivery of local stream is handled by the platform owner. As such, there is no need for communication with other delivery actors
Ensure the required network capacity during operation of the services to the spectators	Availability	Depending of the size of the event and the number of spectators, the required network capacity of the system will be different. The system must have mechanisms in place to either delegate traffic to other CESCMs or dynamically reduce the network requirements of the services in order to accommodate the demand. End-users are able to choose what content will be streamed to their device. This "freedom of choice" can strain the available resources of the system, either intentionally or unintentionally, in a way that will cause a denial of service attack. The DoS may affect the local delivery of content or may affect the global delivery of content

Table 1 (continued)

Security requirements	Objective	Description
Spectators should be able to access their personal data that are used by the telemetry and analytics services	Confidentiality	General Data Protection Regulation (GDPR) enforces transparency of personal information used in digital services. Each spectator must be able to access and control what type of personal information is being used and stored in the system
Ensure the secure handling and storage of spectators' personal information	Confidentiality	Spectators' personal information must be securely handled during the different stages of data (i.e., data at rest, data in motion, data in use)

architectural approach so that to serve the intended transition towards a practical and feasible 5G implementation. The security requirements are listed in Table 1.

3.2 Security Analysis for Use Case 2

Within UC2, the 5G ESSENCE framework involves one or more PS communications providers that will use the resources offered by a deployed 5G ESSENCE platform. Use Case 2 focuses upon two different public safety services, that is: (1) Mission Critical Push-To-Talk (MCPTT), and; (2) mission-critical messaging and localisation service. The MCPTT and Chat & Localisation services allow the secure communication (in the form of voice calls, chats and localisation tacking) between pairs and/or groups of first responders. For diverse emergency situations there is prediction for service deployment in an isolated network slice, in parallel with the proper allocation of all available resources so that to guarantee functionality, connectivity and the prescribed QoS. In case of emergency, the Cloud Edge Small Cell (CESC) of the 5G ESSENCE platform will "add" new resources taking into consideration the request, close-to-zero delay and maintaining the connection even if the backhaul is damaged. Moreover, in the respective trials the 5G ESSENCE SD-RAN controller has the essential role of enforcing the priority access of first-responders by extending the slices to the radio part, thus creating the end-to-end slices that isolate those responders from other's parties' communications. To realise these aims, Fig. 1b) shows the high-level architecture of public safety's 5G deployment. The MC application for PS scenario has a number of stakeholders with their own responsibilities and goals. The different stages of the MC application for public safety require security requirements that are adaptive. The security requirements must take into account the fact that certain during some of the system's stages new hardware and software components will be introduced in a forceful manner. When new components are introduced, security mechanisms must be performed in order to ensure the continuous secure posture of the system. The security analysis revealed the requirements, as listed in Table 2, below.

3.3 Security Analysis for Use Case 3

Use Case 3 revolves around the next generation of IFEC system on-board aircrafts, setting up the ambitious goal to include the sector of civil aviation in the 5G ecosystem by means of the 5G ESSENCE system architecture. The 5G ESSENCE IFEC demo tests and validates the multi-tenancy enabled network solution for passenger connectivity and wireless broadband experience. The multi-RAT CESCs can be implemented as a set of integrated access points, deployed on-board. Afterwards, the 5G ESSENCE CESCs will stream on demand multi-screen video content (both from on-board 5G Edge DC servers and via satellite/air-to-ground links) to the wireless devices. In this case, the 5G ESSENCE CESCs will rely on broadcast links in order to optimise the bandwidth usage. In fact, Fig. 1c depicts the high-level architecture of the airplane's 5G infrastructure deployment. The Main DC is responsible for providing remote connectivity to the system. As mentioned above, the remote connectivity is achieved from a combination of air-to-ground communications and satellite networking. The Main DC is used as the system's storage for on demand content. The Light DC acts as an interface for content consumption by the passengers and as a gateway to Wi-Fi or 5G network connectivity. The Content Providers can use the interface of the CESCM to manage their content and other aspects of their applications. System's security requirements become upon related concerns coming by the system stakeholders.

Table 2 Mission critical scenario security requirements

Security requirements	Objective	Description
System should be able to allocate critical resources to its PS tenants, so that to ensure availability in times of distress	Availability	During times of distress, the communication services of PS tenants are considered as a critical resource of the system. As such, the respective system must ensure their constant availability
Non-operational infrastructure should not impact the availability of the system's services	Availability	Damaged infrastructure results in a number of security issues. Such an issue is about "the way how to provide the infrastructure the necessary hardware and software components so that to enable the continuation of the service". Another issue is about how to enable the secure handover of services and data from the original infrastructure to the replacement. Other concern is about the way how to enable the secure handover of data from the replacement infrastructure to the permanent one, once it is repaired. While the services of the system change hardware and software domains, it is crucial to ensure their availability to their users, especially for PS organisations
Non-operational infrastructure should not impact the confidentiality of the system's services and data	Confidentiality	Depending on the nature of the damages in the infrastructure, both the system's services and data are subject to threats. Such threats will be made by Information Disclosure type of attacks. The system's security constraints will ensure confidentiality
Preserve data availability between handover of services	Availability	During services' handover data sets are most vulnerable, since they are moved from one secure environment to another. An issue during handover is that all sorts of data become unavailable while the initial host service turns "offline", before the second host has time to become operational
Preserve data confidentiality between handover of services	Confidentiality	During services' handover, a number of security mechanisms take place. Those mechanisms ensure that end-users' data will retain their confidentiality
Preserve data integrity between handover of services	Integrity	In order to retain integrity of data during handover, a periodic and phased methodology approach should be followed. This improves data security by enabling security mechanisms to be performed in phases

Table 2 (continued)

Security requirements	Objective	Description
System must ensure the integrity of the end-users' information	Integrity	User's data may be moved to other physical hardware locations inside the Light DC or to a different Light DC. The data will change state (in transit, at rest, in use) during the system's life cycle. Other factors that change the state of data are the changes in the system architecture, whether that change is voluntary (backup, services upgrade) or involuntary (damaged infrastructure). While the hardware and software components of the system change during its life cycle, it is crucial to ensure the integrity of the provided services and data. For example, if part of the infrastructure is temporarily replaced, then the handoff of data must be made while retaining data integrity. The latter refers to retaining the data original format while ensuring security and privacy

Traditional airplanes did not allow network connectivity for the duration of the flight. The main security concern, in this case, is to provide network connectivity to passengers without compromising the integrity of the airplane's internal controls. Another security issue is the exposure of connected devices to external malicious networks. An example of such an attack is the deployment of in-flight honey-pots by malicious passengers. The honey-pots can route traffic to legitimate networks while stealing data from other users. Similar attacks will aim to escape the sandboxed environment provided by the CESC. For this case, the essential security requirements are listed in Table 3.

4 Overview of Results and Discussion

Based on the scope of the original 5G ESSENCE effort we have analysed, *on a per separate use case basis*, related requirements imposed by security concerns, so that to proceed to further development of the corresponding platform for the intended offering of services. For each use case, we have proposed suitable measures to overpass possible constraints and for supporting reliable implementation. However, security in 5G is a multi-faceted issue. As services can be created and torn down in a matter of minutes, there lies the challenge of monitoring risks across the deployed 5G infrastructure as well as securing the tenant workloads. Three tiers of protection are herein considered: (1) The deployment of cybersecurity functionalities on the network level, as Virtual Network Functions (VNF) based services; (2) the deployment of advanced ML learning algorithms, and; (3) the hardening and attestation of existing infrastructure.

Cybersecurity functionalities can be deployed as-a-Service to monitor the traffic for signs of malicious attacks. This approach allows the administrator to perform runtime changes to cybersecurity VNFs (i.e., to apply rules to a Firewall or to an Intrusion Detection System (IDS)). The EM (Elemental Management) component of the ETSI NFV reference architecture can be used to provide runtime configuration of running VNF-based services [19]. Traditional IDSs can then be deployed in order to perform signature-based detection, based on well-known malicious traffic patterns that signify potential attacks. The main drawback of this method is that attack patterns need to be known in advance, and signatures must be preconfigured. Hence, typical systems fail to detect a zero-day attack or an attack with unknown signature. Moreover, it is essential to realise a careful selection of cybersecurity functionalities and in some cases the VNF needs to be placed on the path of traffic (i.e., a firewall). In this case, practical work [20] has shown that the VNF needs to ensure high performance and high availability, otherwise it will negatively affect E2E latency.

Furthermore, as ML becomes a mainstream technology that is present in many consumer products, the cybersecurity industry has been quick to adopt it, to improve on the existing defense capabilities. The 5G ESSENCE project considers the case of Apache Spot [15], a machine learning-based platform for anomaly detection that utilises Latent Dirichlet Allocation [21] to detect a typical traffic pattern. Latent Dirichlet Allocation differs from other common ML classifiers in that it is a Natural Language Processing (NLP) algorithm. The NLP is easy to apply on the variety of different network traffic logs and improves the overall threat intelligence capabilities by including more sources of structured, human-readable, textual data. The ML system can then be trained on typical traffic and identify zero-day or other cyberattacks as anomalous patterns of traffic are observed, without prior knowledge of the attack signature. Other systems offer similar capabilities, such as Sqrrl [22] and Apache Metron [23]. Apache Spot sets itself apart not only by its machine

Table 3 In-flight scenario security requirements

Security requirements	Objective	Description
Sandbox the network access and other functions of the passengers, so that they are not able to tamper with the airplane's internal functions	Integrity	Sandboxing is a security mechanism for separating processes, without risking harm or the host machine or operating system. A sandboxed process cannot affect another sandboxed process. In order to protect the internal functions of the airplane from tampering, it is required to isolated passenger spawned processed
Prevent passengers from eliciting the airplane's real-time location	Integrity	Here the main reason is ensuring safety of air traffic. If a malicious actor is allowed any network connectivity, then he/she will be able to use the detected signals to triangulate airplane's real position, speed or height
Prevent external exposure of the airplane's CESC to other networks	Integrity and Confi-dentiali-ty	The airplane's CESC provides their services by using a combination of satellites and air-to-ground links. A malicious actor can use the same links to expose the airplane's services to external networks. In essence, making the airplane an external facing network node. Depending on the implementation of the in-flight system, a malicious actor may be able to scan and enumerate the airplane's services. If the services can be detected, there is a possibility that malicious actors can tamper with them
Identity management	Confi-dentiali-ty	Both hardware and software infrastructure "run" in a multi-vendor environment that moves from Wi-Fi to LTE (Long Term Evolution) stacks. The system must ensure strict identity management with the aim of preventing authorised access to network resources
Prevent users from copying or distributing licensed content	Authorisation	Films and other content are streamed locally to the user. As such, the user does not have a license to keep the material, nor should the user be technically able to record a copy themselves
Retain end-user data confidentiality when 5G network does not use LTE	Confidentiality	While 5G infrastructure uses LTE, the airplane platform owner uses Wi-Fi to connect end-users with services. The usage of different protocol stacks requires additional mechanism to ensure end-user confidentiality
Physically isolate the network used by the airplane functions and the network used by the passengers	Integrity	Passengers should never be able to access the network used by the airplane's internal systems

learning capabilities, but also from its Open Data Model (ODM). ODM brings together all security-related data (event, user, network, endpoint, etc.) into a singular view that can be used to detect threats more effectively than before in the past. This consolidated view can be leveraged to create new analytic models that were not previously possible and to provide needed context at the event level to effectively determine whether -or not- there is a threat. Furthermore, it also provides the ability to share and reuse threat detection models, analytics and more. This improves interoperability among anomaly detection platforms and fosters the creation of an open data community. Based on the above, we shall expect effective design of the related services and their operational inclusion in the respective platform, for the promotion of 5G innovative features within the 5G ESSENCE platform.

Acknowledgements This work has been performed in the scope of the *5G ESSENCE* Project and has been supported by the European Commission (*under GA No.761592*).

Reference

1. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J.C. (2014). What Will 5G Be? IEEE JSAC, Special issue on 5G Wireless Communications Systems *32*(6), 1065–1082.
2. Chochliouros, I. P., Spiliopoulou, A. S., Kostopoulos, A., Belesioti, M., Spiliopoulou, A.S., & Dardamanis, A. (2016). Challenges for Defining Opportunities for Growth in the 5G Era: The SESAME Conceptual Model. In *Proceedings of the EuCNC-2016*. (pp. 1–5) IEEE.
3. 5G ESSENCE ("Embedded Network Services for 5G Experiences") 5G-PPP Project, Grant Agreement (GA) No.761592. http://www.5g-essence-h2020.eu.
4. Chochliouros, I. P., Kostopoulos, A., Spiliopoulou A. S., Kourtis A., Giannoulakis I., Kourtis M-A., Sfakianakis E., Belesioti M., Kafetzakis E., & Iosifidis M. (2018). Small Cells, NFV and cloud computing as enablers for offering innovative 5G services: From SESAME to the 5G ESSENCE architectural framework. In *Proceedings of the EuCNC-2018*, (pp. 570–574) IEEE.
5. Chochliouros, I. P., Kostopoulos, A., Giannoulakis, I., Spiliopoulou, A.S., Belesioti, M., Sfakianakis, E., Kourtis, A., & Kafetzakis, E. (2017) Using small cells for enhancing 5G network facilities. In *Proceedings of IEEE Conference on Network Function Virtualisation and Software-Defined Networks (NFV-SDN'17)*, (pp. 264–269) IEEE.
6. Chochliouros, I. P., Giannoulakis, I., Spiliopoulou, A. S., Belesioti, M., Kostopoulos, A., Sfakianakis, E., Kourtis, A., Kafetzakis, E. & Agapiou, S. (2017) A novel architectural concept for enhanced 5G network facilities. In *MATEC Web of Conferences 125*, 1–7.
7. Chochliouros, I. P., Spiliopoulou, A. S., Kostopoulos, A., Agapiou, G., Belesioti, M., Sfakianakis, E., Kourtis, M. A., Iosifidis, M., Agapiou, M., & Lazaridis, P. (2019) Inclusion of telemetry and data analytics in the context of the 5G ESSENCE architectural approach. In *Proceedings of AIAI-2019, IFIP AICT 560*, (pp.46–59). Springer.
8. Chochliouros, I.P., et *al.*: Enhancing Network Management via NFV, MEC, Cloud Computing and Cognitive Features: The "5G ESSENCE" Modern Architectural Approach. In: Proceedings of AIAI-2018, IFIP AICT 520, pp.1–12. Springer AG (2018)
9. Kostopoulos, A., Chochliouros, I. P., Giannoulakis, I., Kourtis A., & Kafetzakis, E. (2018) Small cells as-a-service in 5G networks. In *Proceedings of the IEEE BMSB Conference*, (pp.1–4) IEEE.
10. International Organization for Standardization (ISO): ISO-IEC 27005:2018. (2018). Information Technology: Security techniques—Information security risk management. ISO, http://www.iso27001security.com/html/27005.

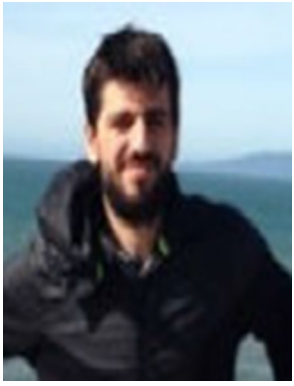
11. The European Union Agency for Cybersecurity (ENISA). (2016) Threat Landscape and Good Practice Guide for Software Defined Networks/5G. https://www.enisa.europa.eu/publications/sdn-threat-landscape.
12. Shostack, A. (2009) The threats to our products. Microsoft . https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/.
13. International Telecommunication Union: Telecommunication Standardization Sector (ITU-T). (2003). ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications. ITU-T.
14. The 5G Infrastructure Public Private Partnership (5G-PPP). https://5g-ppp.eu/.
15. Apache Spot. http://spot.incubator.apache.org/.
16. 5G-SAT. https://github.com/CapriTechLimited/5G-SAT.
17. Franz, M., Lopes, C. T., Huck, G., Dong, Y., Sumer, O., & Bader, G. D. (2016). Cytoscape. js: A graph theory library for visualisation and analysis. *Bioinformatics, 32*(2), 309–311
18. SHIELD ("Securing against intruders and other threats through a NFV-enabled environment") H2020 project, Grant Agreement No.727301. https://www.shield-h2020.eu/.
19. European Telecommunications Standards Institute (ETSI): ETSI GS NFV-MAN 001 V1.1.1 (2014-12). (2014). Network Functions Virtualisation; Management and Orchestration. ETSI.
20. Mathas, C. M., Segou, O. E., Xylouris, G., Christinakis, D., Kourtis, M. -A., Vassilakis, C. & Kourtis, A. (2018) Evaluation of Apache spot's machine learning capabilities in an SDN/NFV enabled environment. In *Proceedings of ARES 2018*, Article No.52, (pp. 1–10) ACM.
21. Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent Diriclet allocation. *Journal of Machine Learning Research, 3*(4–5), 993–1022
22. Sqrrl Data, Inc. https://sqrrl.com/.
23. Apache Metron: Real-time big data security. http://metron.apache.org/.

Ioannis P. Chochliouros graduated from the Department of Electrical Engineering of the Polytechnic School of Aristotle University of Thessaloniki, Greece, and he also holds an M.Sc. (D.E.A.) and a Ph.D. (Doctorat) from the University Pierre et Marie Curie (Paris VI), France. His practical experience as an engineer has been mainly in Telecommunications, as well as in various constructive projects in Greece and the wider Balkan area. Since 1997 he has worked at the Competition Department and as an engineer-consultant of the Chief Technical Officer of the Hellenic Telecommunications Organisation S.A. (OTE). He has been very strongly involved in major OTE's national and international business activities, as a specialist-consultant for technical and regulatory affairs, especially for the evaluation and the adoption of innovative e-Infrastructures and e-Services in Greece and abroad. He has also served as the Head of Technical Regulations Dept. of OTE's Division for Standardisation and Technical Regulations, representing OTE in international standardisation for a and he has been involved in an enormous variety of issues regarding European and international standardisation, with emphasis on modern technologies. In addition, he has also worked as an independent consultant in the scope of several European and/or international research and business studies. Since 2005, he is the Head of OTE's Fixed Network R&D Programs Section and has been involved in different national, European and international R&D projects and market-oriented activities, many of which have received international awards. During his professional career, he has participated either as coordinator or as a scientist-researcher in more than 62 European and national research programs, some of which have received distinctive awards. He is author/co-author of three international books and he has published more than 250 distinct scientific or business papers/reports in the international literature (book chapters and articles in magazines, journals and conferences proceedings), especially for technical, business and regulatory options arising from innovative e-Infrastructures and e-Services. He is an expert in project management activities with an extensive experience in EU-funded projects where he has very successfully exercised coordinator's duties (e.g., 5G-PPP 5G ESSENCE, 5G-PPP SESAME, Privacy-Flag, LiveCity, D-SPACE). He is also an

active participant of various international and national associations, both of scientific and business nature. Dr. Chochliouros has also performed an extended educational activity in Greece and in France, in cooperation with Universities and other high-level Institutes, covering a broad variety of issues in the scope of modern e-communications. Recently he has received the distinctive award of being a member of the IPv6 Hall of Fame.

Anastasia S. Spiliopoulou is a Lawyer, Member of the Athens Bar Association. She also holds a Post-Graduate Diploma (LLM) from the Law School of National and Kapodistrian University of Athens, Greece. She has a long professional experience in telecommunications and IT-related issues and she has been involved in many affairs about regulatory issues and other matters affecting the deployment and the provision of both modern electronic communications networks and services. She is an OTE's (Hellenic Telecommunications Organization S.A.) expert for a great variety of regulatory issues affecting both European and national policies. She is author/coauthor of more than 100 papers in the international literature and has participated to numerous conferences, in several of which as invited speaker.

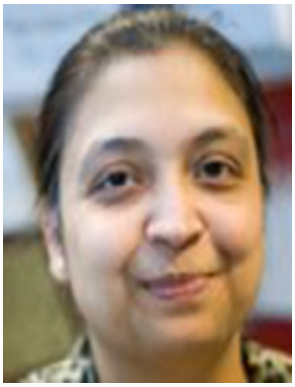
Dr. Alexandros Kostopoulos holds two Master Degrees in Telecommunications (University of Athens), and in Computer Science (University of Piraeus). He received his Ph.D. from Athens University of Economics and Business (AUEB) in 2013. He was a visiting lecturer in AUEB, as well as a postdoctoral researcher at the Institute of Computer Science, in FORTH. He is currently working at the Research and Development Division of Hellenic Telecommunications Organization (O.T.E.) on European and National research projects. He has published several papers in scientific journals and conferences. He has significant experience in network architecture design, and he will contribute to the requirements' analysis, as well as to test-bed experiments and overall evaluation.



Dr. Michail-Alexandros Kourtis received his Ph.D. from UPV/EHU in 2018 and his Diploma and Master's Degree in Computer Science from the Athens University of Economics and Business, in 2011 and 2013 respectively. Since 2015, he has worked on applications of Network Function Virtualisation for cybersecurity, as well as on the definition of privacy and security risk metrics on virtualized infrastructures. His research interests include QoE, QoS, Video Processing, Video Quality Assessment, Image Processing, LTE, 5G, Network Function Virtualization, and Software Defined Networks. He is a contributor at the OPNFV open source project Yardstick, and an active member, participant and contributor at the IETF NFVRG, also a TPC member and reviewer at various conferences and journals.

Dr. Pavlos I. Lazaridis is a Professor in Electronic and Electrical Engineering at the University of Huddersfield, UK. He received the Electrical Engineering degree from the Aristotle University of Thessaloniki, Greece, in 1990, the MSc. degree in Electronics from Université Pierre et Marie Curie, Paris 6, France, in 1992, and the Ph.D. degree in Electronics and telecommunications from Ecole Nationale Supérieure des Télécommunications (ENST) and Paris 6, Paris, in 1996. From 1991 to 1996, he was involved with research on semiconductor lasers, wave propagation, and nonlinear phenomena in optical fibers for the Centre National d'Etudes des Télécommunications (CNET) and teaching at the ENST. In 1997, he became the Head of the Antennas and Propagation Laboratory, TDF-C2R Metz (Télédiffusion de France/France Télécom Research Center), where he was involved with research on antennas and radio coverage for cellular mobile systems (GSM), Digital Audio Broadcasting (DAB), and Digital Video Broadcasting-Terrestrial (DVB-T). From 1998 to 2002, he was with the European Patent Office, Rijswijk, The Netherlands, as a Senior Examiner in the field of Electronics and Telecommunications. From 2002 to 2014, he was involved with teaching and research at the Alexander Technological Educational Institute of Thessaloniki, Greece, and Brunel University, West London. He is leading the EU Horizon 2020 projects ITN MOTOR5G and RISE-RECOMBINE for the University of Huddersfield. He is a member of the IET and a senior member of the IEEE and URSI.

Dr. Zaharias D. Zaharis received the B.Sc. degree in physics, the M.Sc. degree in electronics, the Ph.D. degree, and the Diploma degree in electrical and computer engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1987, 1994, 2000, and 2011, respectively. From 2002 to 2013, he was with the administration of the telecommunications network, Aristotle University of Thessaloniki, and since 2013 he has been with the Department of Electrical and Computer Engineering of the same university. His current research interests include design and optimization of antennas and microwave circuits, signal processing on smart antennas, development of evolutionary optimization algorithms, and neural networks. Dr. Zaharis is a member of the Technical Chamber of Greece and a senior member of IEEE.



Dr. Neeli R. Prasad is a security and wireless technology strategist, who through her career has been driving business and technology innovation, from incubation to prototyping to validation. She has focus and the abilities to transform organizations and networking technologies to address changes in markets. She has made her way up the waves of secure communication technology by contributing to the most groundbreaking and commercial inventions. She has general management, leadership, and technology skills, having worked for service providers and technology companies in various key leadership roles. She is leading a global team of 20 + researchers across multiple technical areas and projects in Japan, India, throughout Europe and USA. She has been involved in projects and plays a key role from concept to implementation to standardization. Her strong commitment to operational excellence, innovative approach to business and technological problems, and aptitude for partnering cross-functionally across the industry have reshaped and elevated her role as project coordinator making her the preferred partner in multinational and European Commission project consortium. Her notable accomplishments include enhancing the technology of multinationals including CISCO, HUAWEI, NIKSUN, Nokia-Siemens and NICT, defining the reference framework for Future Internet Assembly and being one of the early key contributors to Internet of Things. She is also expert member of governmental working groups and cross-continental forums. Previously, she has served as

chief system/network architect on large-scale projects from both the network operator and vendor looking across the entire product and solution portfolio covering security, wireless, mobility, IoT, Machine-to-Machine, eHealth, smart cities and cloud technologies. She was one of the key contributors to the commercialization of WLAN and published two books. She also has 2 books on IoT and convergence of IoT and Automotive.