Rev. Roum. Sci. Techn.– Électrotechn. et Énerg.
Vol. **68**, *2*, pp. 206–211, Bucarest, 2023

MULTI-ACCESS EDGE COMPUTING ANALYSIS OF RISKS AND SECURITY MEASURES

ALINA FLORINA GLAVAN[1], DANIEL GHEORGHICA[2], VICTOR CROITORU[3]

Keywords: Multi-access edge computing (MEC); 5G; ISO; Security.

5G efficiently uses technologies like network slicing (NS), network function virtualization (NFV), software-defined network (SDN), and multi-access edge computing (MEC). At the same time, embracing these technologies and creating new services opens the network to a new set of security challenges. This paper presents a threat analysis of MEC features. The paper's novelty resides in viewing MEC as common ground for the telco and IT sectors. This paper studies the measures according to ISO/IEC 27001:2022 controls. ISO/IEC 27001 is the most popular standard for information security management systems, with a new version published in 2022.

1. INTRODUCTION

Multi-access edge computing (MEC) is presented in paper [1] as an ecosystem that provides benefits for both provider and customer: it alleviates the core network from jobs that have a local impact only by executing the jobs at the very beginning of the chain of demand and enhances user experience by ensuring lower latency.

The needs of digital and agile organizations can be met by implementing virtual network functions (VNFs) and network slicing (NS). NS permits the creation of multiple isolated logical networks on a single physical network. The purpose of VNF technology is to separate network functions from underlying hardware [2].

Network function virtualization (NFV) architecture eases the deployment of new services, facilitates service configuration, and ensures faster time to market [3]. Virtualized network functions can be parts of a service chain. Example functions include verification, authentication, traffic analysis, and allocation functions performed by the mobile network nodes [3].

Cloud computing and software-defined network (SDN) both aim to provide virtualized functionality. Cloud computing allows the creation of virtual machines (VM), while SDN allows telecommunications operators to create virtual networks. A 5G use case is presented in Fig. 1: a critical Internet of things (IoT) slice: industrial Internet of things (IIoT) application. More examples of network slicing in IoT are presented in the paper [4]. Figure 1 is an example of collaboration between the above mentioned technologies.

These technologies increasingly affect the implementation of new services in 5G system(5GS). Slices of networks offer valuable security benefits: logical separation, distinct security perimeters, virtual network functions isolation from other services. Edge computing also has an important role in ensuring user data privacy. As 5GS complexity grows, security and privacy aspects must be studied [5].

New 5G services direct attention toward the evolution of non-IP networking. As the gap between the telecommunication industry and information technology is narrowing, 5G is expected to adopt shared standards for cybersecurity[6]. 5G system complexity is starting to resemble an information technology (IT) system rather than a mobile network as we know it. And yet, the security provided by traditional IT tools is not nearly enough for the telecom industry[7].

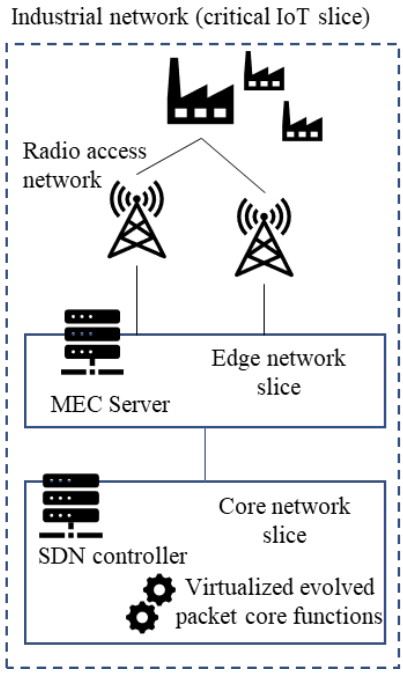

Fig. 1 – Network slicing for the industrial Internet of things (IIoT).

This paper aims to categorize MEC specifics from a cybersecurity perspective. The threat landscape will be narrowed down to MEC, as this is the most exposed part of the network and represents the ever-evolving attack surface.

The main contributions of the authors are:

- reviewing the standardization work applicable to MEC and its role in 5G;
- suggesting a threat discovery methodology starting from MEC features and caveats;
- mapping of MEC threats to ISMS (Information Security Management Systems) controls from ISO/IEC 27001:2022 and ISO/IEC 27002:2022.

The remainder of this paper is organized as follows: the paper starts with a short introduction to MEC and a review of recent work in standardization organizations such as ETSI (European Telecommunications Standards Institute), 3GPP (3rd Generation Partnership Project), ENISA (European Union Agency for Cybersecurity), ISO (International Organization for Standardization). An overview of MEC standardization work is presented in chapter three. Chapter four presents an analysis of MEC characteristics and security concerns. The link between IT and MEC cybersecurity is presented from the IT-specific standard ISO/IEC

[1] Politehnica University of Bucharest, Bucharest, Romania. E-mail: alinafglavan@gmail.com
[2] K-Businesscom SRL, Bucharest, Romania. E-mail: daniel.gheorghica@k-business.com
[3] Politehnica University of Bucharest, Bucharest, Romania. E-mail: croitoru@adcomm.pub.ro

27001:2022 perspective and the ISO/IEC 27002:2022 guide. As 5GS leverages MEC solutions, a review of other work in the security of MEC and related key technologies is presented in chapter five. Subsequently, a discussion about the research gap and future work is provided in chapter six.

2. EDGE COMPUTING IMPLEMENTATION

Edge computing is a subject advanced mostly by two standardization organizations: ETSI ISG and 3GPP [8]. Each of these organizations has its proposal on edge computing architecture for mobile network operators – both working groups aim to create an IT service environment for third-party applications [9]. An alignment between the two proposals was published by ETSI in a paper [8] in 2020.

The acronym MEC stands for multi-access edge computing (current ETSI definition) and mobile edge computing (ETSI definition until 2017). One characteristic of MEC, as envisioned by ETSI, is that it offers the cloud as an IT service environment so that various applications can be deployed at the edge, creating an opportunity for application developers and content providers. The "multi-access" term is a reminder that this technology is access-agnostic and deployments are independent of the underlying access network [10].

Edge computing is considered a core technology in implementing 5GS as it sustains most 5GS high-performance use cases. The verticals supported by this technology range from transport to IIoT. MEC has the characteristic of bringing computing power closer to the end user, and it also takes part in managing the application lifecycle in 5GS. It interacts with the 5G policy component and helps alleviate the burden on the 5G core network by serving user requests locally. It is also important in sustaining mobility-related use cases [10].

Paper [11] presents the idea of cognitive edge computing: a telecommunication edge that implements modern techniques to aid the core network in resource control. The authors design Fig. 2 and present the relation between edge computing and other components in telecommunications: 5G core and cloud computing. Figure 2 presents the tasks performed by edge and cloud computing components in 5G, in line with the ideas introduced in the current paper. Regarding the cloud computing component, the possibility of performing policy evaluation and assisting the core with network-wide goal assessment should be considered due to higher computing and storage capabilities.

3. SECURITY STANDARDS FOR MEC

Paper [6] presents a summary of the security aspects of 5G. An important recommendation in the document is that "5G should adopt common standards for cybersecurity" [6]. 5G solutions that provide low latency or high bandwidth likely include a MEC component[4], meaning MEC should comply with cybersecurity standards.

In the European Union, the new NIS2 (Network and Information Security) Directive [12] was published and aimed to protect critical infrastructure. Edge cloud has to comply with the new directive as telecommunication services and other critical services adopt an edge-based solution. ENISA has submitted for review paper [13] – a cybersecurity certification scheme for cloud services, also applicable to edge computing.

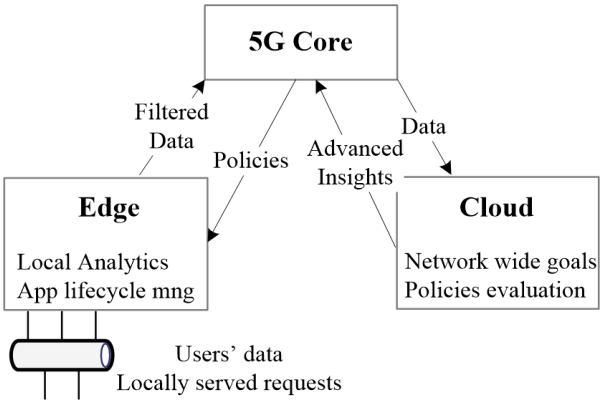

Fig. 2 – Edge and cloud computing in 5G role summary

Paper [9] is based on 5G standardization documents and consolidates cyber threats considering 5G infrastructure specifications. The report starts by presenting a generic architecture of 5G and performs a vulnerability assessment of all the important technologies: NS, SDN, NFV, MEC, and radio access network (RAN). Although the report was published at 3GPP Release 16 (December 2020), being based on standardization documents makes it significant. The paper [9] results are used in ETSI White Paper on MEC security [14].

ISO/IEC 27001 is the most popular standard for information security management systems (ISMS) [15]. The latest version was published in 2022. Although widely implemented in the IT industry, ISO/IEC controls can be used as a guideline for information security in other sectors. One novelty of this version is the classification of controls in four categories only: technological, organizational, people, and physical.

ISO/IEC 27002 was also updated in 2022 and serves as a guideline for standard implementation. Telecom-relevant guidelines are published in ISO/IEC 27011:2016, based on ISO/IEC 27002:2013. ISO/IEC 27011 is in revision to be aligned with ISO 27002:2022. This is a joint effort with ITU-T, and it is to be published in Q3 2023 [16].

One of the novelties in the ISO/IEC 27002:2022 guideline is the introduction of control attributes. The impact of control on a given risk is evaluated using the "control type" attribute. The three values of the attribute are preventive, detective, and corrective.

The control type values define the control concerning the information security incident time:

- preventive refers to a control that acts before an incident occurs;
- detective refers to a control that acts when an incident occurs;
- corrective refers to a control that acts after an incident occurs.

Another important IT standard cited as relevant in [14] is for security assurance level: ISO/IEC 15408 or Common Criteria for Information Technology Security Evaluation. Specifically, the standard presents seven Evaluation Assurance Levels (EAL). If the service includes a MEC component, then the service EAL should be met by the MEC components [14].

4. MEC THREAT LANDSCAPE

In the following, we present our analysis of the MEC threat landscape.

Table 1 presents the characteristics that define MEC and

the security concerns associated. Table 1 is designed by the authors and presents a different take on the information published by ENISA [9] and ETSI [14] by starting a drill down from MEC characteristics to security measures.

Table 1 presents five MEC features and their subsequent vulnerabilities and threats. The features identified are cloud-native, distributed nature, complex multi-party environment, edge of the network locations, and application programming interfaces (APIs). The analysis starts from the benefits brought by each feature and the corresponding vulnerabilities to the author's best knowledge. The list of threats was obtained by studying the identified vulnerabilities. Then, several measures were identified and suggested in Table 1 for each of the five MEC features.

This paper classifies MEC-specific measures from Table 1 by "control type" values introduced in the ISO/IEC 27002:2022 code of practice. This guide was chosen because of its influence in defining telecom standard ITU-T X.1051[17]. Nevertheless, ETSI's definition of MEC as an "IT service environment" in [10] justifies the study of IT security standards in MEC security.

One of the most important features identified for MEC is the cloud-native architecture [9]: build, deploy, and manage operator-specific and third-party applications in an edge computing environment. Adopting cloud-native architecture brings the benefits of microservices and containers: easy, independent deployment of micro-services, efficient software upgrades and patches, scalability, and resiliency. Although the micro-services or containers are managed independently, communication in micro-service chaining should be authorized. Security risks may also arise from the shared infrastructure and platform [9,14] – software patching should be integrated into the pipeline, and platforms must be updated as required.

Table 1

MEC threat landscape and ISO control attributes

Feature	Vulnerabilities	Threats	Measures	ISO control type
Cloud native	Cross-contamination, improper isolation of resources; Application and shared host platform vulnerabilities; Central orchestration; Improper controlling and accounting for deployments;	Abuse of privilege, unauthorized access, eavesdropping, interception. modification of parameters, spoofing identity, DoS; Abuse of insufficient identity, credential, access and key management; Failures, malfunctions; Configuration drift; Exploitation of vulnerabilities from third-party application and shared host platform; Abuse or nefarious use of services	1. Authorized access, identity, credential and key management; 2. Secure transport protocols; 3. Data encryption; 4. Sensitivity-based instance segregation; 5. Enforce security regulations for cloud services; 6. Application testing; 7. App resource usage assessment; 8. Collect and process security logs;	#preventive
			9. System patching;	#preventive #corrective
			10. Threat detection; 11. Intelligence gathering; 12. Change management;	#preventive #detective
Distributed nature	No system-wide security assurances; Improper regulatory mechanisms implementation; Lack of local DDoS protection	DDoS, data tampering, identity spoofing; Inability to respond to lawful interception; Cyberattacks	1. Control and user plane separation (CUPS) architecture (lawful interception); 2. External location for log collection; 3. Access control on logs; 4. Propper logging of security events;	#preventive
			5. Packet filtering and port restriction;	#preventive #corrective
Complex multi-party environment	Improper edge actors drill check; Human error; Improper app lifecycle management; Improper monitoring mechanisms for all actors; Improper collection of charging information;	Unauthorized access to data, eavesdropping, DoS, lateral movements, tampering, spoofing attacks, operator error; Improper controlling and accounting; Supplier vulnerabilities (MEC parties); Fraud	1. Monitor MEC Apps parameters; 2. Validate app behavior integrity (trusted computing); 3. Identify and detect vulnerabilities; 4. CIS baselines application;	#detective
			5. Trust assessment of involved parties; 6. Network segmentation; 7. Segregation of data and resources; 8. Secure collection and transmission of charging information; 9. Propper logging of security events; 10. External location for log collection; 11. Access control on logs;	#preventive
Edge of the network locations	Improper monitoring of physical facilities or security events; Improper maintenance, capacity planning, contingency planning	Physical security: destruction, unauthorized access, data theft or tampering, abuse of privileges; Failures, unavailable services	1. Facilities monitoring: physical security and events review; 2. Resource monitoring;	#preventive #detective
			3. Resource allocation techniques / capacity management; 4. Backup and contingency planning;	#preventive #corrective
Application-Programming Interfaces (APIs)	Exploitation of software vulnerabilities (open source APIs, third-party integration); improper EAS API implementation	Unauthorized access to data, eavesdropping, interception, DoS, elevation of privileges	1. Common API Framework (CAPIF) enforcement; 2. Proper authentication and authorization; 3. Proper event logging;	#preventive
			4. DDoS protection policies; 5. Cyberattacks detection.	#preventive #detective #corrective

Proper controlling and accounting for deployments are recommended in [9]. A possible consequence of a successful attack is using cloud resources for malicious activities. Cross-contamination and improper isolation of resources

should be considered in the design phase, as these can cause an outage of other services hosted on the same platform. Resilience is strongly recommended in the implementation of telecom-specific functions as well as sensitivity segregation of microservices to avoid or respond to availability attacks [9]. From a threat perspective, Table 1 lists: exploitation of vulnerabilities in third-party applications and host platforms, abuse of privilege, eavesdropping and other intrusion techniques, and improper monitoring of events [14]. Twelve measures were identified for the cloud-native characteristic. The measures are divided by ISO "control type" attribute and their role in preventing, detecting, or correcting security incidents. The preventive measures proposed for the cloud-native feature refer to implementing proper data protection (through data encryption, secure transport protocols, and controlled access to information) [9], enforcement of security regulations, and the assessment of deployed applications – a measure that could aid in detecting behavior deviation. System patching is a preventive measure (keeping the system up to date) and corrective (after finding the root cause of the security incident). For detection, it is recommended to rely on the proper collection, protection, and analysis of logs [9].

Given the distributed nature of MEC, five measures are suggested to counteract identified threats. Among the benefits is user data privacy (as traffic can be contained locally) and facilitating high-performance services [18]. One security risk is failing to enforce the same security mechanisms on all MEC hosts [19]. On the other hand, a MEC host can be isolated in case of attack detection, with minimum impact on service delivery [19]. A telecom-specific vulnerability is the improper implementation of lawful interception mechanisms. This mechanism is ensured in control and user plane separation (CUPS) architecture [14]. The five measures suggested to counteract DDoS attacks, data tampering, and failure to respond to lawful interception are classified as preventive and corrective. Packet filtering and port restriction is a measures that can be applied both upon attack suspicion and at attack identification.

MEC is a complex ecosystem, a framework where multiple parties interact and depend on one another [14]. MEC has multiple types of assets, each of which can be managed by a different party: MEC host, MEC platform, MEC application, and virtualized infrastructure[9]. The benefits in the adoption of this multi-party framework are lower time to market and encouraging 5G adoption. The vulnerabilities of such a diverse landscape come from improper third-party trust assessment [14,19], human error, improper monitoring of the MEC application lifecycle, and behavior profiling [14]. The risk of fraud arises from the improper collection of charging information [9]. The measures are sorted into preventive and detective control types and aim to assist in preventing or detecting unauthorized access to data, DoS attacks, and fraud. To this purpose, eleven security measures are recommended, of which: trusted computing and CIS (centre for internet security) baselines [14], trust assessment of involved parties [14], application behavior profiling and monitoring, segregation of data and resources, proper logging of charging and security events [9]Click or tap here to enter text..

With respect to where MEC assets are deployed, the main benefits of distributed locations are: faster data offloading and supporting high bandwidth, low latency applications. The threats are related to improper physical security [9][19], maintenance and capacity planning [9]. The four measures presented in Table 1 are: proper facilities monitoring [9][19] and review of security events, resource monitoring, capacity planning and planning for contingency and backup [9]. Measures like backup and contingency planning and resource allocation mechanisms can prevent outage and ensure faster recovery of affected systems.

One of the most important and vulnerable components in MEC are the Application-Programming Interfaces. CAPIF (Common API Framework) is the standard proposed by 3GPP for API implementation in MEC[9]. As these APIs will be exposed for third-party integration, proper authentication and access control must be implemented, as well as availability protection policies[14]. Table 1 suggests five measures for the MEC API security threats, in order to counteract DDoS attacks and unauthorized access to data among others.

The relation between the controls from ISO/IEC 27001:2022 and measures from Table 1 is presented in the following. Categories for each measure listed in Table 1 cover all four code of practice categories: technological, organizational, people, and physical. Only some controls are listed due to article size restraints. As an example, measures related to threat detection can be associated with ISO people control 6.8 (Information security event reporting), ISO technological controls 8.15-8.16 (logging and monitoring) and ISO organizational controls 5.8 (threat intelligence), and 5.24-5.28 (controls related to assessment, response, learning processes in case of information security incidents). Organizational controls such as 5.18 (access rights), 5.12 (classification of information), and technological control 8.12 (data leakage prevention) relate to the first measure from Table 1 cloud-native section.

Although MEC is associated with the telco scene, Table 1 presents multiple issues specific to an IT service environment. These are guidelines and measures for cloud-native applications, distributed services, and API-exposed services. Differences come from the distribution scale specific to MEC and the fact that most IT services are deployed in more contained environments, such as data centers.

Cybersecurity attack goals are almost the same all over the industry: data theft, service disruption, and fraud are among them. The possibility that MEC could be the entry point for many 5GS verticals validates the need for measures and controls. As introduced in Table 1, standard security procedures for IT products must be considered for MEC-deployed applications if the two domains work together to deliver a service.

5. SECURITY RELEVANCE OF THE CURRENT PAPER

MEC, SDN, NFV, and NS are the technologies that enable most of the 5GS use cases. Paper [20] presents the benefits of using these technologies in MEC-based solutions. In the following, a very brief view on security impact is presented, considering these interworking technologies:

1) NFVI and NFV: the security specifications of NFVI can be reused in MEC security design, and the NFV orchestrator can also coordinate MEC apps [19,20].
2) Network slicing: many threats listed in Table 1 can be prevented by separating the traffic and isolating the computing resources. NS is the technology that

enables most 5GS use cases [19].

3) SDN: SDN executes complex networking activities and ensures QoS, thus alleviating the MEC nodes from such tasks. SDN also introduces numerous threats to edge services. The SDN controller is susceptible to availability attacks, side-channel attacks, and flow poisoning. At the same time, MEC vulnerabilities directly reflect on SDN-based networks [20].
4) Cloud-RAN(CRAN): deploying MEC applications in a CRAN physical location risks resource depletion for network functions by third-party applications [21].

Table 2 presents filtered literature published since 2018.

Table 2

Related work

Reference	Standard	Other standards	MEC threat	Mapping
[19]	ETSI MEC ISG	yes	yes	no
[22]	ITU-T	yes	yes	no
[23]	no	no	brief	no
[24]	ETSI MEC ISG	no	yes	no
[25]	ETSI MEC ISG	no	yes	no
[26]	no	no	yes	no
[27]	ITU-T, NGMN	yes	brief	no
[28]	ETSI MEC ISG	no	brief	no
Present paper	ISO/IEC 2022	yes	yes	yes

The available literature was screened against four criteria. Table 2 presents the papers that have met at least one of the following criteria:

1) Does the work approach security from a standardization work perspective?
2) Does the work reference other standardization work?
3) Does the work include a MEC threat landscape survey?
4) Does the work map the threats on standard-specific attributes?

The paper follows the ISO/IEC 27001:2022 standard and refers to other standardization work in the introduction and the third chapter. The fourth chapter presents a MEC threat landscape analysis and proposes measures for the identified vulnerabilities and threats. Table 1 maps measures to ISO/IEC 27001:2022 controls and suggests their classification based on the "control type" attribute: preventive, detective, and corrective.

Machine learning and artificial intelligence (ML/AI) techniques are gaining higher status and confidence with time. Many research areas are explored in the literature, from medicine [29,30] to renewable energy [31] and telecommunications [32]. Concerning security issues investigated by the literature, Table 3 presents a selection of papers that leverage (ML/AI) techniques to respond to some of the threats identified in Table 1. The learning type was simplified to supervised and unsupervised learning only, while the column "Subject" can be associated with the measures presented in Table 1.

Table 3

ML/AI solutions for telco security assurance

Reference	Learning type	Subject
[33]	Unsupervised	Application behavior assessment
[11]	Supervised	Resource management
[34]	Supervised	Availability attacks detection
[35]	Supervised	False data injection detection

As most of the literature on the security of MEC and telecom networks address threats also presented in Table 1, the current paper can be viewed as a bridge between the information presented in the standardization documents and the literature. Figure 3 presents the connection between the three elements: standardization organizations' work – current paper – literature.

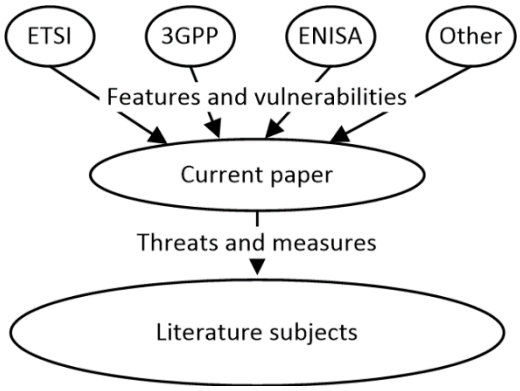

Fig. 3 – Relevance and positioning of the current paper

6. CONCLUSIONS

The paper presents a new perspective on the security of MEC, an emerging technology in telecommunications, by studying information security management system controls. Starting from MEC characteristics and benefits, a threat drill down is suggested for measures and ISO/IEC 27001:2022 control identification. To the authors' best knowledge, this paper represents the first attempt to map MEC threats and measures to ISO/IEC 27001:2022 controls and control types.

3GPP 5G advanced roadmap reveals greater interest in artificial intelligence and machine learning (AI/ML). As in [36], proposed studies address various areas such as network energy savings and network performance, support for AI/ML-enabled applications, and management of AI/ML capabilities in 5GS. Another study [37] that might accompany Release 18 addresses potential security and privacy issues considering the evolving suite of AI/ML-based services that will use 5GS advanced.

In future work, we aim to contribute to these directions and study the maturity of AI/ML solutions concerning guaranteeing security in telecommunications.

ACKNOWLEDGMENT

The results presented in this article have been funded by the Ministry of Investments and European Projects through the Human Capital Sectoral Operational Program 2014-2020, Contract no. 62461/03.06.2022, SMIS code 153735.

Received on 20 May 2023.

REFERENCES

1. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta. D. Sabella, *On multi-access edge computing: a survey of the emerging 5g network edge cloud architecture and orchestration*, IEEE Communications Surveys and Tutorials, **19**, *3*, pp. 1657–1681 (2017).
2. B.M. Gago, *How network slicing works and why it is key to 5G - Telefónica*, telefonica.com, (2022). Accessed: Mar. 19, 2023. [Online]. Available: https://www.telefonica.com/en/communication-room/blog/how-network-slicing-works-and-why-it-is-key-to-5g/
3. G. Carrozzo, R. Szabo, K. Pentikousis, *Network function virtualization:*

resource orchestration challenges draft-caszpe-nfvrg-orchestration-challenges-00 (2015). Accessed: Mar. 19, 2023. [Online]. Available: https://datatracker.ietf.org/doc/ html/draft-caszpe-nfvrg-orchestration-challenges-00
4. M. Liyanage, P. Porambage, A. Y. Ding, A. Kalla, *Driving forces for multi-access edge computing (MEC) IoT integration in 5G*, ICT Express, **7**, *2*, pp. 127–137 (Jun. 2021).
5. ***5GPPP Architecture Working Group, *View on 5G architecture*, (2021).
6. ***EPRS Scientific Foresight Unit (STOA), *Privacy and security aspects of the 5G technology* (2022). Accessed: Mar. 20, 2023. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/697205/EPRS_STU(2022)697205(ANN1)_EN.pdf
7. ***SecurityGen, *Risks in telecom supply chain security*. Accessed: Mar. 20, 2023. [Online]. Available: https://secgen.com/articles/RISKS_IN_TELECOM_SUPPLY_CHAIN_SECURITY.
8. ***ETSI White Paper #36, *Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specifications* (2020). Accessed: Apr. 02, 2023. [Online]. Available: www.etsi.org
9. ***European Union Agency for Cybersecurity, *ENISA Threat Landscape for 5G Networks Report*, ENISA (2020). Accessed: Feb. 15, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.
10. D. Sabella et al., *Edge computing: from standard to actual infrastructure deployment and software development* (2021). Accessed: Sep. 24, 2021. [Online]. Available: https://networkbuilders.intel.com/solutionslibrary/edge-computing-from-standard-to-actual-infrastructure-deployment-and-software-development
11. A.F. Glavan et al., *Cognitive edge computing through artificial intelligence*, 13th International Conference on Communications, COMM 2020 – Proceedings, pp. 285–290 (2020).
12. ***Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | shaping Europe's digital future*. Accessed: Apr. 24, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
13. ***European Union Agency for Cybersecurity, *EUCS – cloud services scheme*, ENISA (2020). Accessed: Apr. 24, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.
14. D. Sabella et al., *MEC security: Status of standards support and future evolutions,* ETSI White Paper, **46**, pp.1-26 (2021). Accessed: Apr. 02, 2023. [Online]. Available: www.etsi.org
15. ***International Organization for Standardization, *ISO/IEC 27001 standard – information security management systems* (2022).
16. ***ISO/IEC 27011 ISMS for telecoms* (2016), Accessed: Apr. 18, 2023. [Online]. Available: https://www.iso27001security.com/html/27011.html
17. ***International Telecommunication Union, *X.1051: Information technology - security techniques - code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations* (2016)
18. Q. Pham, F. Fang, *A Survey of multi-access edge computing in 5G and beyond: fundamentals, technology integration, and state-of-the-art*, IEEE Access, **8**, pp. 116974-117017 (2020).
19. G. Nencioni, R.G. Garroppo, R.F. Olimid, *5G multi-access edge computing: security, dependability, and performance*, arXiv preprint arXiv:2107.13374 (2021).
20. M. Liyanage, P. Porambage, A. Y. Ding, *Five Driving Forces of Multi-Access Edge Computing*, arXiv preprint arXiv:1810.00827 (2018).
21. A. Reznik et al., *Cloud RAN and MEC: A perfect pairing*, ETSI MEC 23 **25** (2018).
22. I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, *Security for 5G and beyond*, IEEE Communications Surveys & Tutorials, **2**, *4*, pp.3682-3722 (2019).
23. F. Salahdine, T. Han, and N. Zhang, *Security in 5G and beyond recent advances and future challenges*, Security and Privacy, **6**, *1*, p.e271 (2023).
24. P. Ranaweera, A. D. Jurcut, M. Liyanage, *Survey on multi-access edge computing security and privacy*, IEEE Communications Surveys and Tutorials, **23**, *2*, pp. 1078–1124 (2021).
25. N. Abbas, Y. Zhang, A. Taherkordi, T. Skeie, *Mobile Edge Computing: A Survey*, IEEE Internet Things J, **5**, *1*, pp. 450–465 (2018).
26. S.M. Vidhani, A.V. Vidhate, *Security Challenges in 5G Network: A technical features survey and analysis*, 5th IEEE International Conference on Advances in Science and Technology, ICAST 2022, pp. 592–597 (2022).
27. R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions*, IEEE Communications Surveys and Tutorials, **22**, *1*, pp. 196–248 (2020).
28. P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, *Survey on Multi-Access Edge Computing for Internet of Things Realization*, IEEE Communications Surveys and Tutorials, 20, 4, pp. 2961–2991 (2018), doi: 10.1109/COMST.2018.2849509.
29. A. Lakshmi, *A disease prediction model using spotted hyena search optimization and bi-lstm*, Rev. Roum. Sci. Techn. – Électrotechn. Et Énerg, **68**, *1*, pp. 113–118 (2023).
30. H. Gupta et al., *Category boosting machine learning algorithm for breast cancer prediction*, Rev. Roum. Sci. Techn.– Électrotechn. et Énerg, **66**, *3*, pp. 201–206 (2021).
31. N. Sabri, A. Tlemçani, A. Chouder, *Real-time diagnosis of battery cells for stand-alone photovoltaic system using machine learning techniques*, Rev. Roum. Sci. Techn.– Électrotechn. et Énerg, **66**, *2*, pp. 105–110 (2021).
32. J. Zhu, Y. Song, D. Jiang, H. Song, *A new deep-q-learning-based transmission scheduling mechanism for the cognitive internet of things*, IEEE Internet Things J, **5**, *4*, pp. 2375–2385 (2018).
33. A.F. Glavan, V. Croitoru, *Cloud environment assessment using clustering techniques on microservices dataset*, 14th International Conference on Communications, COMM 2022 – Proceedings, pp. 1-6 (2022).
34. F. Hussain et al., *A two-fold machine learning approach to prevent and detect IoT botnet attacks*, IEEE Access, **9**, pp. 163412–163430 (2021).
35. S.R. Sankepally, N. Kosaraju, V. Reddy, U. Venkanna, *Edge intelligence based mitigation of false data injection attack in IoMT framework*, OITS International Conference on Information Technology (OCIT), pp. 422–427 (2022).
36. ***Finding AI in 3GPP* (2022), Accessed: Mar. 16, 2023. [Online]. Available: https://www.3gpp.org/technologies/finding-ai-in-3gpp.
37. ***3GPP, *TR Specification # 33.898*, 3GPP Portal (2022), Accessed: Mar. 16, 2023. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4088