University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

Risk Analysis and Threat Ranking for the Mobile Edge Computing Layer of the Fifth Generation Mobile Network

Mohammad Ragheb[1] and Mohammad Reza Keshavarzi[2]

1. Corresponding author, Invited Professor of Telecommunication Engineering at Qom University of Technology, Email: Mohammad_Ragheb@yahoo.com
2. ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran, Email: mrkeshavarzi@itrc.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 17 July 2025
Received in revised form 29 Aguest 2025
Accepted 6 Octobr 2025
Published online 1 December 2025

Keywords:
Fifth Generation Mobile Network (5G), Multiple Access Edge Computing (MEC), MEC Security Vulnerabilities and Threats, Conventional and Specific MEC Security Solutions, Threat ranking.

ABSTRACT

The fifth generation of mobile networks (5G) offers new and advanced services such as virtual/augmented reality (AR/VR), high-definition video streaming, remote surgery, Internet of Things (IoT) and smart cars with strict requirements. The European Telecommunications Standards Institute (ETSI) has introduced Multiple Access Edge Computing (MEC) for efficient and fast data processing in mobile networks. MEC is a key technology that enables these new services by deploying multiple appliances with computing and storage capabilities at the edge of the network, close to end users. Among other technological requirements, security is an important factor in realizing MEC deployment. In this article, while reviewing the 5G architecture and then focusing on the MEC architecture, threats, vulnerabilities and security solutions provided by researchers and scientific authorities in this field are examined. Finally, by evaluating the impact and probability of success of threats in 5G, we analyze the risk in order to provide a good ranking of threats. The results of our studies and research in this article will help secure the 5G network and deploy security solutions.

Cite this article: Ragheb, M. & et al, (2025), Risk Analysis and Threat Ranking for the Mobile Edge Computing Layer of the Fifth Generation Mobile Network. *Enginiiring Management and Soft Computing, 11* (2). 282-325.
DOI: https://doi.org/10.22091/jemsc.2025.13352.1287

DOI: https://doi.org/10.22091/jemsc.2025.13352.1287
Publisher: University of Qom

1) INTRODUCTION

Multi-access Edge Computing (MEC) is an emerging paradigm strongly proposed by the European Telecommunications Standards Institute (ETSI) to overcome the problems arising from complexities in evolving mobile and wireless communication networks. The fundamental principle in MEC is to extend cloud computing (CC) capabilities to the edge of the mobile network to mitigate the limitations attributed to the existing cloud infrastructure [1]. In other words, MEC encompasses data centers and processing units in an aggregated manner, such that computing, storage, networking, and data analysis resources are deployed in locations close to the data source [2] and [3]. The fifth generation of mobile technology (5G) is one of the rationales for the emergence of MEC. The guaranteed performance criteria of 5G include: data rates exceeding 10 Gbps, service-level latency below 1 ms, ultra-high reliability of 99.99999%, a 90% reduction in energy consumption, and support for 300,000 devices in a single cell [1] and [4]. To meet these requirements, migrating the service infrastructure to a nearby location is a critical approach. Therefore, MEC enables new 5G services by deploying multiple devices with computing, storage, and network service capabilities at the edge of the network, close to end-users, solving latency, bandwidth, and reliability issues for emerging use cases such as smart vehicles, virtual/augmented reality (AR/VR), high-quality video streaming, remote surgery, and the Internet of Things (IoT), which require service delivery close to users. These factors have made MEC a prominent technology beyond 5G deployment.

Network security means securing communication networks from intrusions and potential vulnerabilities, based on which confidentiality, integrity, availability of information, authentication, and access authorization are achieved. The emergence of software-based approaches in the 5G mobile network, such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Network Slicing (NS), necessitates additional requirements for ensuring security [5]. Meanwhile, MEC is the access point to all services published by the Radio Access Network (RAN) layer. This entity is one of the weakest points in the entire network in terms of security. Most IoT devices on the market use weak encryption schemes and other security measures to maintain an affordable price range in order to compete. Deploying cloud computing resources in MEC, in data centers or data rooms with much less physical control and protection than centralized data centers, exposes critical computing resources to physical security threats that can lead to service compromise or even access to central resources. Most of these devices are vulnerable to cloning and physical tampering, exposing the entire mobile network to numerous attacks [1]. The authors in reference [6] examined the literature and challenges of MEC with respect to three aspects: security, performance, and reliability. Maintaining confidentiality, integrity, and trust management guarantees are key requirements in MEC deployment. It is evident that virtualization technologies are vital for realizing MEC and creating a serviceable platform with dynamic resource allocation capabilities. Vulnerabilities and potential attacks on virtual machines (VMs) are unique and have significant implications for the MEC system.

2) Solution METHOD

2-1) Equation

Risk= Probability of a successful threat* Severity of that threat (1)

3) Conclusion

In 5G networks, edge computing enables efficient and rapid data processing in mobile networks. Multi-access Edge Computing (MEC) is a key technology that facilitates these new services by deploying multiple devices with computing and storage capabilities at the network edge, close to end-users. In this context, security is a critical factor in realizing MEC deployment. In this paper, we review the 5G architecture and then focus on the MEC architecture, examining the threats, vulnerabilities, and security solutions proposed by academic references. In the next step, we analyze the risk criteria by evaluating the impact/severity and probability of success of the identified threats to 5G. Using the obtained risks,

we rank the threats. The results of this paper indicate that the top 5 threats in the 5G mobile edge network are, in order: APTs, DoS/DDoS, Spoofing, Privilege Escalation, and Reduction of Quality (RoQ). The results of this paper contribute to securing the 5G network and deploying security solutions.

4) Tables and Figures

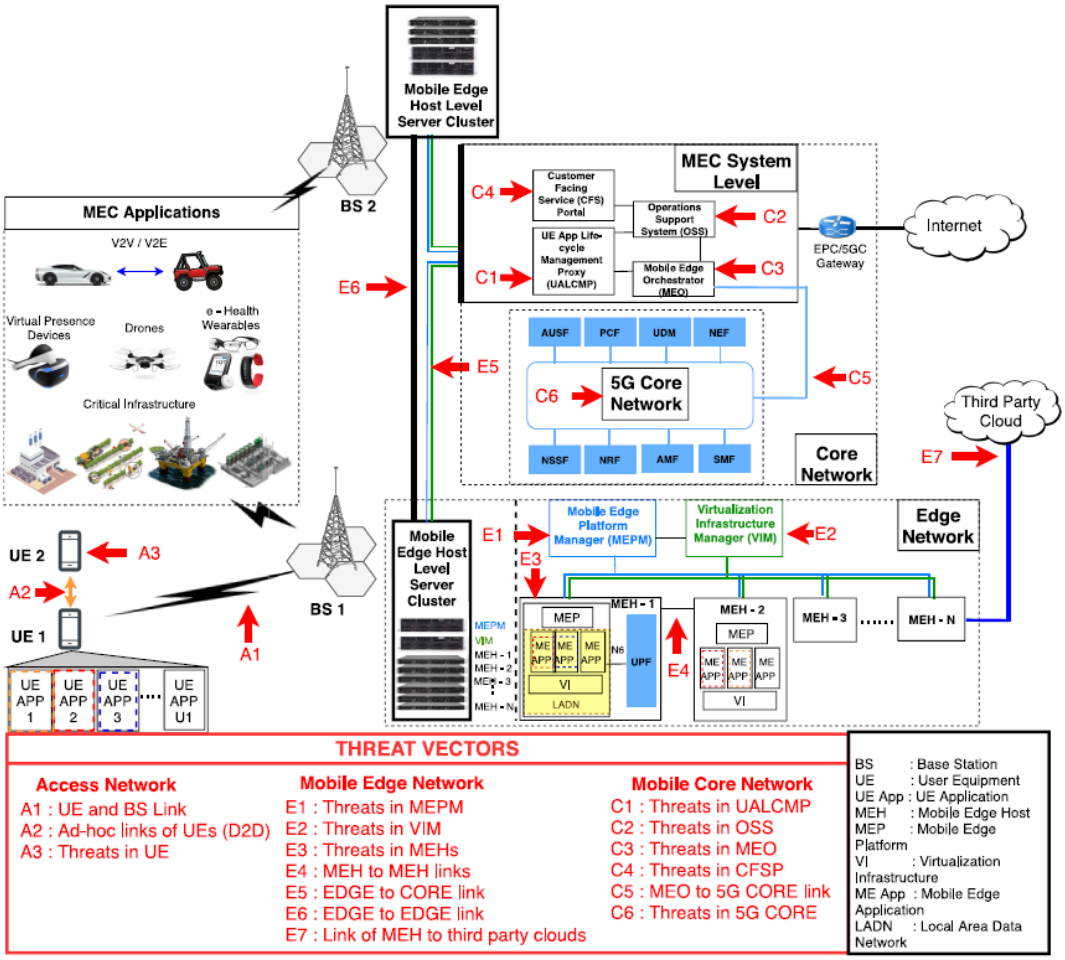


Fig. 1: Locational threat vectors of a typical MEC deployment

Table 1: Threats/Attacks and their impact on CIAAA security requirements

Threats/Attacks	Confidentiality	Integrity	Availability	Authentication	Authorization	Impact/Damage/Severity between 0` and 10
General threats						
Viruses / Worms		×	×	×		Medium (5)
DoS/DDos			×			High (8)
Eavesdropping and Hijacking	×	×		×	×	High (8)

Jamming	×		×			High (8)
MitM	×	×	×			High (8)
Relay attack	×	×	×			Medium (5)
APTs	×	×			×	Critical (10)
Sybil attack	×	×	×			High (8)
Spoofing attack	×	×	×	×		High (8)
Non- Crypt analytic attacks						
Side-Channel Attacks (SCAs)	×	×	×		×	High (8)
Physical damage		×	×		×	High (8)
Hardware Trojan (HT)	×	×	×			Critical (10)
Networking/Routing attacks						
Malicious Node injection		×	×	×		High (8)
Sinkhole attack	×	×	×			Medium (5)
Wormhole attack	×	×	×			High (8)
Reduction of Quality (RoQ) attack	×	×	×			High (8)
Denial of sleep attack	×	×	×			Medium (5)
Virtualization/VM based Threats						
Service manipulation		×	×		×	High (8)
Privilege Escalation	×	×	×		×	Critical (10)
VM Manipulation attack	×	×	×			High (8)
DNS Amplification/Manipulation attack	×	×	×			High (8)
VM escape attack	×	×	×		×	Critical (10)
VNF location shift attack	×	×	×			High (8)
Security log troubleshooting failure	×				×	Medium (5)
Softwarized Threats						

Software Vulnerability	×	×	×	×	×	High (8)
Data exfiltration **(include location privacy)**	×	×	×			Critical (10)
Malicious code injection	×	×	×	×		High (8)

References

[1] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018. DOI: 10.1109/COMST.2018.2849509

[2] A. Reznik, Y. Fang, and S. Ullah, "MEC in an enterprise setting: A solution outline," ETSI, Sophia Antipolis, France, White Paper, 2018. Accessed: May 16, 2019. [Online]. Available:
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_ FINAL.pdf .
ISBN No. 979-10-92620-25-2

[3] "ENISA threat landscape" report, Oct. 2023.

[4] 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 Commun.Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017. **DOI:** 10.1109/COMST.2017.2705720

[5] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018. DOI:10.1109/COMST.2018.2815638

[6] G. Nencioni, R. G. Garroppo and R. F. Olimid, "5G Multi-Access Edge Computing: A Survey on Security, Dependability, and Performance," *IEEE Access*, vol. 11, pp. 63496-63533, 2023. **DOI:** 10.1109/ACCESS.2023.3288334

[7] P. Ranaweera, A. D. Jurcut, M. Liyanage, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078 – 1124, 2021. DOI: 10.1109/COMST.2021.3062546

[8] *Multi-Access Edge Computing (MEC); Terminology*, Standard GS MEC 001, Version 3.1.1, ETSI, Jan. 2022.

[9] *Cloud Edge Computing: Beyond the Data Center*, OpenStack, Austin, TX, USA, 2018.

[10] *Multi-Access Edge Computing (MEC); Framework and Reference Architecture*, Standard GS MEC 003, Version 3.1.1, Mar. 2022.

[11] *Multi-Access Edge Computing (MEC); Study on Inter-MEC Systems and MEC-Cloud Systems Coordination*, Standard GR MEC 035, Version 3.1.1, ETSI, Jun. 2021.

[12] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing gadget-free digital services," *Computer*, vol. 51, no. 11, pp. 66–77, 2018. DOI: 10.1109/MC.2018.2876017

[13] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 181–186. DOI: 10.1109/CSCN.2017.8088619

[14] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020. DOI: 10.1109/COMST.2019.2933899

JEMSC.QOM
شاپا الکترونیکی: ۲۶۷۵-۲۵۳۸
مدیریت مهندسی و رایانش نرم
دانشگاه قم

تحلیل ریسک و رتبه‌بندی تهدیدات لایه محاسبات لبه شبکه تلفن همراه نسل پنجم

محمد راغب[۱] و محمدرضا کشاورزی[۲]

۱. نویسنده مسئول، دکترای مهندسی برق، مخابرات (سیستم). رایانامه: mohamad_ragheb@yahoo.com
۲. استادیار، پژوهشکده فناوری ارتباطات، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران. رایانامه: mrkeshavarzi@itrc.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۱/۰۷

تاریخ بازنگری: ۱۴۰۴/۰۴/۱۶

تاریخ پذیرش: ۱۴۰۴/۰۶/۱۳

تاریخ انتشار: ۱۴۰۴/۰۹/۱۰

کلیدواژه‌ها:
شبکه تلفن همراه نسل پنجم (G۵)، رایانش لبه چنددسترسی (MEC)، آسیب‌پذیری‌ها و تهدیدات امنیتی MEC، راهکارهای امنیتی مرسوم و خاص MEC، اولویت‌بندی تهدیدات.

چکیده

نسل پنجم شبکه‌های تلفن همراه (G۵)، خدمات جدید و پیشرفته‌ای ازجمله واقعیت مجازی/افزوده (AR/VR)، پخش ویدئو با کیفیت بالا، جراحی از راه دور، اینترنت اشیا (IoT) و خودروهای هوشمند را با الزامات سخت‌گیرانه ارائه می‌دهد. موسسه استانداردهای ارتباطات از راه دور اروپا (ETSI)، محاسبات لبه با دسترسی چندگانه (MEC) را برای پردازش کارآمد و سریع داده‌ها در شبکه‌های تلفن همراه معرفی کرده‌است. MEC یک فناوری کلیدی است که این خدمات را با استقرار چندین تجهیز با قابلیت‌های محاسباتی و ذخیره‌سازی در لبه شبکه، نزدیک به کاربران نهایی ارائه می‌نماید. در میان سایر الزامات فناورانه، امنیت عامل مهمی در تحقق استقرار MEC می‌باشد. در این مقاله، ضمن مروری بر معماری G۵ و سپس تمرکز بر معماری MEC، تهدیدات، آسیب‌پذیری‌ها و راهکارهای امنیتی ارائه‌شده توسط پژوهشگران و مراجع علمی در این حوزه بررسی می‌شوند. درنهایت با ارزیابی تاثیر/شدت و احتمال موفقیت تهدیدات بر روی شبکه G۵، به تحلیل ریسک می‌پردازیم تا به کمک آن، رتبه‌بندی خوبی از تهدیدات ارائه کرده باشیم. نتایج مطالعات و تحلیل‌های ما در این مقاله، به بهره‌برداران شبکه G۵ این اطلاع را می‌دهد که باید کدامیک از تهدیدات را در اولویت بررسی قرار داد. نتایج این مقاله، به امن‌کردن شبکه G۵ و استقرار راهکارهای امنیتی کمک می‌کند.

استناد: راغب، محمد و همکاران. (۱۴۰۴). «تحلیل ریسک و رتبه‌بندی تهدیدات لایه محاسبات لبه شبکه تلفن همراه نسل پنجم». *مدیریت مهندسی و رایانش نرم*، دوره ۱۱ (۲). صص: ۳۲۵-۲۸۲. https://doi.org/10.22091/jemsc.2025.13352.1287

ناشر: دانشگاه قم

۱) مقدمه و پیشینه تحقیق

رایانش لبه چنددسترسی[۱] (MEC)، یک الگوی نوپا می‌باشد که استفاده از آن از سوی موسسه استانداردهای مخابرات اروپا (ETSA) جهت غلبه بر مشکلات ناشی از پیچیدگی‌های شبکه‌های ارتباطی سیار و بدون‌سیم درحال‌تکامل بسیار پیشنهاد شده‌است. اصل اساسی در MEC این است که قابلیت‌های رایانش ابری[۲] (CC) را به لبه شبکه تلفن همراه گسترش دهد تا محدودیت‌های نسبت داده‌شده در زیرساخت ابر موجود را ناچیز کند [۱]. به‌عبارت‌دیگر، MEC مراکز داده و واحد پردازش را به‌صورت تجمیعی دربر دارد بطوریکه منابع محاسباتی، ذخیره‌سازی، شبکه‌بندی و تحلیل داده در مکان‌های نزدیک به منبع داده مستقر می‌گردد [۲] و [۳]. نسل پنجم فناوری تلفن همراه (5G)، یکی از دلایل منطقی برای ظهور MEC است. معیارهای عملکرد تضمین‌شده 5G عبارتنداز: نرخ داده بالغ بر ۱۰ گیگابایت بر ثانیه، تاخیر سطح خدمت زیر ۱ میلی‌ثانیه، قابلیت‌اطمینان فوق‌العاده بالا ۹۹.۹۹۹۹ درصد، کاهش مصرف انرژی ۹۰ درصد و پشتیبانی از ۳۰۰۰۰۰ تجهیز در یک سلول واحد [۱] و [۴]. به‌منظور برآورده‌کردن این الزامات، مهاجرت زیرساخت خدمات به یک مکان نزدیک، یک رویکرد حیاتی است. بنابراین MEC خدمات جدید 5G را با استقرار چندین تجهیز با قابلیت‌های رایانشی، ذخیره‌سازی و خدمات شبکه در لبه شبکه، نزدیک به کاربران نهایی فعال می‌کند و مشکلات تاخیر، پهنای باند و قابلیت‌اطمینان موارد استفاده نوظهور مانند خودروهای هوشمند، واقعیت مجازی/افزوده[۳] (AR/VR)، پخش ویدئو با کیفیت بالا، جراحی از راه دور و اینترنت اشیا[۴] (IoT) که نیاز به ارائه خدمات نزدیک به کاربران را دارند، حل می‌کند. این عوامل باعث شده‌است که MEC به فناوری برجسته در ورای استقرار 5G تبدیل شود.

امنیت شبکه به‌معنای امن‌سازی شبکه‌های ارتباطی از نفوذها و آسیب‌پذیری‌های احتمالی می‌باشد و بر مبنای آن، محرمانگی[۵]، یکپارچگی[۶]، دردسترس‌بودن (دسترسی‌پذیری)[۷] اطلاعات، احراز هویت و اجازه دسترسی[۸] حاصل می‌گردد. ظهور رویکردهای نرم‌افزاری در شبکه تلفن همراه 5G مانند: شبکه‌های نرم‌افزارمحور[۹] (SDN)، مجازی‌سازی عملکرد شبکه[۱۰] (NFV) و برش شبکه[۱۱] (NS)، نیازمند الزامات بیشتری برای تضمین امنیت هستند [۵]. در این میان، MEC نقطه

---

1 Multi-Access Edge Computing

۲ Cloud computing؛ رایانش ابری به مجموعه‌ای از فناوری‌های لازم و توانمند اطلاق می‌شود که راهکارهای انعطاف‌پذیر وخدمات گسترده‌تری را برای سازمان‌ها یا اشخاص ارائه می‌دهد. به‌عبارت‌دیگر، رایانش ابری به ارائه خدمات محاسباتی مبتنی بر تقاضا، از برنامه‌های کاربردی گرفته تا فضای ذخیره‌سازی (Storage) و توان محاسباتی (Computational power) از طریق اینترنت و با روش پرداخت بر مبنای مصرف گفته می‌شود. رایانش ابری مبتنی بر نیاز هر فرد به او خدمت‌رسانی می‌کند. از مزایای رایانش ابری می‌توان به صرفه‌جویی در هزینه، ادغام منابع، انعطاف‌پذیری آسان و مقیاس‌پذیربودن اشاره کرد.

3 Augmented Reality/Virtual Reality
4 Internet of things
5 Confidentiality
6 Integrity
7 Availability

۸ Authentication and authorization، خاطر نشان می‌نماید احراز هویت تایید می‌کند شخص یا سیستم، هویت صحیحی دارد درحالیکه اجازه دسترسی، مشخص می‌کند آن شخص یا سیستم به چه بخش‌ها و عملیاتی دسترسی دارد. در فرآیند کامل، ابتدا هویت فرد یا سیستم تایید می‌شود (Authentication) و سپس سطح دسترسی و مجوزهای موردنیاز برای آن تعیین می‌شود (Authorization).

9 Software defined network
10 Network Function Virtualization
11 Network Slicing

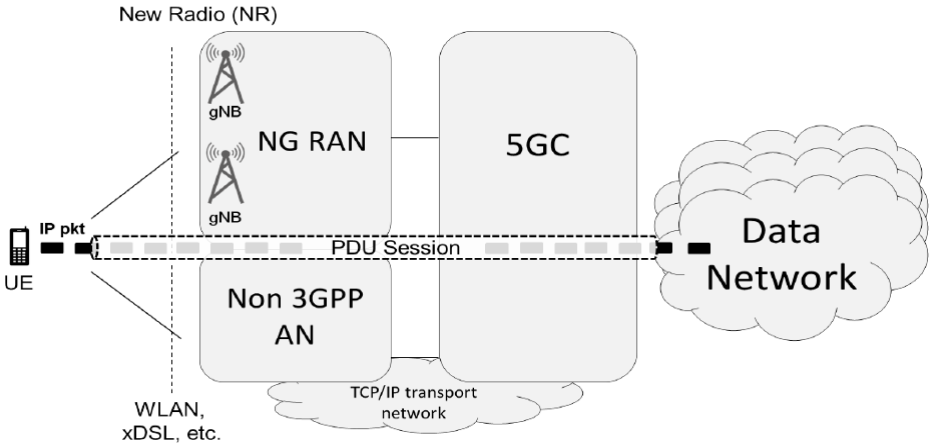
دسترسی به تمام خدماتی است که توسط لایه شبکه دسترسی رادیویی[۱۲] (RAN) منتشر می‌شود. این موجودیت یکی از ضعیف‌ترین نقاط کل شبکه از نظر امنیت است. اکثر تجهیزات IoT موجود در بازار به‌منظور رقابت، از طرح‌های رمزگذاری ضعیف و سایر اقدامات امنیتی برای حفظ محدوده قیمت مقرون‌به‌صرفه استفاده می‌کنند. استقرار منابع محاسباتی ابر در MEC در مراکز داده یا اتاق‌های داده، با کنترل فیزیکی و حفاظت بسیار کمتری نسبت به مراکز داده مرکزی، منابع محاسباتی مهم را درمعرض تهدیدات امنیتی فیزیکی قرار می‌دهد که می‌تواند باعث به‌خطر افتادن خدمت یا حتی دسترسی به منابع مرکزی شود. اکثر این تجهیزات در برابر همسانه‌سازی[۱۳] و دستکاری فیزیکی آسیب‌پذیر هستند و کل شبکه تلفن همراه را درمعرض حملات بی‌شماری قرار می‌دهند [۱]. نویسندگان در مرجع [۶]، ادبیات و چالش‌های MEC را با توجه به سه جنبه امنیت، عملکرد و قابلیت‌اطمینان مورد بررسی قرار داده‌اند. حفظ محرمانگی، یکپارچگی و تضمین‌های مدیریت اعتماد، از الزامات اصلی در استقرار MEC هستند. بدیهی است فناوری‌های مجازی‌سازی برای تحقق MEC و ایجاد یک سکوی قابل خدمت با قابلیت تخصیص منابع پویا، حیاتی هستند. آسیب‌پذیری‌ها و حملات محتمل بر روی ماشین‌های مجازی[۱۴] (VM) منحصربه‌فرد هستند و پیامدهای قابل‌توجهی را برای سیستم MEC ایجاد می‌کنند.

در این مقاله، با مطالعه و بهره‌مندی از اسناد اصلی استانداردسازی 5G ازجمله 3GPP و ENISA[۱۵] و نیز سایر مراجع [۳] و [۷]، به دسته‌بندی تهدیدات، آسیب‌پذیری‌ها و راهکارهای امنیتی ارائه‌شده توسط پژوهشگران و مراجع علمی در این حوزه می‌پردازیم. همچنین با ارزیابی تاثیر/آسیب[۱۶] و احتمال حضور تهدیدات، میزان ریسک[۱۷] هر کدام از تهدیدات را ارزیابی کرده و به هر کدام نمره‌ایی اختصاص می‌دهیم. درنهایت به رتبه‌بندی تهدیدات احصاشده می‌پردازیم. مطالعات و تحقیقات انجام‌گرفته در این کار پژوهشی، به امن‌کردن شبکه 5G و استقرار راهکارهای امنیتی کمک می‌کند.

۲) معماری شبکه و خدمات 5G

در کلی‌ترین حالت، یک شبکه 5G از یک شبکه دسترسی[۱۸] (AN) یا RAN[۱۹] و یک شبکه هسته [۲۰] (5GC) تشکیل شده‌است (شکل ۱). خود شبکه دسترسی از یک شبکه دسترسی رادیویی نسل جدید (NG-RAN) شامل یک رابط رادیویی جدید[۲۱] (NR) و یا یک شبکه غیر 3GPP (مانند WiFi، xDSL و غیره) تشکیل شده‌است. شبکه AN به یک شبکه 5GC متصل می‌شود. موجودیت‌های مختلف شبکه توسط یک شبکه انتقال TCP/IP زیربنایی متصل می‌شوند.

12 Radio Access Network
13 Cloning
14 Virtual Machine
۱۵ بنگاه اتحادیه اروپا برای امنیت رایانه‌ای (European Network and Information Security Agency)، اتحادیه اختصاص‌داده‌شده برای رسیدن به سطح امنیت بالای رایانه‌ای در اروپا است. این اتحادیه در سال ۲۰۰۴ تاسیس گردیده و اعتمادپذیری محصولات ICT ، خدمات و فرآیندها را با طرح‌های گواهی امنیت رایانه‌ای ارتقا می‌دهد و با ذینفعان کلیدی‌اش برای تقویت قابلیت‌اعتماد در اقتصاد، افزایش انعطاف‌پذیری ساختار اتحادیه و نهایتا برای نگه‌داشتن جامعه اروپا و شهروندانش به‌صورت دیجیتالی امن، از طریق اشتراک دانش، ظرفیت‌سازی و بالابردن سطح آگاهی کار می‌کند.
16 Impact/damage
17 Risk
18 Access network
19 Radio access network
20 5G core
21 New radio interface



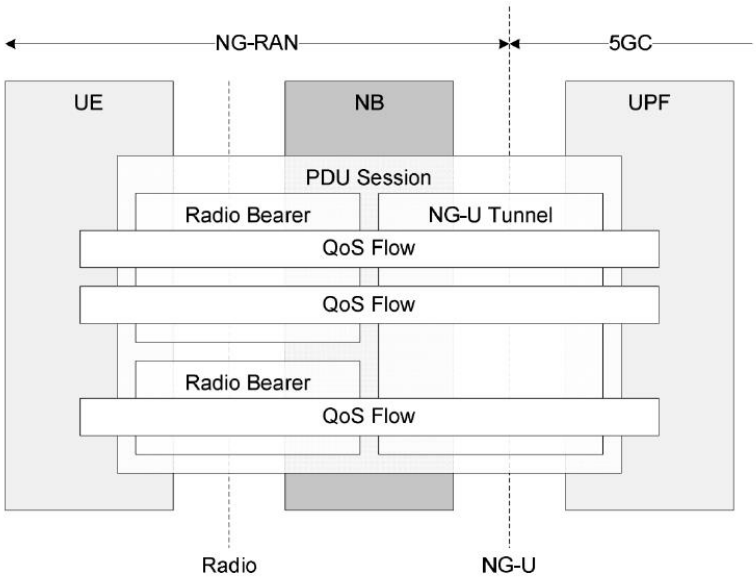
شکل ۱. معماری شبکه 5G از منظر کلی

یک شبکه 5G جهت اتصال تجهیزات کاربر[۲۲] (UE) به شبکه‌های داده خارجی، مورد استفاده قرار می‌گیرد. خدمت اتصال 5G نشست PDU[23] نام دارد. از نقطه‌نظر انتقال، یک نشست PDU توسط دنباله‌ای از تونل‌های NG در 5GC و یک یا چند حامل رادیویی در رابط رادیویی ساخته می‌شود. این مجموعه از "لوله‌ها[۲۴]" درنهایت برای تبادل ترافیک کاربر، UE را به توابع کنترلی آن و به شبکه داده خارجی متصل می‌کند (شکل ۲). وظیفه اصلی شبکه تلفن همراه، ایجاد و رهاکردن تونل‌ها و حامل‌ها به‌صورت پویاست تا حرکات و حالت‌های کاربر (بیکار، متصل و غیره) را دنبال کند.

یک نشست PDU بسیار شبیه یک حامل EPS[۲۵] در 4G-LTE است. درواقع یک نشست PDU می‌تواند نه تنها بسته‌های IP صفحه کاربر بلکه اترنت یا فریم‌های بدون ساختار را نیز منتقل کند. بنابراین امکان ارتباط لایه دوم را بین گروه‌های UE فراهم می‌کند. مدل 5G QoS مبتنی بر مفهوم جدید جریان QoS[۲۶] است. جریان‌های QoS مختلف ممکن است به یک نشست PDU تعلق داشته باشد[۲۷].

در NG-RAN، جداسازی صفحه کنترل و کاربر[۲۸] انجام می‌شود. در صفحه کاربر، یک یا چند تابع صفحه کاربر[۲۹] (UPF) وجود دارد که نشست PDU را تشکیل می‌دهند و عمدتا ارسال بسته بین تونل‌های مختلف NG-U (شکل ۲) را انجام می‌دهند. سایر توابع شبکه متعلق به صفحه کنترل می‌باشند.

22 User Equipment
23 Protocol data unit
24 Pipes
25 EPS bearer
26 Quality of Service flow
۲۷ خاطرنشان می‌نماییم بهترین دانه‌بندی QoS، حامل EPS است. خدمات QoS مختلف به حامل‌های QoS مختلف نیازمندند.
28 Control and User Plane Separation
29 User Plane Function



شکل ۲. نشست‌های PDU و جریان‌های QoS صفحه کاربر

یکی از مهمترین نوآوری‌ها در معماری 5G، مجازی‌سازی کامل شبکه هسته است. به‌عنوان مثال: نرم‌افزارسازی توابع شبکه، قابلیت حمل آسان‌تر و انعطاف‌پذیری بیشتر سیستم‌ها و خدمات شبکه را ممکن می‌سازد. شبکه‌های نسل پنجم این مزیت را دارند که در تخصیص منابع شبکه، انعطاف‌پذیر هستند. درواقع SDN و NFV این سطح از چابکی را فراهم می‌کنند. مجازی‌سازی تابع شبکه(NFV)، فناوری توانمندکننده را برای قراردادن توابع مختلف شبکه در اجزای مختلف شبکه براساس نیازها/ملزومات عملکرد فراهم می‌کند و نیاز به سخت‌افزار مخصوص تابع یا خدمت را از بین می‌برد. شبکه‌بندی نرم‌افزارمحور (SDN)، کارکردهای شبکه سطح پایین را برای ساده‌کردن مدیریت شبکه خلاصه می‌کند.

۳) فناوری توانمندکننده MEC

معیارهای عملکرد تضمین‌شده 5G شامل: نرخ داده تا ۲۰ گیگابایت بر ثانیه، تاخیر سطح خدمت زیر ۱ میلی‌ثانیه، قابلیت‌اطمینان فوق‌العاده بالا، کاهش مصرف انرژی و پشتیبانی از ۳۰۰۰۰۰ تجهیز در یک سلول واحد می‌باشد. به‌منظور برآورده‌کردن این الزامات، مهاجرت زیرساخت خدمات به یک مکان نزدیک، یک رویکرد حیاتی است. خدمت‌رسان‌های MEC در لبه شبکه 5G، نزدیک‌تر به دکل‌های سلولی و نقاط دسترسی مستقر می‌شوند. لذا MEC منابع محاسباتی، ذخیره‌سازی و شبکه را در لبه فراهم کرده و امکان پردازش محلی داده‌ها را میسر می‌سازد. همچنین MEC میزبان برنامه‌های کاربردی و خدماتی مانند واقعیت افزوده (AR)، تحلیل ویدئویی و خودکارسازی صنعتی است که به تاخیر کم و پهنای باند بالا نیاز دارند. بنابراین ایده MEC، فناوری نوظهور برای نسل پنجم شبکه تلفن همراه و فراتر از آن، با ملاحظات فوق شکل گرفته و طراحی می‌شود.

در مشخصات ETSI [۸]، MEC به‌عنوان "سیستمی که یک محیط خدمات فناوری اطلاعات (IT) و قابلیت‌های رایانش ابری را در لبه شبکه دسترسی فراهم می‌کند و شامل یک یا چند نوع فناوری دسترسی در نزدیکی کاربران خود

است" تعریف می‌شود. MEC درواقع یک فناوری کلیدی است که خدمات جدید 5G را با استقرار چندین تجهیز با قابلیت‌های رایانشی، ذخیره‌سازی و خدمات شبکه در لبه شبکه، نزدیک به کاربران نهایی فعال می‌کند و مشکلات تاخیر، پهنای باند و قابلیت‌اطمینان مواردستفاده نوظهوری مانند یادگیری ماشین[۳۰] (ML)، AR/VR، IoT و توابع شبکه که نیاز به ارائه خدمات نزدیک به کاربران دارند را حل می‌کند.

MEC شاخه‌ای از رایانش ابری است که برنامه‌های کاربردی را از مراکز داده متمرکز به لبه شبکه (نزدیک‌تر به کاربران نهایی و تجهیزات آنها) می‌آورد. رایانش لبه، خدمات رایانشی را در لبه شبکه برای پردازش بلادرنگ و رایانش مبتنی بر ابر برای عملیاتی که قابلیت‌های قوی نیاز دارند، فراهم می‌کند. در غیاب رایانش لبه، پردازش داده در خدمت‌رسان‌های ابری متمرکز انجام می‌شود که منجر به تاخیر بالا و هزینه‌های افزایشی انتقال داده می‌شود. با کمک رایانش لبه، تصمیمات سریع نزدیک کاربر نهایی برای خدمات اضطراری که نیاز به تاخیر کمی دارند، انجام می‌شود. در ادامه، اهمیت MEC برای 5G به‌صورت زیر فهرست شده‌است:

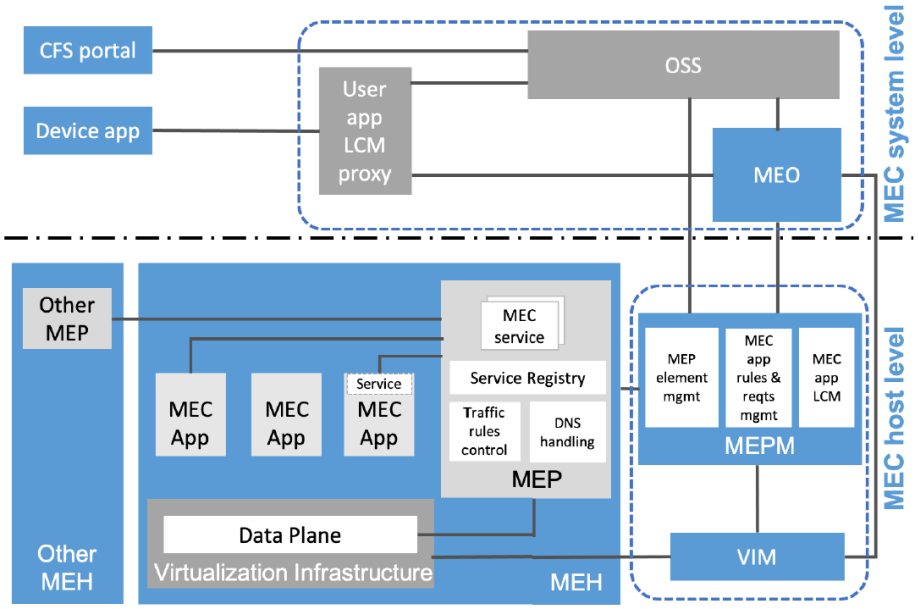
- کاهش تاخیر: با پردازش داده‌ها به‌صورت محلی، MEC مسافتی را که داده‌ها باید طی کنند به‌حداقل می‌رساند که بطور قابل‌توجهی تاخیر را کاهش داده و پاسخگویی برنامه کاربردی را بهبود می‌بخشد.
- افزایش پهنای باند: MEC با پردازش داده‌ها به‌صورت محلی، امکان استفاده کارآمدتر از پهنای باند را فراهم کرده و بار شبکه هسته را کاهش می‌دهد.
- تجربه کاربر[۳۱] را بهبود می‌دهد. برنامه‌های کاربردی مانند واقعیت افزوده (AR)، بازی‌های برخط و پخش ویدئو از تاخیر کم و پهنای باند بالا بهره‌مند می‌شوند و درنتیجه تجربه کاربری روان‌تر و فراگیرتری را ارائه می‌دهند.
- پشتیبانی از برنامه‌های کاربردی جدید: MEC طیف گسترده‌ای از برنامه‌های کاربردی و خدمات جدید را که نیاز به پردازش داده‌های بلادرنگ دارند مانند: وسایل نقلیه خودران، جراحی از راه دور و کارخانه‌های هوشمند، فعال می‌کند.
- برش شبکه: MEC می‌تواند با برش شبکه، یکپارچه شود و به کارگزارها اجازه می‌دهد محیط‌های شبکه سفارشی را برای برنامه‌های کاربردی و خدمات خاص ایجاد کنند.
- افزایش امنیت: با پردازش داده‌ها به‌صورت محلی، MEC می‌تواند با کاهش نیاز به انتقال داده‌های حساس به مراکز داده از راه دور، امنیت داده‌ها و حریم خصوصی را افزایش دهد.
- کارآیی هزینه: MEC می‌تواند با انتقال پردازش از مراکز داده متمرکز و بهینه‌سازی منابع شبکه، به کاهش هزینه‌ها کمک کند.

30 Machine Learning
31 User experience

از این‌رو، MEC کمک می‌کند اهداف 5G ازقبیل: پشتیبانی از باند پهن تلفن همراه (eMBB)، ارتباطات بسیار مطمئن با تاخیر کم (URLLC) و ارتباطات نوع ماشین انبوه[۳۲] (mMTC) محقق شود. علاوه‌براین، MEC توانمندساز هوشمندی لبه[۳۳] است که پیش‌بینی می‌شود یکی از نوآوری‌های اصلی نسل ششم 6G شبکه‌های تلفن همراه باشد.

۳-۱) معماری MEC

سیستم MEC به‌عنوان مجموعه‌ای از میزبان‌های MEC (MEH) و مدیریت MEC لازم برای اجرای برنامه‌های کاربردی MEC تعریف می‌شود [۸]. شکل ۳ معماری مرجع کلی ETSI MEC را نشان می‌دهد که به دو سطح تقسیم می‌شود: سطح میزبان MEC[۳۴] و سطح سیستم MEC[۳۵].



شکل ۳. معماری مرجع ETSI MEC [٦]

۱) سطح میزبان MEC :

سطح میزبان MEC یا MEH شامل یک زیرساخت مجازی‌سازی است که رایانش، ذخیره‌سازی و منابع شبکه را برای اجرای برنامه‌های کاربردی MEC (MEC Apps) و اجرای سکوی MEC (MEC Platform یا MEP) فراهم می‌کند. MEC Apps به‌عنوان ماشین‌های مجازی (VM) اجرا می‌شوند و می‌توانند خدمات MEC را ارائه و مصرف کنند. MEP مجموعه‌ای از کارکردهای[۳۶] موردنیاز برای اجرای MEC Apps است. MEP همچنین می‌تواند میزبان خدمات MEC باشد.

32 Massive Machine-Type Communication
33 Edge intelligence
34 *MEC Host*
35 *MEC system*
36 Functionalities

مدیریت سطح میزبان MEC از مدیر سکوی MEC (MEPM) و مدیر زیرساخت مجازی‌سازی (VIM) تشکیل شده‌است. MEPM چرخه عمر[۳۷]، قوانین و الزامات برنامه‌های کاربردی MEC (به عنوان مثال: منابع موردنیاز، تاخیر) را مدیریت می‌کند و توابع مدیریت عنصر را برای MEP فراهم می‌نماید. VIM تخصیص و نظارت بر منابع مجازی را مدیریت می‌کند و نیز خطاها و گزارش‌های عملکرد را به MEPM ارسال می‌نماید. معمولا برای پیاده‌سازی VIM از OpenStack استفاده می‌شود [۹].

۲) سطح سیستم MEC :

مدیریت سطح سیستم MEC شامل هماهنگ‌کننده MEC (MEO [۳۸]) ، OSS کارگزار[۳۹] و پراکسی مدیریت چرخه عمر برنامه کاربردی [۴۰] (UALCMP) کاربر است [۱۰].

MEO آن مولفه هسته است که یک نمای کلی از سیستم کامل MEC را دارد. MEO بسته‌های برنامه را وارد کار می‌کند (یکپارچگی و اصالت همچنین مطابقت با خطی‌مشی‌های کارگزار را اجرا می‌کند)، MEHهای مناسب برای نمونه‌سازی[۴۱] برنامه کاربردی MEC مبتنی بر قوانین و الزامات مربوطه را انتخاب می‌کند و نمونه‌سازی، خاتمه‌سازی و جابجایی برنامه کاربردی MEC را (درصورت نیاز) راه‌اندازی می‌کند.

OSS کارگزار درخواست‌ها را از پورتال خدمات مواجهه با مشتری CFSP[۴۲] یا از برنامه‌های کاربردی تجهیز از طریق پراکسی LCM برنامه کاربردی کاربر، دریافت می‌کند. CFSP به مشتریان شخص ثالث کارگزارها اجازه می‌دهد تا برنامه‌های کاربردی MEC را انتخاب و سفارش دهند یا اطلاعات سطح خدمات مربوط به برنامه‌های کاربردی ارائه‌شده را دریافت نمایند. برنامه کاربردی در تجهیز مربوطه می‌تواند با سیستم MEC ارتباط برقرار نماید. به‌این‌صورت‌که، در پاسخ به درخواست کاربر از طریق یک برنامه کاربردی تجهیز، یک برنامه کاربردی کاربر در سیستم MEC نمونه‌سازی می‌شود. پراکسی LCM برنامه کاربردی، به برنامه‌های کاربردی تجهیز اجازه می‌دهد تا درخواست ورود، نمونه‌سازی و خاتمه‌سازی برنامه‌های کاربردی کاربر در سیستم MEC را داشته باشد. اگر OSS تصمیم به اعطای درخواست داشته باشد، آن را برای پردازش بیشتر به MEO ارسال می‌کند.

۳) اتحادیه MEC [43]:

معماری MEC می‌تواند گسترش یابد تا امکان ارتباط بین سیستمی MEC را فراهم کند. برای این منظور، اتحادیه MECبه‌عنوان "یک مدل متحد از سیستم‌های MEC که استفاده اشتراکی از خدمات و برنامه‌های MEC را فراهم می‌کند" تعریف می‌شود [۱۱]. جدول ۱ کارکردهای عناصر عمده معماری را خلاصه‌بندی می‌کند [۶] و [۱۰] .

جدول ۱: عناصر کلیدی در معماری MEC

عنصر	کارکردها
۱) MEH :	

37 Life-cycle
38 MEC Orchestrator
39 Operator's Operations Support System
40 User Application Life-Cycle Management Proxy
41 Instantiation
42 Customer Facing Service Portal
43 MEC FEDERATION

MEP (۱-۱	محیط لازم برای برنامه‌های کاربردی MEC را ارائه می‌دهد. خدمات MEC را میزبانی می‌کند. مبتنی بر قواعد ترافیک دریافتی صفحه داده را راهنمایی می‌کند. DNS Proxy/Server را پیکربندی می‌کند. دسترسی به ذخیره‌سازی مداوم را فراهم می‌سازد. اطلاعات زمان‌بندی را فراهم می‌سازد.
۱-۲) ساختار مجازی‌سازی	رایانش، ذخیره و منابع شبکه را برای برنامه‌های کاربردی MEC فراهم می‌سازد. صفحه داده ترافیک را در بین خدمات، برنامه‌های کاربردی MEC ، DNS Proxy/Server و شبکه‌های دسترسی مختلف مسیریابی می‌کند.
MEC APP (۱-۳	خدمات MEC را ارائه می‌دهد. رویه‌های پشتیبانی مربوط به چرخه عمر برنامه کاربردی را اجرا می‌کند.
۲) مدیریت سطح-میزبان MEC :	
MEPM (۲-۱	چرخه عمر، قواعد و الزامات برنامه‌های کاربردی را مدیریت می‌کند. برای اجرای یک تصویر نرم‌افزاری ساختار مجازی‌سازی را آماده می‌کند. توابع مدیریتی را برای MEP فراهم می‌کند.
VIM (۲-۲	تخصیص و پایش منابع مجازی را مدیریت می‌کند. برای اجرای یک تصویر نرم‌افزاری ساختار مجازی‌سازی را آماده می‌کند. گزارش عملکرد و نقص را به MEPM ارسال می‌کند.
۳) مدیریت سطح-سیستم MEC :	
MEO (۳-۱	یک بررسی اجمالی از سیستم MEC کامل نگهداری می‌کند. بسته‌های برنامه کاربردی را قرار می‌دهد. برای نمونه‌سازی برنامه کاربردی MEC ، MEHهای مناسب را انتخاب می‌کند. نمونه‌سازی، خاتمه و محل مجدد برنامه کاربردی MEC را راه‌اندازی می‌کند.
OSS (۳-۲	برای نمونه‌سازی و خاتمه برنامه‌های کاربردی درمورد اعطای درخواست، تصمیم می‌گیرد.
User app (۳-۳ LCM Proxy	به برنامه‌های کاربردی تجهیز برای درخواست قراردادن، نمونه‌سازی و خاتمه برنامه‌های کاربردی کاربر اجازه می‌دهد. به برنامه‌های کاربردی تجهیز درباره وضعیت برنامه‌های کاربردی کاربر اطلاع‌رسانی می‌کند.
MEC Federation (۳-٤ MEF	اطلاعات سیستم MEC که توسط یک MEO ارسال می‌شود را ثبت می‌کند. سیستم‌های MEC را کشف می‌کند.

۴) آسیب پذیری‌ها و تهدیدات امنیتی MEC

در ملاحظات امنیتی MEC، چند حوزه آسیب‌پذیری شناسایی شده‌اند که در این بخش آنها را با جزئیات مورد بررسی قرار می‌دهیم.

۴-۱) اهمیت امنیت MEC

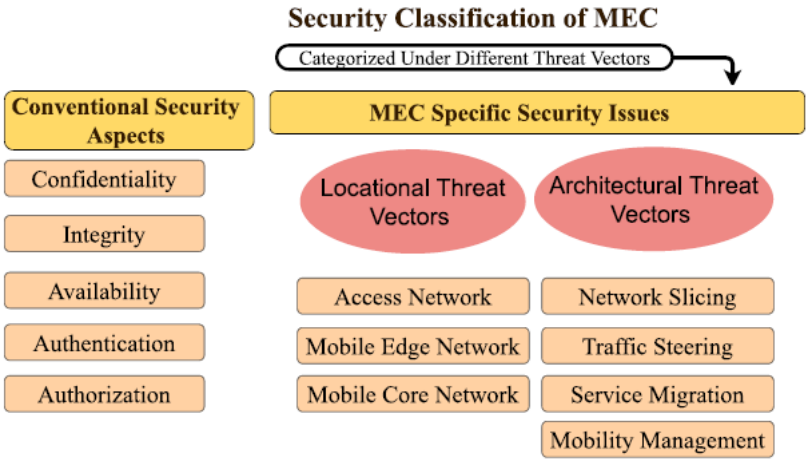
لبه شبکه تلفن همراه، نقطه دسترسی به تمام خدماتی است که در RAN منتشر می‌شود. استقرار منابع محاسباتی ابر در لبه شبکه، در مراکز داده یا اتاق‌های داده با کنترل فیزیکی و حفاظت بسیار کمتری نسبت به مراکز داده مرکزی، منابع محاسباتی

مهم را درمعرض تهدیدات امنیتی فیزیکی قرار می‌دهد که می‌تواند باعث به‌خطر افتادن خدمت یا دسترسی به منابع مرکزی شود [۳]. اکثر این تجهیزات در برابر همسانه‌سازی و دستکاری فیزیکی آسیب‌پذیر هستند و کل شبکه تلفن همراه را درمعرض حملات بی‌شماری قرار می‌دهند. بررسی اعتبار این تجهیزات در لبه یک نگرانی جدی است.

٤-٢) دسته‌بندی امنیت MEC

ازآنجاییکه امنیت مفهوم گسترده‌ای است، یک طبقه‌بندی مناسب برای جنبه‌های امنیتی مختلف که در MEC حادث می‌شود موردنیاز است. در اینجا، امنیت عمدتا تحت جنبه‌های امنیتی مرسوم و مسائل امنیتی خاص MEC، طبقه‌بندی می‌شود (مطابق شکل ۴). امنیت تحت جنبه‌های امنیتی مرسوم یا کلاسیک، جنبه‌های محرمانگی، یکپارچگی، دردسترس‌بودن، احراز هویت و اجازه دسترسی درنظر گرفته می‌شوند (بخش ۴-۳). مسائل امنیتی خاص MEC نیز براساس کاربرد تهدید آنها استنتاج شده‌است (بخش ۴-۴).

بردارهای تهدید[۴۴] (TVs) برای شناسایی آسیب‌پذیری‌ها/روندهای مرتبط با استقرار MEC تشکیل شده‌اند. این TVها برای وضوح بهتر به جنبه‌های مکانی، معماری و سایر جنبه‌های دیگر دسته‌بندی می‌شوند.



شکل ٤ . دسته‌بندی امنیت MEC

٤-٣) جنبه‌های امنیتی مرسوم MEC

این بخش، جنبه‌های امنیتی کلاسیک استقرار MEC را بیان می‌کند. این جنبه‌ها را می‌توان به‌عنوان الزاماتی برای بهبود امکان‌پذیری راه‌اندازی MEC درنظر گرفت.

الف) محرمانگی

محرمانگی، عمل جلوگیری از خواندن یا دسترسی اشخاص غیرمجاز به مطالب حساس است. تکامل شبکه‌های تلفن همراه از GSM تا LTE از الگوریتم‌های رمزگذاری A5/2 تا الگوریتم رمزگذاری EEA استفاده می‌کنند. بااین‌حال، برای RAN مبتنی بر 5G و فراتر از آن، پروتکل‌های ارتباطی باید مطابق با موارد استفاده و برنامه‌های کاربردی درحال‌استفاده، سفارشی شوند. انتقال اطلاعات در زیرساخت لبه و به سمت شبکه هسته باید با سطح قابل‌توجهی از امنیت رمزگذاری شود.

44 Thereat vectors

افشای ناموجه اطلاعات در این سطح، از طریق وضعیت‌های سیستم بی‌حفاظ گذاشته شده و نخستینه‌های رمزنگارانه، آسیب بیشتری به سیستم MEC نسبت به شبکه AN تلفن همراه وارد می‌کند. تجهیزات IoT مبتنی بر 3GPP با سطوح تهدید مشابهی با UEهای تلفن همراه مواجه هستند. بااین‌حال، دامنه تهدید آنها به‌دلیل کمبود منابع و ناتوانی در راه‌اندازی اقدامات امنیتی کافی، از تجهیز UE معمولی فراتر می‌رود.

ب) یکپارچگی

دستکاری و تخریب داده‌ها برای گمراه‌کردن طرف‌های یک ارتباط، نقض یکپارچگی است. همانند محرمانگی، یکپارچگی مفهومی است که بطور گسترده برای شبکه‌های تلفن همراه مورد توجه قرار گرفته‌است. سکوی لبه MEC مجازی‌شده، به اطلاعات کنترلی که از طریق کانال‌های بازخورد برای بهینه‌سازی عملیات موجودیت‌های مجازی منتقل می‌شود، متکی است. بنابراین یکپارچگی نقش کلیدی در زمینه MEC ایفا می‌کند زیرا این خدمات، خودکار هستند و خدمات مستقل برای عملکرد موثر به اطلاعات دقیق نیاز دارند. در شبکه‌های تلفن همراه، یکپارچگی از طریق حملات مداخله‌جویانه مانند تلاش‌های مرد در میان[۴۵] (MitM) یا رله[۴۶] که برای دستکاری یا سوءاستفاده از محتوای انتقال‌یافته به/از شبکه هسته انجام می‌شود، نقض می‌شود. در MEC برخلاف یک شبکه تلفن همراه معمولی، کانال‌های اضافی درمعرض مهاجم قرار می‌گیرند. پیوندهای ایجادشده بین سطح لبه MEC، سطح سیستم MEC و شبکه هسته تلفن همراه، بردارهای تهدید بیشتری را برای نقض یکپارچگی اضافه می‌کند. در این بین، تزریق کدهای مخرب[۴۷] به یک جریان اطلاعات قانونی می‌تواند بیشترین تخریب را برای سکوی لبه ایجاد کند [۱۲].

ج) دسترسی‌پذیری

دردسترس‌بودن، وجود همه‌جانبه منابع MEC برای مصرف‌کنندگانی است که مایل به اشتراک خدمات هستند. این عامل در درجه اول به عملکرد شبکه و اثربخشی رابط‌های شبکه بستگی دارد. بنابراین عملکرد شبکه تلفن همراه برای MECبسیار مهم است. حملات همسایه DoS [۴۸] که خدمت‌ها را مختل می‌کنند، دلیل اصلی اختلالات دسترسی در کانال‌های ارتباطی هستند. در شبکه LTE موجود، وضعیت اتصال کنترل منابع رادیویی (RRC) مشکلاتی را با اعتبارسنجی eNodeB برای UE ایجاد می‌کند [۱۳]. بنابراین فرصت‌هایی برای حملات DoS ایجاد می‌کند و دردسترس‌بودن eNodeBs را به خطر می‌اندازد.

د) احراز هویت

احراز هویت، فرآیند تایید هویت طرفین درگیر در ارتباط یا دسترسی به منابع است. این سازوکارها یا توسط یک طرف واحد انجام می‌شود یا بطور متقابل از طریق یک سناریوی گسترده انجام می‌گردد. طرح‌های احراز هویت از معیارهای مختلف اصالت برای اعتبارسنجی موجودیت‌ها استفاده می‌کنند. کلیدها، ابزار عمومی هستند که برای احراز هویت موجودیت‌های غیرانسانی استفاده می‌شوند. بسته به حوزه‌ای که احراز هویت در آن انجام می‌شود، سازوکارها به‌عنوان

45 Man-in-the-Middle

46 Relay

۴۷ Malicious code injection، قطعه کد یک عامل مخرب به یک عامل فعال یا یک محتوای اجرایی درحال‌انتقال تزریق می‌شود. چنین حملاتی با سناریوهای مهاجرت خدمت در MEC قریب‌الوقوع هستند.

48 DoS-adjacent attacks

احراز هویت اولیه یا ثانویه طبقه‌بندی می‌شوند. احراز هویت برای UEهای مبتنی بر MEC از طریق رابط هوایی RAN ، عمدتا به‌عنوان یک رویکرد اولیه انجام می‌شود. بنابراین تجهیزات و خدمات ناهمگون IoT نیازمند احراز هویت متنوعی هستند. حفاظت UE را می‌توان از طریق بهبود سازوکارهای احراز هویت و توافق کلید[۴۹] (AKA) که توسط LTE استفاده می‌شود، به‌دست آورد [۱۳]. علاوه‌براین، AKA مبتنی بر 5G و پروتکل احراز هویت توسعه‌یافته AKA دو طرح احراز هویت اجباری هستند که در فاز اول 5GPP پیشنهاد شده‌اند [۱۴].

هـ) اجازه دسترسی

اجازه دسترسی، عملکرد تضمین دسترسی به موجودیت‌های احراز هویت‌شده و طبقه‌بندی‌شده در سطوح قابلیت‌های مختلف است. بسته به نوع خدمتی که UE درخواست می‌کند، OSS سطح قابلیت برنامه کاربردی لبه تلفن همـــــراه[۵۰] (ME App) مشخص‌شده در سطح لبه را تایید می‌کند. اکثر نقض‌های اجازه دسترسی به‌عنوان یک نقض احراز هویت شناخته می‌شوند.

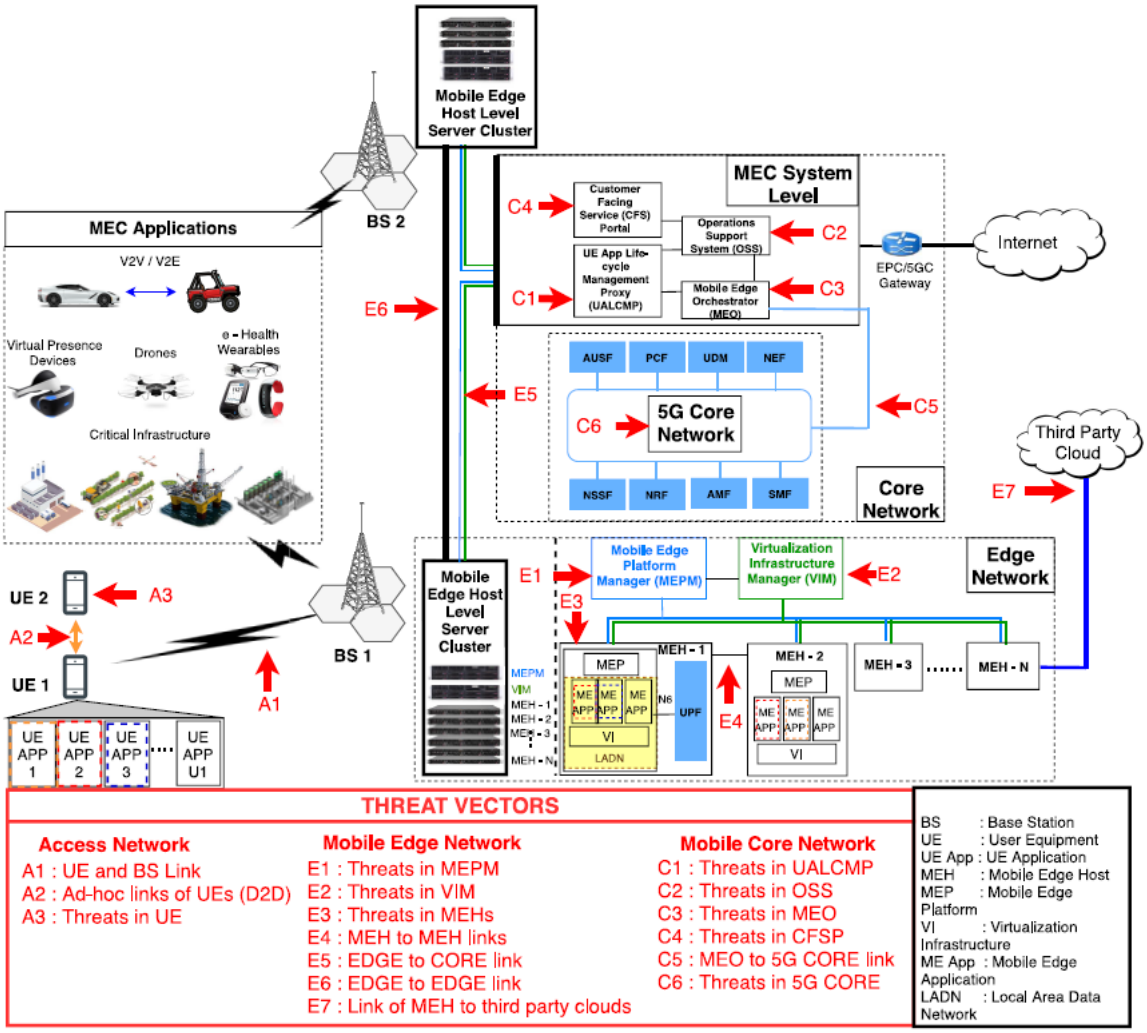
٤-٤) جنبه‌های امنیتی خاص MEC

در این بخش، بردارهای تهدید (TVها) را که در سناریوی استقرار MEC درنظر گرفته شده، در انطباق با معماری استاندارد ETSI ارائه می‌کنیم. شکل ۵، محل TVهای اعمال‌شده در سطوح مختلف در ساختار MEC را نشان می‌دهد. آنها براساس حوزه نفوذشان به سه حوزه: شبکه دسترسی، شبکه لبه تلفن همراه و شبکه هسته طبقه‌بندی می‌شوند. علاوه‌براین، TVهایی که محل خاصی ندارند، بیشتر به‌عنوان TVهای معماری و سایر TVها برای درک کاربرد آنها طبقه‌بندی می‌شوند.

۴-۴-۱) بردارهای تهدید مرتبط با شبکه دسترسی

در هر سیستم ارتباطی، تهدیدها بیشتر از شبکه دسترسی (RAN) سرچشمه می‌گیرند. دلیل اصلی این تهدیدها، فناوری‌های متنوعی است که در RAN مستقر شده‌اند. ما TVهای مرتبط با RAN را به سه دسته کلی طبقه‌بندی کرده‌ایم که در بخش‌های فرعی A1 ، A2 و A3 زیر توضیح داده شده‌اند.

49 5G Authentication and Key Agreement
50 Mobile Edge Application



شکل ۵. بردارهای تهدید استقرار MEC نوعی از نظر موقعیت مکانی

۱) A1 (پیوند بین تجهیزات کاربر و ایستگاه پایه):

اتصال UE به ایستگاه پایه (BS)، معمولی‌ترین پیوند ارتباطی موجود و آسیب‌پذیرترین پیوند در برابر تهدیدات، در یک سیستم ارتباطی سیار است. ازآنجاییکه تهدید A1 به مشخص‌ترین بخش شبکه ارتباطی سیار اعمال می‌شود، یک مهاجم می‌تواند مداخله کند یا تجهیز مخربی را برای به‌خطرانداختن BS معرفی کند. فناوری‌های جدید مانند MIMO، گیرنده‌های آگاه از تداخل، کدگذاری/مدولاسیون پیشرفته، موج میلی‌متری (mmWave)، بارگذاری Wi-Fi، LTE و دسترسی اشتراک‌گذاری‌شده با مجوز[۵۱] (LSA) به‌منظور بهبود بازدهی طیفی در شبکه دسترسی معرفی شده‌است. اتصال UE از طریق این فناوری‌های ناهمگون، نگرانی‌هایی را درمورد عوامل سازگاری و قابلیت‌همکاری ایجاد می‌کند که می‌تواند توسط مهاجمان قابل‌بهره‌برداری باشد.

آسیب‌پذیری‌ها: ماهیت پخش رابط هوایی بدون سیم که UE را به BS پیوند می‌دهد، مستعد حملاتی است. مانند:

51 Licensed Shared Access

۱. شنود و سرقت[۵۲]
۲. اختلال و انکار خدمت (DoS)
۳. تزریق گره مخرب

۲) A2 (اتصال Ad-hoc بین تجهیزات کاربر):

تهدیدات در A2 با پیوندهایی که بین UEها در مُد Ad-hoc ایجاد می‌شوند، مرتبط هستند. این پیوندها از کانال‌های ارتباطی کوتاه‌بُردی استفاده می‌کنند که تحت تاثیر UE apps خاص برای انتقال داده استفاده می‌شوند. نوع اتصال دستگاه به دستگاه، (D2D) است که بدون نیاز به هیچ BS ای برای اتصال، یک پیوند ارتباطی مستقیم بین دو تجهیز برقرار می‌شود [۱۵]. فناوری‌های ارتباطی کوتاه‌بُرد عبارتنداز: بلوتوث، بلوتوث کم‌انرژی[۵۳] (BLE)، ارتباط حوزه نزدیک[۵۴] (NFC)، ZigBee، Wi-Fi مستقیم، اینترنت اشیا باند باریک (NB-IoT)، SIGFOX یا هر فناوری که می‌تواند یک شبکه Ad-hoc تلفن همراه[۵۵] (MANET) را که قادر به استقرار اتصالات بین UEها هستند، تشکیل دهد [۱] ، [۱۲] و [۱۶].

آسیب‌پذیری‌ها: آسیب‌پذیری‌های این TV به کانال ارتباطی ایجادشده بین UEها محدود می‌شود. تهدیدات ناشی از UE مستقیما بر نفوذ به سیستم‌های MEC در این TV تاثیر نمی‌گذارد. یک UE مورد نفوذ قرارگرفته توسط یک حمله مبتنی بر D2D می‌تواند از اتصال خود با BS برای آلوده‌کردن خدمت‌رسان‌های MEC جهت دستکاری‌های مختلف MEHاستفاده کند. در این راستا، حملات متعددی به فناوری‌های ارتباطی کوتاه‌برد مانند: شنود، جعل هویت[۵۶]، جعل[57]، سواری رایگان[۵۸]، DoS و نقض حریم خصوصی محتمل است [۱۵]. بیشتر این حملات به‌دلیل ماهیت پروتکل‌های ارتباطی تعبیه‌شده در فناوری‌های ارتباطی کوتاه‌بُرد امکان‌پذیر هستند. این فناوری‌ها بجای استفاده از اقدامات امنیتی، استفاده از پهنای باند را برای D2D در اولویت قرار می‌دهند.

۳) A3 (تجهیز UE):

تجهیز UE می‌تواند یک تلفن همراه، رایانه شخصی، دوربین مدار بسته، حسگر پوشیدنی یا سیستم حسی باشد که می‌تواند در تماس مستقیم با BS باشد یا از طریق یک تجهیز دروازه به BS متصل شود. انواع فناوری‌های نسبت داده‌شده بـه UE در جنبه‌های سیستم عامل (اندروید، iOS، ویندوز، WebOS و غیره)، مدیریت حافظه (SD ، micro-SD و HDD)، ارتباطات (RF، RFID، NFC، بلوتوث، وای‌فای و اترنت)، طراحی فیزیکی و ساختار، به استقرار غیرمحتمل یک راهکار امنیتی عمومی برای UEها در حد جامع کمک می‌کند. UE حاوی اطلاعات مربوط به جنبه‌های مختلف زندگی روزمره یک فرد مانند: اطلاعات خصوصی (عکس‌ها، گزارش‌های پزشکی، آمار پزشکی و فیلم‌های دوربین‌های مداربسته)، موقعیت مکانی (GPS)، روال‌های روزمره (خرید و حمل‌ونقل)، اطلاعات سازمانی، اطلاعات زیرساخت‌های حیاتی (مصرف انرژی، وضعیت مالی، بانکی و خدمات اضطراری) و آمار حساب برخط می‌باشد که در آن افشای چنین

52 Eavesdropping and Hijacking
53 Bluetooth Low Energy
54 Near Field Communication
55 Mobile Ad hoc Network
56 Impersonation
57 forging
58 Free-riding

گواهینامه‌ها و پارامترهایی می‌تواند برای فرد، آسیب‌زا باشد [۱۶]. بنابراین تهدیدات برای حریم خصوصی کاربران تلفن همراه یک نگرانی بزرگ است. منابع تعبیه‌شده در یک UE از نظر توان پردازش، ظرفیت ذخیره‌سازی و عمر باتری مهمترین عوامل برای این بردار تهدید هستند [۱۷].

آسیب‌پذیری‌ها: تهدیدها می‌توانند توسط یک UE، با اطلاع کاربر یا بدون اطلاع کاربر پیاده شوند. حتی یک کاربر قادر است یک عامل نرم‌افزار مخرب را بطور ناخواسته فعال کند. خطر آسیب‌پذیربودن UEها در برابر حملات فیزیکی و از راه دور، این بردار تهدید را بسیار حیاتی می‌کند. UEها در برابر آسیب فیزیکی، حملات کانال جانبی[۵۹] (SCA)، تزریق کد مخرب و تروجان‌های سخت‌افزاری، آسیب‌پذیر هستند درحالیکه سایر حملات توضیح داده‌شده در A1 و A2، برای رابط‌های ارتباطی قابل‌اعمال هستند.

۴-۴-۲) بردارهای تهدید مرتبط با شبکه لبه تلفن همراه (MEN)

در این بخش، موجودیت‌های واقع در شبکه لبه یا سطح میزبان MEC مانند: مدیر سکوی لبه تلفن همراه[۶۰] (MEPM)، مدیر زیرساخت مجازی‌سازی[۶۱] (VIM) و میزبان لبه تلفن همراه[۶۲] (MEH)، برای ایجاد محدوده‌های تهدید مورد بررسی قرار می‌گیرند. محل قرارگیری خدمت‌رسان‌های MEC در مقایسه با مراکز داده معمولی، بومی‌سازی شده‌است. بنابراین سطح لبه MEC (یعنی میزبان) مستعد حملات امنیتی ملموس یا فیزیکی است.

۱) E1 (مدیر سکوی لبه تلفن همراه (MEPM)):

MEPM موجودیتی است که فعالیت‌های MEH را با استفاده از اتصالی که با سکوی لبه تلفن همراه (MEP) دارد، نظارت می‌کند. این موجودیت توابع نظارتی و تخصیص منابع را با اتصالاتی که با VIM، MEO و OSS حفظ می‌کند، انجام می‌دهد.

آسیب‌پذیری‌ها: قراردادن موجودیت‌های MEN در لبه، بردارهای حمله مبتنی بر دستکاری فیزیکی را محدود می‌کند. بااین‌حال، خطر در مقایسه با CC مرسوم بالاتر است. این آسیب‌پذیری‌ها عبارتنداز:

۱. تغذیه داده‌های جعلی پیکربندی/بازخورد
۲. آلوده‌شدن از طریق ME Apps و UE Apps
۳. حملات مبتنی بر VM

۲) E2 (مدیر زیرساخت مجازی (VIM)):

VIM وظیفه کامل تسهیل‌سازی ME Apps منابع زیرساخت مجازی‌شده را در هر MEH از طریق یک مجاورت لبه منفرد اجرا می‌کند. اتصالات VIM به MEO و MEPM آمار را برای انجام وظایف مدیریت و نظارت بر LADN مستقر در MEHها تغذیه می‌کند. ازآنجاییکه این موجودیت، اصلی است که برای تسهیل منابع مجازی در لبه تخصیص داده

---

59 Side Channel Attacks، یک حمله تحلیل-رمز مانند تحلیل رمز آکوستیک است و برای تعیین اعتبارنامه‌های امن در یک شیوه‌نامه انجام می‌شود. SCAها در یک محیط لبه بی‌حفاظ گذاشته‌شده، درمعرض MEHها و UE هستند.

60 Mobile Edge Platform Manager

61 Virtualization Infrastructure Manager

62 Mobile Edge Hosts

می‌شود، نقش VIM شبیه به یک هایپروایزر برای MEHها است. بنابراین VIM وظایف تخصیص، مدیریت، انتشار و نظارت بر عملکرد منابع مجازی را انجام می‌دهد [۱۸].

آسیب‌پذیری‌ها: عملکرد هایپروایزر VIM، مهاجمانی را جذب می‌کند که قصدشان دستکاری قابلیت‌های تخصیص منابع با هدف کاهش منابع است. این آسیب‌پذیری‌ها عبارتنداز:

۱. حملات مبتنی بر VIM
۲. گمراه‌کردن موجودیت‌های سطح سیستم

۳) E3 (میزبان لبه تلفن همراه (MEH))

MEH موجودیت عملکردی اصلی در سطح میزبان است که عملیات محاسباتی، ذخیره‌سازی یا شبکه را در MEC انجام می‌دهد. یک MEH از یک MEP، زیرساخت مجازی‌سازی (VI) و یک صفحه داده یا LADN تشکیل شده‌است که اتصال محلی را بین ME Apps حفظ می‌کند. علاوه‌براین، تابع صفحه کاربر (UPF) یک موجودیت شبکه دسترسی 5G است که در داخل MEH برای ادغام شبکه هسته 5G در LADN گنجانده شده‌است. ازآنجاییکه MEH تنها موجودیتی است که محتوای انتقال‌یافته از UE Apps را ذخیره می‌کند، خطر سوءاستفاده زیاد است.

آسیب‌پذیری‌ها: MEHها هدف اصلی هر حمله‌ای هستند که از AN به سمت سیستم MEC سرچشمه می‌گیرد. ازآنجاییکه آنها عناصر عملکردی اصلی هستند که از پردازش، ذخیره‌سازی و محاسبات خدمت پشتیبانی می‌کنند، هرگونه تلاش برای نفوذ به سیستم MEC از طریق یک اقدام مخرب، باید از دیدگاه مهاجمان به سمت MEH هدایت شود.

٤) E4 (اتصال بین میزبان‌های لبه تلفن همراه)

ME Apps ممکن است برای پردازش برنامه‌های پیشرفته نیاز به اتصال با یک یا چند MEH داشته باشند که در آن یک MEH منابع لازم برای انجام عملکرد موردنظر را ندارد. این امر مستلزم اتصال بین ME Appها است که تحت MEH کار می‌کنند و از طریق MEP ایجاد می‌شوند. این برای برنامه‌های کاربردی پیشرفته مانند اینترنت اشیای صنعتی، نظارت یا خدمات زیرساخت حیاتی محتمل است. به محض اینکه به دو موجودیت MEH یعنی VI و LADN دسترسی پیدا شد، VIM و UPF مربوطه باید علاوه بر اشتراک‌های موجود در MEPM مطلع شوند.

آسیب‌پذیری‌ها: یک ME App مخرب که از روش‌های تحت E3 پدیدار شده‌است، می‌تواند سایر ME Appهای متصل و عناصر MEP را علاوه بر موجودیت‌های داخل یک MEH آلوده کند. بااین‌حال، ارتباطات بین MEHها داخلی است و برای مهاجمان پنهان است. بنابراین حملات از نوع MitM، غیرمحتمل است. تزریق‌های مخرب و ME Apps جعلی از تهدیدات این بخش هستند.

۵) E5 (اتصال سکوی MEC بین لبه و هسته):

ارتباط دوطرفه بین موجودیت‌های سطح سیستم لبه تلفن همراه و موجودیت‌های سطح میزبان، یک پیوند مهم در MEC است. ازآنجاییکه این دو سطح توسط مکان از هم جدا می‌شوند، اتصال می‌تواند از طریق پیوندهای ارتباطی دوربُرد با استفاده از فناوری‌هایی مانند مایکروویو (MW)، فیبر نوری (FO)، ماهواره یا RF ایجاد شود. فرآیند ثبت‌نام برای یک MES خاص درخواست‌شده توسط یک UE App از طریق این پیوند ایجاد می‌شود [۱۸].

UEهایی که به یک سیستم MEC متصل می‌شوند، ابتدا باید در OSS از طریق اتصال گسترش‌یافته از BS به موجودیت UALCMP در هسته ثبت‌نام کنند. این رابط اولیه UE Apps با سکوی MEC است. ماهیت UE App (خواه توسط یک موجودیت مورد اعتماد یا مخرب اداره شود)، اعتبار و محتوای منتقل‌شده از UE App به ME App، عواملی هستند که باید در این بردار تهدید بررسی شوند.

آسیب‌پذیری‌ها: یک مهاجم می‌تواند در این پیوند ارتباطی مداخله کند. حتی اگر امکان مداخله با پیوندهای ارتباطی دوربُرد کمتر است، قرارگرفتن درمعرض اطلاعات کنترلی می‌تواند به مهاجم این فرصت را بدهد که از موجودیت‌های سطح میزبان MEPM ، VIM و MEH به دلخواه سوءاستفاده کند. بطور مشابه، اگر مهاجم موفق به تغییر پارامترهای به‌روزرسانی وضعیت منتقل‌شده از سطح میزبان به سطح سیستم شود، MEO و OSS ممکن است درمعرض حملات قطع خدمت قرار گیرند. حملات این بخش عبارتنداز: حمله به کانال‌های رادیویی، حملات به پیوندهای MW، حمله به اتصالات FO و حمله به پیوندهای ماهواره‌ای.

٦) E6 (اتصال بین Mobile Edge Apps که تحت میزبان‌های Mobile Edge در ایستگاه‌های پایه مختلف کار می‌کنند):

در این سناریو، برنامه کاربردی کاربر (UE App) به برنامه‌های کاربردی ME Apps که تحت مدیریت میزبان‌های MEHs قرار دارند و در دو ایستگاه پایه (BS) مجزا مستقر هستند، دسترسی پیدا می‌کند. این ایستگاه‌های پایه تحت کنترل یک واحد ارکستریشن (MEO) در سطح سیستمی MEC مدیریت می‌شوند. یک برنامه کاربردی جمع‌سپاری یا یک برنامه شبکه هوشمند که دو نمونه از یک ME App را در مکان‌های مختلف اجرا می‌کند، نمونه‌ای از چنین سناریویی است. حتی زمانیکه نمونه‌های ME App در سطوح لبه با پراکندگی جغرافیایی کار می‌کنند، توسط یک حوزه اعتماد منحصربه‌فرد که توسط یک OSS و یک MEO ساخته شده‌است، اداره می‌شوند.

آسیب‌پذیری‌ها: اتصال بین دو سطح میزبان که توسط یک سطح سیستم کنترل می‌شود، می‌تواند مستعد حملات مداخله‌ای باشد همانطوریکه در E5 توضیح داده شده‌است. این حملات درونی قادر به نفوذ به هر دو سطح میزبان MEC هستند.

۷) E7 (اتصال با میزبان لبه تلفن همراه و خدمت‌رسان‌های ابری):

درمورد خدماتی که توسط مصرف‌کنندگان شخص ثالث میزبانی می‌شوند، MEH به‌عنوان یک پیاده‌سازی ابری انبوه مبتنی بر اینترنت اشیا، اتصال به یک ابر متمرکز یا یک سکوی خدمت‌رسان را حفظ می‌کند. در آن سناریو، MEH یا (MEHها) محتوایی را که دراختیار دارد، قبل از انتقال آنها به خدمت ابری، پیش‌پردازش می‌کند. بطور معمول خدمت ابری، خدمات لبه را به‌صورت یک تابع و به‌عنوان یک خدمت[۶۳] (FaaS) میزبانی می‌کند که از طریق یک برنامه کاربردی MEC پوشش ابری پیاده‌سازی شده‌است [۱۹]. اتصال به خدمت‌رسان ابری از طریق LAND موجودیت MEH ایجاد می‌شود.

63 Function as a Service

آسیب‌پذیری‌ها: خط‌مشی‌ها و قوانین امنیتی اتخاذشده برای این نوع کانال، منطقه‌ای است که به‌ندرت مورد بررسی قرار گرفته‌است. فراهم‌کننده‌های خدمت ابری (CSPها) در برابر چنین بردارهای حمله‌ای، حساس هستند. بنابراین مسائل مربوط به قابلیت‌همکاری، ممکن است محتمل باشد. دراینجا حملات مداخله‌گرانه مانند حملات MitM، رله یا حملات جعل هویت برای کانال ارتباطی که از MEH به سکوی ابری گسترش می‌یابد، محتمل هستند. حملات پنهانی که توسط مهاجمان انجام می‌شود تا به‌عنوان یک خدمت ابری ظاهر شوند، می‌توانند حملات فروچاله[۶۴] یا کرم‌چاله[۶۵] را انجام دهند. حملات بویش بسته‌ها[۶۶] و تزریقات مخرب نیز از دیگر تهدیدات هستند.

۴-۴-۳) بردارهای تهدید مرتبط با شبکه هسته

شبکه هسته از تجهیزات سطح سیستم MEC مانند UALCMP، CFSP، سیستم پشتیبانی عملیات (OSS) و MEO به شبکه بک‌هال توسعه می‌یابد که با اتصال به اینترنت گسترش می‌یابد.

۱) C1 (UALCMP):

این موجودیت، نقطه تماس اولیه برای هر UE App است که قصد اشتراک در خدمات MEC را دارد. عملکرد اصلی UALCMP رسیدگی به چندین درخواست UE App در حین تعیین چرخه عمر آنهاست. ازآنجاییکه این موجودیت دارای عملکرد پراکسی است، عملکرد آدرس‌دهی داخلی برای سیستم MEC تسهیل می‌شود تا UE Apps را به ME App متناظر خود یا ME APPs که در MEN کار می‌کنند، مرتبط کند.

آسیب‌پذیری‌ها: حملاتی که بر روی UALCMP انجام می‌شود، در رابط‌های دسترسی آن برای بارگذاری بیش‌ازحد هدف قرار می‌گیرند و عبارتنداز: بردارهای حمله در رابط دسترسی مانند حملات DoS، DDoS یا حمله با تغییر قیافه، دستکاری چرخه عمر Appها و ایجاد پیامدهایی برای OSS.

۲) C2 (سیستم پشتیبانی از عملیات OSS):

OSS، درخواست‌های خدمت ارسال‌شده از طریق پورتال UALCMP یا CFSP را درحالیکه توابع ME App را نمونه‌سازی یا خاتمه می‌دهد، اعطا می‌کند. OSS، پیوندهایی را جهت استخراج اطلاعات کنترل، به MEPM و MEO برقرار می‌کند. OSS، مجوز استفاده از ME Apps را که برای یک خدمت خاص MEC پیکربندی شده‌اند، به مشترکین اعطا می‌کند. لذا این موجودیت برای مهاجمان جهت دسترسی به MEC حیاتی است.

آسیب‌پذیری‌ها: ازآنجاییکه سطح میزبان MEC به تاییدیه برای تحریک MESهای OSS وابسته است، قصد مهاجمان، به‌تاخیرانداختن عملیات آن از طریق UALCMP است. حملات DoS یا DDoS و تغذیه اطلاعات نادرست در فرآیند ثبت، از حملات و آسیب‌پذیری‌ها هستند.

۳) C3 (ارکستراتور لبه تلفن همراه):

MEO، عملکرد هسته مفهوم MEC را نشان می‌دهد که نقش هایپروایزر را برای سیستم جامع MEC اختصاص می‌دهد. آن میزبان‌های MEC مستقر شده و وضعیت استفاده از منابع را در لبه مشاهده می‌کند. به‌عنوان هایپروایزر، MEO

64 Sinkhole
65 Wormhole
66 Packet sniffing attacks

بر ماشین‌های مجازی و سخت‌افزارهای زیرین که برای مجازی‌سازی پیکربندی شده‌اند، نظارت می‌کند [۲۰]. توابع اصلی MEO عبارتنداز: انتقال خدمات، مدیریت تحرک و نظارت بر هدایت ترافیک. نقش MEO هنوز برای سناریوهایی که سیستم MEC با سایر فناوری‌ها مانند زیرساخت NFV (NFVI) با قابلیت NFV Orchestration (NFVO) ادغام می‌شود، قابل اجرا است.

آسیب‌پذیری‌ها: در سناریویی که MEO به‌عنوان هایپروایزر درمعرض خطر قرار می‌گیرد، بهره‌برداری‌های پیکربندی خودکار شبکه، بهره‌برداری‌های ارکستراسیون، پیکربندی نادرست مخرب و بهره‌برداری‌های کنترل‌کننده SDN، محتمل هستند [۲۰]. پارامترهای پیکربندی ارسال‌شده از موجودیت‌هایی مانند MEPM، OSS، UALCMP و VI نیز برای استفاده از MEO حیاتی هستند. بنابراین باید سازوکارهایی برای شناسایی اینگونه حملات و رفع آنها بکار گرفته شود. حملات دستکاری منابع و نیز حملات عیب‌یابی گزارش امنیتی در اینجا مطرح است.

٤) C4 (CFSP):

CFSP، دسترسی ME Apps به خدمات شخص ثالث را زمانیکه قادر به فراخوانی اطلاعات سطح خدمت از چنین برنامه‌های کاربردی است، تسهیل می‌کند [۱۸]. نظارت بر پارک خودرو، وسایل نقلیه متصل و داده‌های بزرگ اینترنت اشیا، برنامه‌های کاربردی هستند که برای استقرار MEC مناسب هستند. این استقرارها از حسگرهایی استفاده می‌کنند که حجم انبوهی از داده‌ها را جمع‌آوری می‌کنند که در یک خدمت‌رسان لبه MEC پیش‌پردازش شده و برای تحلیل بیشتر به یک خدمت‌رسان مشارکتی متمرکز منتقل می‌شوند [۲۱].

آسیب‌پذیری‌ها: ازآنجاییکه نقش CFSP رسیدگی به درخواست‌هاست، می‌تواند مستعد حملات مبتنی بر خدمت مانند DoS و DDoS باشد. علاوه‌براین، سازوکارهای تایید مناسب باید توسط CFSP برای فعال‌کردن هدایت ترافیک برنامه‌های کاربردی شخص ثالث به موجودیت‌های سطح میزبان MEC استفاده شود. موارد استفاده قابل‌اعمال برای E7، نمونه‌هایی از خدمات توسعه‌یافته هستند که توسط CFSP برای برنامه‌های کاربردی شخص ثالث تایید شده‌اند. یک CFSP به‌خطرافتاده، می‌تواند اشتراک‌های خدمت OSS را دستکاری کند.

٥) C5 (قابلیت اتصال بین MEO و شبکه هسته 5G):

یک رابط امن باید برای MEO و شبکه هسته 5G تعریف شود. سیگنال‌های کنترلی از طریق این رابط بین شبکه هسته 5G و MEO ردوبدل می‌شود. ازآنجاییکه این رابط، اصلی است که با شبکه هسته 5G در تعامل می‌باشد، این یکی از رابط‌های مهم در کل معماری MEC است. میزبانی‌کردن عناصر شبکه هسته 5G و MEO در یک میزبان فیزیکی امکان‌پذیر است. بااین‌حال، پیاده‌سازی آنها در دو میزبان فیزیکی متفاوت، محتمل‌تر است. در این‌صورت، پیوند ارتباطی بین MEO و شبکه هسته 5G باید از طریق شبکه فیزیکی برقرار شود. این شبکه را می‌توان با استفاده از هر فناوری شبکه مانند بدون‌سیم، سیمی یا نوری پیاده‌سازی کرد. بسته به رسانه اتصال و مکان مستقرشده، این موجودیت‌ها با چالش‌های امنیتی متفاوتی مواجه خواهند شد.

آسیب‌پذیری‌ها: رابط بین MEO و هسته 5G هنوز تعریف نشده‌است. بااین‌حال، چندین تهدید امنیتی را می‌توان در رابطه با این رابط شناسایی کرد. مانند: حملات TCP/IP به کانالی که MEO و هسته 5G را به‌هم پیوند می‌دهد و نیز فقدان یک رابط استاندارد است.

٦) C6 (شبکه هسته 5G):

درنهایت شبکه هسته 5G، کل شبکه 5G را کنترل می‌کند. شبکه هسته 5G، قابلیت‌های MEC را برای خدمات انتخاب‌شده فعال می‌کند. علاوه‌براین، تمام سیگنال‌های کنترلی از طریق شبکه هسته 5G به سیستم MEC ارسال می‌شود. بنابراین شبکه هسته 5G عنصر حیاتی است که عملکرد صحیح کل سیستم MEC را تضمین می‌کند.

آسیب‌پذیری‌ها: ازآنجاییکه شبکه هسته 5G، موجودیت اصلی کنترل کل شبکه 5G است، هرگونه حمله به شبکه هسته 5G تاثیر قابل‌توجهی بر سیستم 5G MEC خواهد داشت. ماهیت هسته نرم‌افزاری‌شده آن را بسیار آسیب‌پذیر می‌کند.

۴-۴-۴) بردارهای تهدید مرتبط با معماری

این بردارهای تهدید، بردارهای آسیب‌پذیری را که می‌تواند در پیشرفت‌های معماری مرتبط با استقرار MEC وجود داشته باشد، توضیح می‌دهد.

۱) AR1 (برش شبکه-NS):

برش شبکه، تقسیم یک شبکه فیزیکی به چندین شبکه منطقی است که برای فعال‌کردن استفاده همزمان از یک شبکه فیزیکی منفرد در سطوح مختلف مجازی/منطقی می‌باشد و جهت برنامه‌های کاربردی ناهمگون اینترنت اشیا و کاهش هزینه‌های سرمایه‌ای و عملیاتی کاربرد دارد. بنابراین یک سکوی شبکه مبتنی بر تقاضای چابک و پویا را در بالای یک زیرساخت شبکه فیزیکی ایجاد می‌کند. طبق مدل ICN[۶۷] شبکه 5G، چارچوب NS دارای پنج صفحه عملکردی است: صفحه تجاری خدمت، صفحه ارکستراسیون/مدیریت خدمت، صفحه ارکستراتور جهانی IP/ICN، صفحه ارکستراسیون/مدیریت خدمت حوزه و صفحه زیرساخت. در مقایسه با سایر طرح‌های اشتراک‌گذاری منابع مانند اشتراک‌گذاری RAN، شبکه‌های هسته اختصاصی[۶۸] (DCNs) و DCN پیشرفته (eDCN)؛ NS، یک محدوده بیشتر، پشتیبانی مجازی‌سازی، پشتیبانی از ماژولارسازی عملکرد، اتصال سرتاسر و فنون جداسازی بهتر را ارائه می‌دهد. AR1، آسیب‌پذیری‌های مرتبط با فرآیندها و فنون NS را مورد بحث قرار می‌دهد.

آسیب‌پذیری‌ها و تهدیدات: بیشتر تهدیدات معطوف به برش شبکه از طریق آسیب‌پذیری‌های شبکه وجود دارد و شامل موارد زیر می‌باشند: عدم وجود طرح‌های احراز هویت متقابل بین موجودیت‌ها در برش‌های مختلف، ارتباط ناامن بین نمونه‌های برش شبکه[۶۹] (NSIs) و مدیران برش شبکه[۷۰] (NSMs)، ناسازگاری شیوه‌نامه‌ها و خط‌مشی‌های امنیتی متنوع در بخش‌های مختلف، سطوح امنیتی مختلف در برش‌های مختلف که می‌تواند به مهاجم اجازه دهد تا با دسترسی از یک برش امنیتی پایین‌تر منابع یک برش امن را تخلیه کند و الصاق UE به برش‌های متعدد که تمایل به آمیخته‌سازی روزنه‌های

67 Information Centric Networking
68 Dedicated Core Networks
69 Network Slice Instances
70 Network Slice Managers

اطلاعاتی را درصورت وجود یک UE App آلوده افزایش می‌دهد. در حمله به آسیب‌پذیری‌های برش، بردارهای حمله MitM، Tracing، DoS، DDoS و SCA رخ می‌دهد. مسائل اعتبارسنجی برش، حملات جعل هویت، پیچیدگی در NSها و ناسازگاری بین برش‌ها نیز از دیگر تهدیدات/آسیب‌پذیری‌ها هستند.

۲) AR2 (فرمان‌دادن ترافیک[71]):

فرمان ترافیک سکوی MEC توسط نقطه مرجع Mp2 منتقل می‌شود (اتصال بین MEP و صفحه‌داده VI در یک MEH). پیکربندی صفحه‌داده توسط سکوی MEC مدیریت می‌شود، جاییکه درخواست‌های هدایت ترافیک را به تابع کنترل خط‌مشی (PCF) منتقل می‌کند. PCF قوانین هدایت ترافیک مربوطه را به SMF می‌فرستد، جاییکه SMF نشست‌های مربوط به PDU را مدیریت می‌کند [۱۹]. علاوه‌براین، زنجیره عملکرد خدمت[72] (SFC)، فنی است که خط‌مشی هدایت ترافیک را با تطبیق ساختارهای SDN و NFV تسهیل می‌کند. SFC جعبه‌های میانی (MBboxes) یا توابع خدمت (SF) مانند دیوارهای آتش، موجودیت‌های بازرسی بسته عمیق[73] (DPI)، فهرست‌های کنترل دسترسی[74] (ACLs)، سیستم‌های تشخیص نفوذ/پیشگیری (IDS/IPS) یا ترجمه آدرس شبکه[75] (NAT) را تشکیل می‌دهد. ازآنجاییکه SDN و NFV زیرساخت MEC را برای اتصال سطح سیستم، سطح میزبان و شبکه دسترسی تشکیل می‌دهند، SFC یک فن هدایت ترافیک مناسب برای استقرار MEC است. این TV در حال بررسی نقص در قوانین هدایت ترافیک در موجودیت‌های شبکه هسته 5G، معماری MEC و موجودیت‌های شبکه واسطه است.

آسیب‌پذیری‌ها و تهدیدات: شبکه هسته 5G به‌دلیل نیاز به ارائه برنامه‌های کاربردی متنوع، چالش‌های معماری جدیدی را ارائه می‌دهد. بنابراین شبکه هسته به این خدمات، با موجودیت‌های یکپارچه در سطح لبه MEC پاسخ می‌دهد. الزام خط‌مشی‌های مربوط به هدایت ترافیک تلفن همراه در سطح لبه، یک الزام اصلی است. بنابراین آسیب‌پذیری‌های مربوط به این TVها بر روی موجودیت‌های شبکه 5G، SFC و سرآیندهای ترافیک متمرکز شده‌اند.

۳) AR3 (مهاجرت خدمت[76]):

فرآیند انتقال محتوای اجرایی پیکربندی‌شده، می‌تواند آسیب‌پذیری‌ها و نقص‌های بی‌سابقه‌ای را در محیط MEC آشکار کند. در یک انتقال خدمت مبتنی بر CC، خدمت‌هایی که در ابتدا در محیط‌های ابری میزبانی می‌شوند به خدمت‌رسان‌های لبه‌ای که نزدیک به تجهیزات تلفن همراه قرار دارند، منتقل می‌شوند. این امر تاخیر را کاهش داده و ظرفیت شبکه دسترسی را بهبود می‌بخشد.

آسیب‌پذیری‌ها و تهدیدات: مهاجرت خدمات به معنای انتقال کل یک سکوی قابل خدمت یا بخشی از آن به میزبان‌های لبه تلفن همراه است که در لبه کار می‌کنند. بااین‌حال، امنیت فرآیند مهاجرت به‌دلیل تنوع منابع مورداستفاده و دامنه خدمات، یک منطقه خاکستری است. فرآیند مهاجرت با خدمتی آغاز می‌شود که در یک MEH یا چند MEH عمل می‌کند. ماهیت غیراصولی اتصال مبتنی بر اینترنت در میان موجودیت‌های لبه MEC مسائل امنیتی را ایجاد می‌کند که به

71 Traffic Steering
72 Service Function Chaining
73 Deep Packet Inspection
74 Access Control Lists
75 Network Address Translation
76 Service Migration

VIM، UEها و کانال‌های عبور داده‌های مهاجرت گسترش می‌یابد [۲۲]. تزریق کد مخرب و حمله به عوامل تلفن همراه هنگام مهاجرت از حملات این بخش هستند.

٤) AR4 (مدیریت تحرک):

اصطلاح «تحرک» را می‌توان به‌عنوان حفظ اتصال یک UE در هنگام رومینگ، از یک منطقه تحت پوشش خاص و از یک BS خدمت‌رسان به دیگری جهت حفظ تداوم خدمات از طریق یک سازوکار hand-off توصیف کرد [۲۱]. پوشش یک BS می‌تواند از چندین BS ماکرو، BS سلول کوچک (SCBS)، نقاط دسترسی Wi-Fi (APs) تا استاندارد RAN BS متفاوت باشد. بنابراین نگرانی‌هایی درمورد امنیت با BS دارای ظرفیت‌های مختلف که مدل‌های مختلف پوشش و تحویل را ارائه می‌دهند، مطرح می‌شود.

آسیب‌پذیری‌ها: ماهیت ناهمگون پیکربندی‌ها، خط‌مشی‌های ارتباط کاربر–خدمت‌رسان و حوزه‌های اعتماد در میان مناطق یا سلول‌های مختلف پوشش، مسائل مرتبط با تحرک است که منجر به تداخل شدید و آلودگی سیگنال راهنما می‌شود. لذا این مسائل، عملکرد انتقال را کاهش داده و تاخیر ارائه خدمات را افزایش می‌دهد. تهدیدات دردسترس‌بودن، پیچیدگی در تحرک UE، حملات مبتنی بر VM، حملات جعل هویت و BSهای 5G با سطح امنیتی پایین، از حملات این بخش هستند.

۵) راهکارهای امنیتی

بعد از شناسایی بردارهای تهدید سیستم MEC، به بررسی راهکارهای امنیتی جهت این TVها مطابق با استانداردهای ETSI و سایر مراجع معتبر می‌پردازیم.

۵–۱) راهکارهای امنیتی مرتبط با تهدیدات شبکه دسترسی

- راهکارهای موجود مرتبط با تهدید A1: امنیت رابط هوایی که مثلث امنیتی CIA را تضمین می‌کند، به روش‌های ۱) استفاده از نخستینه‌های[۷۷] رمزنگارانه و اثربخشی آنها، ۲) راهکارهای شبکه دسترسی و ۳) راهکارهای موجود در سطح لایه فیزیکی دسته‌بندی می‌گردد.
- راهکارهای موجود مرتبط با تهدید A2: تضمین امنیت D2D عمدتا شامل احراز هویت است درحالیکه حملات مداخله‌گرانه را می‌توان از طریق یک مدل امنیتی لایه‌ای کاهش داد. در مدل امنیتی لایه‌ای، سازوکارهای امنیتی مختلفی در هر لایه به‌شرح زیر بکار گرفته می‌شود: ۱) لایه برنامه کاربردی: رمزگذاری مبتنی بر هویت، رمزنگاری منحنی بیضوی[۷۸]، مدیریت کلید گروهی، مدیریت کلید احتمالی و رمزگذاری مبتنی بر ویژگی خط‌مشی رمزگذاری (CP-ABE)، ۲) لایه شبکه: ارتباطات D2D امن چندپرش، تقسیم و بهم‌زدن داده‌ها مبتنی بر کدگذاری امن شبکه، مدل‌سازی اهداف مهاجم با استفاده از نظریه بازی، کنترل مسیریابی و مدیریت کلید گروهی مبتنی بر PKI، ۳) لایه MAC: چارچوب کنترل دسترسی چنداولویت برای حریم خصوصی مکان و هویت، ۴) لایه فیزیکی: استخراج

77 Primitive
78 Elliptic Curve Cryptography

کلید، طرح تخصیص منابع رادیویی مبتنی بر اطلاعات وضعیت کانال (CSI) و طرح کنترل‌کننده دسترسی توان توام مبتنی بر محرمانگی [۱۵].

- راهکارهای موجود مرتبط با تهدید A3: ازآنجاییکه حملات برای این TV، UE و کانال‌های ورودی/خروجی آن را هدف قرار می‌دهد، راهکارها بر روی شناسایی و اصلاح SCAها و بدافزارهای نفوذی به UE متمرکز هستند [۲۵]–[۲۳].

۵–۲) راهکارهای امنیتی مرسوم در MEC

موارد و راهکارهای مرسوم در این زمینه به شرح ذیل است:

۱) کاهش نقض‌های محرمانگی: طرح‌های رمزگذاری مبتنی بر تونل، IPSec یا TLS/SSL که سازگاری‌های مناسبی برای تضمین امنیت سرتاسر (E2E) دارند و نیز مقاومت کوانتومی[۷۹] یا روش‌های رمزنگاری ضد کوانتومی برای محدودکردن برتری مهاجمان با منابع فراوان.

۲) کاهش نقض‌های یکپارچگی: سازوکارهای احراز هویت و توافق کلید (5G-AKA) که سازوکارهای تضمین یکپارچگی را برای کانال‌های سیگنالینگ مدیریت می‌کند. در مقایسه با LTE ، 5G از یکپارچگی در سطح کاربر پشتیبانی می‌کند [۱۴]. برای تجهیزات اینترنت اشیا، طرح‌های رمزگذاری مبتنی بر درهم‌سازی و مبتنی بر کلید نشست می‌تواند برای اطمینان از یکپارچگی در سطح لایه فیزیکی استفاده شود.

۳) کاهش نقض‌های دسترسی‌پذیری: با خط‌مشی قراردادن برای موجودیت‌های مجازی‌شده تحقق می‌یابد. ازآنجاییکه محیط مجازی ایجادشده توسط ME Apps در یک MEH را می‌توان براساس نوع خدمت سفارشی کرد، ME Apps مختلف باید بطور مجزا از یکدیگر عمل کنند. بنابراین قراردادن ME Apps در MEH بطور مستقیم بر عامل دردسترس‌بودن تاثیر می‌گذارد.

۴) کاهش نقض‌های احراز هویت: توابع غیرقابل همسانه‌سازی فیزیکی (PUF) [۲۶]، داده‌های شتاب‌سنج[۸۰] [۲۷] و نور مرئی [۲۸] (به‌عنوان Li-Fi اشاره می‌شود) که برای بهبود احراز هویت شبکه‌های Wi-Fi بررسی شده‌اند. علاوه‌براین، روش‌های جدیدی برای امن‌سازی فازهای احراز هویت LPWAN [۲۹]، NB-IoT [۳۰]، RFID [۳۱] و BLE [۳۲] معرفی شده‌اند.

۵) کاهش نقض‌های اجازه دسترسی: وجود یک مدیر سکوی مورداعتماد[۸۱] (TPM) که می‌تواند برای شناسایی موجودیت‌های غیرقانونی از طریق معیارهای عملکرد آنها استفاده شود. نقض قوانین اجازه دسترسی را می‌توان از طریق یک سازوکار احراز هویت امن کاهش داد. MEPM که به‌عنوان ارکستراتور سکوی لبه عمل می‌کند، مسئول کنترل عملیات کنترل دسترسی امن است. علاوه‌براین، بلاکچین را می‌توان برای امن‌سازی چارچوب مدیریت اجازه دسترسی سیستم MEC بکار گرفت تا تخلفات را به‌حداقل برساند و در عین‌حال گزارش‌های سیستم را امن نگه دارد.

79 Quantum Resistance
80 Accelerometer data
81 Trusted Platform Manager

۵-۳) راهکارهای امنیتی مرتبط با شبکه لبه تلفن همراه

شبکه لبه تلفن همراه درحال‌تشکیل یک زیرساخت مجازی‌سازی مستقل است که همه موجودیت‌های سطح میزبان MEC تعریف‌شده توسط ETSI را به‌هم متصل می‌کند. بنابراین TVهای E1-E7، چالش‌های جدیدی را ایجاد می‌کنند که نیازمند راهکارهای نوپایی است که با آگاهی و هوش پیشرفته کار می‌کنند. درنتیجه راهکارهای زیر آرمانی هستند:

- بکارگیری یک مدیر سکوی مورداعتماد (TPM): در سطح میزبان لبه تلفن همراه، VIM و VI موجودیت‌هایی هستند که به احتمال زیاد توسط حملات خارجی به‌دلیل تسهیل منابع ME Apps درمعرض خطر قرار می‌گیرند. یک ماژول سکوی مورداعتماد[۸۲] (TPM) می‌تواند برای کاهش تهدیدات ناشی از VNFهای VI براساس دستکاری منابع همانطوریکه توسط Lal و همکاران پیشنهاد شده‌است، استفاده شود [۲۰].
- منطقه‌بندی امنیتی[۸۳]: جداسازی ترافیک از طریق VI برای ترافیک داده و مدیریت ترافیک، مدیریت ترافیک را ساده می‌کند درحالیکه ماشین‌های مجازی آلوده به سطح مدیریت (یعنی VIM) را مصادره می‌کند. این را می‌توان از طریق منطقه‌بندی امنیتی یا تشکیل مناطق غیرنظامی[۸۴] (DMZs) با اعمال کنترل دسترسی متمایز و خط‌مشی‌های دیوار آتش در مناطق مختلف به‌دست آورد [۲۰]. Nova-network و Neutronنمونه‌هایی از گروه‌های امنیتی موجود در Openstack هستند [۲۰]. علاوه‌براین، تشکیل DMZ برای TVهای E4، E5، E6 و E7 مفید خواهد بود که در آن اتصالات بین موجودیت‌های سطح لبه حفظ می‌شود.
- تشخیص نفوذ مبتنی بر درون‌نگری ماشین مجازی[۸۵] (VMI): درون‌نگری ماشین مجازی (VMI) روشی برای بازرسی محتوا و رفتار زمان اجرای ماشین‌های مجازی مستقر در یک VI است. روش‌های درون‌نگری هایپروایزر یا VMI برای تشخیص الگوهای غیرعادی در رفتار ماشین‌های مجازی یا هایپروایزر استفاده می‌شود. VMIها فعالیت‌های VMها را از نظر پردازنده و استفاده از حافظه نظارت می‌کنند.
- هوش مصنوعی[۸۶] (AI): روش‌های هوش مصنوعی اغلب برای توسعه راهکارهای امنیتی مستقل و سیستم‌های اطلاعاتی استفاده می‌شوند. این روش‌ها بطور گسترده و موفقیت‌آمیز جهت تشخیص بدافزار و ناهنجاری در MEC بکار می‌روند [۳۳]. یک سازوکار امنیتی مستقل برای سیستم MEC به‌دلیل ماهیت

82 Trusted Platform Module
83 Security zoning
۸۴ Demilitarized Zones، شبکه DMZ بطور خلاصه نوعی زیر شبکه محافظ است که به‌عنوان پل ارتباطی بین یک شبکه امن داخلی با شبکه غیرامنی مثل اینترنت عمل می‌کند و علاوه‌بر حفظ امنیت شبکه داخلی، ممکن است برخی خدمات همگانی شبکه داخلی را در بستر شبکه خارجی ارائه کند. فضای جداسازی‌شده شبکه DMZ، مجهزبه دیوارهای آتش و دروازه‌های امنیتی است که ترافیک بین شبکه DMZ و شبکه محلی را تحت نظر دارد. خدمت‌رسان DMZ به‌صورت پیش‌فرض مجهز به دروازه امنیتی دیگری است که از آن در برابر ترافیک ورودی از شبکه‌های خارجی مثل اینترنت محافظت می‌کند.
85 Virtual Machine Introspection
86 Artificial Intelligence

ناهمگون، تعداد بسیار زیاد تجهیزات متصل و استقرار مجازی‌سازی‌شده ذاتی است. ابتکارات مختلفی جهت تطبیق هوش مصنوعی برای پیشرفت‌های امنیتی مبتنی بر رایانش لبه راه‌اندازی شده‌است [۳۴] ، [۳۵].

- بلاکچین: بلاکچین یک چارچوب مدیریت داده امن و غیرمتمرکز است که با مفهوم ارز دیجیتال بیت کوین پدیدار شده‌است [۳۶]. این مفهوم بر محدودیت‌های سیستم‌های مدیریت داده متمرکز با امنیت بهبودیافته منتسب به بلوک‌های داده توزیع‌شده، غلبه می‌کند. حتی با وجود آگاهی از محتوا که برای مشترکین MEC تسهیل شده‌است، برون‌سپاری داده‌های خصوصی به طرف دیگر همچنان نگرانی‌هایی را ایجاد می‌کند. برای غلبه بر این مشکلات حریم خصوصی، بلاکچین[87] یک راهکار آشکار است. از دیدگاه MEC، بلاکچین می‌تواند برای امن‌سازی احراز هویت UE قابل‌استفاده باشد.
- برش شبکه: در برش شبکه، یک شبکه فیزیکی برای توانمندسازی خدمات متنوعی که به‌صورت همزمان ارائه می‌شوند، بطور منطقی به برش‌های مختلف تقسیم می‌شوند. با این رویکرد، هزینه‌های استفاده از منابع می‌تواند بطور قابل‌توجهی کاهش یابد. برش شبکه، ویژگی‌های پشتیبانی مجازی‌سازی، ماژولارسازی عملکرد، اتصال سرتاسر و جداسازی بهتر را در مقایسه با سایر مفاهیم اشتراک‌گذاری منابع ارائه می‌دهد.

توابع غیرقابل همسانه‌سازی فیزیکی یا PUFها: PUF یک موجودیت فیزیکی است که در یک ساختار فیزیکی قرار داده می‌شود. امروزه PUFها در مدارهای مجتمع پیاده‌سازی و معمولا در کاربردهایی که نیازمندی‌های امنیتی بالایی دارند و بطور خاص رمزنگاری می‌شوند، استفاده می‌شوند. همه PUFها از تغییرات محیطی مانند دما، ولتاژ تغذیه و تداخل الکترومغناطیسی تاثیر می‌پذیرند و کارآیی آنها تغییر می‌کند. PUF یک شیءِ فیزیکی است که به‌ازای یک ورودی و شرایط (چالش)، یک خروجی تحت عنوان «اثرانگشت دیجیتال» فیزیکی تعریف‌شده ارائه می‌دهد که این خروجی به‌عنوان یک شناسه منحصربه‌فرد و بیشتر برای تجهیزات نیمه‌رسانا مثل ریزپردازنده‌ها استفاده می‌شود.

۵-۴) راهکارهای امنیتی مرتبط با شبکه هسته

ازآنجاییکه شبکه هسته یا سطح سیستم MEC یک ساختار مجازی‌شده را تشکیل می‌دهد، راهکارهای خاص قابل‌اعمال به MEN را در اینجا به‌صورت زیر دسته‌بندی می‌کنیم:

- به‌روزرسانی اعتبارنامه‌های امنیتی: به‌روزرسانی به‌موقع وصله‌های امنیتی[88]، به‌ویژه هنگام فعال‌سازی خدمات دسترسی از راه دور نظیر Secure Shell (SSH)، در موارد ضروری توصیه می‌شود. علاوه‌براین، استقرار و الزام به اجرای یک خط‌مشی رمز عبور قوی برای مدیران در سطح ابر و سیستم، یک ضرورت اساسی در چارچوب الزامات امنیت سایبری به‌شمار می‌رود.
- ابزارهای مستحکم‌سازی کرنل[89]: استفاده از لینوکس تقویت‌شده امنیت (SELinux) برای سطح سیستم MEاز ابزارهای مستحکم‌سازی کرنل مانند مجازی‌سازی امن (sVirt) یا hidepd سود می‌برد که در آن

87 Blockchain
88 Security patches
89 Kernel hardening tools

جداسازی بین فایل‌های داده و فرآیندها ایجاد می‌شود. بنابراین زیرساخت کرنل‌های لینوکس امکان حمله متقابل به تلاش‌های اشباع خارجی یا داخلی را در هر موجودیت در سطح سیستم افزایش می‌دهد.

- درون‌نگری هایپروایزر: درون‌نگری هایپروایزر می‌تواند در سطح سیستم برای تشخیص رفتار غیرعادی استفاده شود.
- تایید از راه دور: پیونددادن خدمت‌رسان تایید از راه دور با سطوح لبه و سیستم، MEO را قادر می‌سازد تا فرآیندهای ثبت‌شده را به‌صورت شفاف برای تایید پیاده کند [۳۷].
- سکوی مورد اعتماد NFVI: ین و همکاران در مرجع [۳۸] یک سکوی قابل‌اعتماد NFVI (NFVI-TP) برای شبکه‌های 5G آینده پیشنهاد می‌کنند که در آن جریان‌های ترافیک با استفاده از SDN و محاسبات ابری که برای راه‌اندازی خدمات اتخاذ شده‌است، هدایت می‌شوند. به‌دلیل گسترش امنیت مجازی و توابع اعتماد در سرتاسر سیستم NFVI، شکل‌گیری این چارچوب جامع جهت استقرار در سطح سیستم MEC امکان‌پذیر است. تمرکز طراحی سکوی پیشنهادی به‌سمت شبکه 5G، اطمینان از همزیستی شبکه هسته و موجودیت‌های سطح سیستم است.
- چارچوب SDN/NFV: چارچوبی توسط فریس و همکاران [۳۹] جهت اعمال امنیت در استقرار SDN/NFV برای موارد استفاده از MEC-IoT پیشنهاد شده‌است. چارچوب مذکور با سه صفحه تشکیل شده‌است: صفحه کاربر، صفحه ارکستراسیون امنیتی و صفحه اجرای امنیت. صفحه کاربر، ابزارهایی را جهت پیکربندی خط‌مشی‌های امنیتی قابل‌اعمال برای سیستم و شبکه مانند: احراز هویت، اجازه دسترسی، فیلترکردن، حفاظت از کانال و ارسال روبه‌جلو ارائه می‌کند. صفحه ارکستراسیون امنیتی، سازوکارهای امنیتی مبتنی بر خط‌مشی را برای بکارگیری عوامل امنیتی و افزایش آگاهی هوشمند بکار می‌گیرد. بنابراین عملکردهای این صفحه شامل تفسیر خط‌مشی، نظارت و ارائه توانمندسازی‌های امنیتی است. صفحه اجرای امنیت، عملکردهای کنترل و مدیریت حوزه‌های عملیاتی (IoT/ SDN/ NFV MANO)، زیرساخت و مجازی‌سازی (موجودیت فیزیکی برای انجام عملکردهای محاسباتی، ذخیره‌سازی و شبکه)، VNF (سازوکارهای امنیتی و اعتماد در VI)، شیوه‌نامه‌های EAP و DTLS را ترکیب می‌کند. بنابراین چارچوب پیشنهادی به سطح لبه MEC گسترش می‌یابد چراکه عملیات و حوزه‌های MEC را بطور جامع ادغام می‌کند.
- چارچوب‌های امنیتی: چارچوب‌های خط‌مشی امنیتی برای امن‌سازی VNFها در شبکه‌های NFV در مرجع [۴۰] پیشنهاد شد.
- اصلاح ارکستراتور NFV: اصلاحاتی در ارکستراتور NFV فعلی برای مدیریت سازوکارهای امنیتی 5G در [۴۱] پیشنهاد شد.

۵-۵) راهکارهای امنیتی موجود مرتبط با معماری ساختار MEC

۱) AR1 (برش شبکه): چندین روش برای کاهش خطرات امنیتی در برش‌های شبکه پیشنهاد شده‌است که در استقرار MEC قابل‌پذیرش است [۴۲] و عبارتنداز:

- طرح‌های احراز هویت: انطباق طرح‌های احراز هویت متقابل بین NSMها و موجودیت‌های سکوی میزبان قبل از راه‌اندازی NSI، حملات جعل هویت را رهگیری می‌کند. علاوه‌براین، NSMها باید خود را در هر تعامل، احراز هویت کنند.
- ممیزی و اعتبارسنجی NSIs: NSIهایی که توابع مجازی یا VMها را اجرا می‌کنند، باید بطور دوره‌ای ممیزی و اعتبارسنجی شوند تا از حملات مبتنی بر VM جلوگیری شود.
- تمایز امنیتی و جداسازی برش: سطوح مختلف امنیتی باید برای برش‌های شبکه با جداسازی کافی اعمال شود تا دسترسی عوامل مخرب محدود شود.
- چارچوب احراز هویت: نویسندگان در مرجع [۴۳] یک چارچوب احراز هویت خدمت‌گرا برای پشتیبانی از برش شبکه در خدمات اینترنت اشیا با قابلیت 5G پیشنهاد کردند. چارچوب پیشنهادی بر روی معماری محاسبات مه جهت توصیف توالی‌های احراز هویت تمرکز دارد. بااین‌حال، استقرار برش‌های شبکه در چارچوب پیشنهادی باتوجه به شباهت در ساختار خدمات در موجودیت‌های شبکه دسترسی با الگوهای مه و MEC سازگار است درحالیکه شبکه هسته برای هر دو مورد توسط 5G ارائه می‌شود. این چارچوب اهداف حریم خصوصی، حفظ انتخاب برش، احراز هویت ناشناس خدمت‌گرا و توافق کلید خدمت‌گرا را تعیین می‌کند.

۲) AR2 (فرمان دادن ترافیک): همانطورکه SFC، در حال تبدیل‌شدن به یک پیاده‌سازی محبوب و اجباری برای دستیابی به هدایت ترافیک کارآمد در شبکه‌های مجازی یا نرم‌افزاری است، اکثر راهکارهای رایج به آن مربوط می‌شوند:

- راهکارهای مبتنی بر SFC
- تصمیم‌گیری مبتنی بر فازی در امنیت کاربردی
- چارچوب امنیتی برای SFC

۳) AR3 (مهاجرت خدمت): درک پویایی موجود در مهاجرت خدمت برای توسعه اقدامات امنیتی معماری MEC بسیار مهم است و امنیت آن با تعریف چارچوب مهاجرت امن و نیز بکارگیری بلاکچین جهت امن‌سازی مهاجرت صورت می‌گیرد.

۴) AR4 (مدیریت تحرک): راهکارهای تحرک موجود یا برای ایجاد تونل‌ها، شیوه‌نامه‌های امنیتی یا مدل‌های مبتنی بر پارامترهای لایه فیزیکی پیشنهاد شده‌اند. همه این راهکارها با آگاهی از تحرک پویا شکل می‌گیرند:

- مدیریت تحرک توزیع‌شده از طریق تونل‌زنی پویا
- شیوه‌نامه امنیتی آگاه از تحرک
- محرمانگی در مدل‌های تحرک امنیت در لایه فیزیکی

۶) رتبه‌بندی تهدیدات

در این بخش می‌خواهیم به رتبه‌بندی تهدیدات MEC شبکه 5G بپردازیم. برای رتبه‌بندی تهدیدات با معرفی معیار ریسک، به هر کدام از تهدیدات نمره‌ای اختصاص می‌دهیم تا درنهایت بتوانیم تهدیدها را اولویت‌بندی نماییم.

ریسک به معنای «خطر»، «احتمال زیان» یا «عدم قطعیت پیرامون یک رویداد» ترجمه می‌شود. بطورکلی ریسک عبارتست از: امکان وقوع یک واقعه نامطلوب یا غیرمنتظره که می‌تواند بر دستیابی به اهداف، تاثیر منفی بگذارد. براساس تعاریف IEEE، ریسک یک کمیت عینی است که برای توصیف میزان آسیب به یک سامانه خاص از فعالیت‌ها و فناوری‌های متعدد بکار می‌رود [۴۴]. ریسک را می‌توان به‌صورت ترکیبی از احتمال وقوع یک رویداد و پیامدهای ناشی از وقوع آن رویداد تعریف کرد. عناصر تشکیل‌دهنده ریسک عبارتنداز:

- احتمال وقوع[۹۰]: اینکه یک رویداد خاص چقدر ممکن است رخ دهد.
- پیامد[۹۱]: اگر آن رویداد رخ دهد، چه اثری بر فرد، سازمان یا سیستم خواهد داشت.

باید توجه داشت که ریسک همواره با عدم قطعیت همراه است اما با «خطر قطعی» متفاوت است چون اگر وقوع یک رویداد کاملا قطعی باشد، دیگر ریسک وجود ندارد و تنها پیامد قطعی مطرح است. در یک جمع‌بندی:

- ریسک همواره با احتمال و عدم قطعیت سروکار دارد.
- هرچه احتمال وقوع یک تهدید یا شدت پیامد آن بیشتر باشد، ریسک بالاتر خواهد بود.
- مدیریت ریسک یعنی شناسایی، تحلیل و کنترل عواملی که می‌توانند احتمال یا شدت نتایج منفی را کاهش دهند.

دراین‌صورت، ریسک به‌صورت ضرب‌در «احتمال موفقیت تهدید» در «میزان تاثیر یا شدت آن تهدید» تعریف می‌شود. به‌عبارت‌دیگر:

$$\text{ریسک} = \text{احتمال موفقیت یک تهدید} \times \text{شدت آن تهدید} \quad (۱)$$

برمبنای مرجع [۳]، پنج وضعیت برای میزان تاثیر/شدت تهدیدات درنظر گرفته شده‌است که برمبنای آن یک امتیاز عددی ارائه می‌گردد تا بتوان تهدیدات را اولویت‌بندی کرد (جدول ۲):

الف) تهدیدات دارای تبعات جدی و غیرقابل‌جبران (شدت بحرانی و عدد ۱۰ برای آن درنظر می‌گیریم).

ب) تهدیدات دارای تبعات مهم و قابل‌جبران ولی با هزینه زیاد (شدت بالا و عدد ۸ برای آن درنظر می‌گیریم).

ج) تهدیدات دارای تبعات میانه و قابل‌جبران با هزینه معقول (شدت میانه و عدد ۵ برای آن درنظر می‌گیریم).

د) تهدیدات دارای تبعات نه‌چندان‌مهم و قابل‌جبران با هزینه کم (شدت کم و عدد ۲ برای آن درنظر می‌گیریم).

ه) تهدیدات با تبعات ناچیز و قابل‌جبران با هزینه بسیار مختصر (شدت صفر و عدد صفر برای آن درنظر می‌گیریم).

90 Likelihood/probability
91 Consequence/impact

جدول ۲: میزان تاثیر/شدت تهدید

میزان شدت	محدوده نمره‌دهی
هیچ (None)	صفر
کم (Low)	۰.۱-۳.۹
متوسط (Medium)	۴.۰-۶.۹
بالا (High)	۷.۰-۸.۹
بحرانی	۹.۰-۱۰.۰

به‌منظور محاسبه ریسک، ابتدا احتمال موفقیت تهدیدات/حملات ذکرشده را با استناد به منابع معتبر (مانند اسناد ENISA و مجلات ISI) که به نوعی نظرات خبرگی محققین و اهالی صنعت می‌باشد، بررسی می‌کنیم. سپس میزان تاثیر همین حملات مورد تحقیق و مطالعه قرار می‌گیرد.

جدول ۳، تهدیدات/حملات به MEC و نیز ارتباط‌شان با بردارهای تهدید را خلاصه می‌کند. این جدول با مطالعه مرجع [۷] تدوین شده‌است. رنگ‌های مختلف، بیانگر احتمال موفقیت تهدیدها هستند. به‌عبارت دقیق‌تر، رنگ قرمز یعنی احتمال بالا (نمره ۰٫۷۵)، رنگ سبز یعنی احتمال متوسط (نمره ۰٫۵) و رنگ زرد یعنی احتمال کم (نمره ۰٫۲۵).

توجه شود که در این جدول، احتمال موفقیت تهدیدات/حملات با جزئیات بهتر درج شده‌است. یعنی در نقاط مختلف MEC، این احتمال به‌چه‌صورت خواهد بود. برای ارزیابی احتمال موفقیت هر تهدید/حمله، با جمع‌کردن مقادیر مرتبط با سطرهای آن و سپس تقسیم‌کردن بر ۲۰ (جهت نرمال‌سازی)، مقدار احتمال را خواهد داد. نتیجه چنین کاری، در جدول ۴ آمده‌است. از جدول ۴ موارد زیر قابل‌استنباط است:

- حمله رد خواب رفتگی[۹۲]، دسته خاصی از حملات DoS است که مهاجم، از اینکه گره‌های حسگر باتری‌دار به‌حالت خواب رفتگی بروند، جلوگیری می‌کند و درنتیجه بر عملکرد شبکه تاثیر می‌گذارد. به‌عبارت‌دیگر، این حمله از طریق وادارکردن تجهیزات شبکه‌های IoT به روشن‌ماندن، باتری آنها را تمام می‌کند. MES درگیر با UE آسیب‌دیده، منجر به وقفه می‌شود. این حملات، بردارهای تهدید جدی در لایه دسترسی هستند.
- استخراج داده‌ها[۹۳] نوعی سرقت داده است مانند انتقال عمدی، غیرمجاز و مخفیانه داده‌ها از رایانه یا یک تجهیز دیگر. استخراج داده‌ها می‌تواند به‌صورت دستی یا خودکار با استفاده از بدافزار انجام شود. این حمله در میان مخرب‌ترین تهدیدات امنیت رایانه‌ای قرار دارد.
- حملات DoS/DDoD ، APTها و نیز حملات Spoofing از محتمل‌ترین حملات در لایه لبه می‌باشند.

92 Denial of sleep

۹۳ Data exfiltration؛ داده‌های یک موجودیت یا یک سیستم آلوده بدون تایید منتقل می‌شود.

جدول ۳. تهدیدات/حملات در لایه لبه تلفن همراه و میزان احتمال وقوع آنها در نقاط مختلف

جدول ٤. احتمال وقوع تهدیدات لبه تلفن همراه

Prob. Successful Attack	Threats/Attacks
	General threats
0.3	Viruses / Worms
0.35	DoS/DDos
0.15	Eavesdropping
0.08	Jamming
0.26	MitM
0.2	Relay attack
0.35	APTs
0.21	Sybil attack
0.33	Spoofing attack
	Non- Crypt analytic attacks
0.05	Side-Channel Attacks (SCAs)
0.04	Physical damage
0.04	Hardware Trojan (HT)
	Networking/Routing attacks
0.14	Malicious Node injection
0.21	Sinkhole attack
0.21	Wormhole attack
0.31	Reduction of Quality (RoQ) attack
0.08	Denial of sleep attack
	Virtualization/VM based Threats
0.21	Service manipulation
0.23	Privilege Escalation
0.18	VM Manipulation attack

0.23	DNS Amplification attack
0.15	VM escape attack
0.18	VNF location shift attack
0.19	Security log troubleshooting failure
	Softwarized Threats
0.26	Software Vulnerability
0.08	Data exfiltration
0.11	Malicious code injection

در حال حاضر می‌خواهیم مولفه‌ای دیگر در ارزیابی ریسک یعنی تاثیر/شدت تهدیدات را بررسی کنیم. برای ارزیابی این مهم، خوب است که ببینیم تهدیدات ذکرشده در جدول ۳، کدامیک از خدمات امنیتی محرمانگی (Confidentiality)، یکپارچگی (Integrity)، دسترسی‌پذیری (Availability)، احراز هویت (Authentication) و مجوز دادن (Authorization) را نقض می‌کند. در جدول ۵، این موضوع به خوبی نشان داده شده‌است. نکته مهم این است که بر مبنای تاکید مراجع علمی، این الزامات در ارزیابی تاثیر/شدت، بسته به کاربرد (نوع کسب‌وکار)، مدت زمان حمله و تاثیر اقتصادی تفاوت می‌کنند. برای مثال: سناریوی دستگاه‌های متصل به لبه که تحلیل‌های بی‌درنگ یا برنامه‌های شهر هوشمند را مدیریت می‌کنند را درنظر بگیرید. ویروسی (Viruse) که در این نقطه پخش می‌شود باعث قطع خدمت و مشکلات عملیاتی می‌گردد که میزان آسیب و تاثیر آن high است اما ویروسی که در لبه به چند کاربر سرایت می‌کند، شدتی از نوع low دارد.

حال می‌بایست رابطه‌ای بین تهدیدات و ملزومات امنیتی تعیین کنیم. نتیجه مطالعات و ارزیابی‌های ما مبتنی بر مطالعه سند ENISA، چند مقاله ISI و نیز نظر خبرگی سه متخصص حوزه امنیت، در جدول ۵ تدوین شده‌است. در این جدول، نماد × یعنی نقض الزام امنیتی و عدم وجود نماد به این معناست که تهدید موردنظر، آن الزام امنیتی را نقض نمی‌کند. همچنین یک عدد متوسط برای میزان تاثیر/شدت تهدیدات در جدول ۵ ستون سمت راست، ارائه کرده‌ایم که این اعداد مبتنی بر نظر خبرگی سه محقق و متخصص در حوزه شبکه و امنیت تدوین شده‌است.

جدول ۵. تهدیدات/حملات و تاثیر آنها بر روی الزمات امنیتی CIAAA

Impact/Damage/Severity between 0` and 10	Authorization	Authentication	Availability	Integrity	Confidentiality	Threats/Attacks
General threats						

Medium (5)		×	×	×		Viruses / Worms
High (8)			×			DoS/DDos
High (8)	×	×		×	×	Eavesdropping and Hijacking
High (8)			×		×	Jamming
High (8)			×	×	×	MitM
Medium (5)			×	×	×	Relay attack
Critical (10)	×			×	×	APTs
High (8)			×	×	×	Sybil attack
High (8)		×	×	×	×	Spoofing attack
Non- Crypt analytic attacks						
High (8)	×		×	×	×	Side-Channel Attacks (SCAs)
High (8)	×		×	×		Physical damage
Critical (10)			×	×	×	Hardware Trojan (HT)
Networking/Routing attacks						
High (8)		×	×	×		Malicious Node injection
Medium (5)			×	×	×	Sinkhole attack
High (8)			×	×	×	Wormhole attack
High (8)			×	×	×	Reduction of Quality (RoQ) attack
Medium (5)			×	×	×	Denial of sleep attack
Virtualization/VM based Threats						
High (8)	×		×	×		Service manipulation
Critical (10)	×		×	×	×	Privilege Escalation
High (8)			×	×	×	VM Manipulation attack
High (8)			×	×	×	DNS Amplification/Manipulation attack
Critical (10)	×		×	×	×	VM escape attack
High (8)			×	×	×	VNF location shift attack

Medium (5)	×				×	Security log troubleshooting failure
Softwarized Threats						
High (8)	×	×	×	×	×	Software Vulnerability
Critical (10)			×	×	×	Data exfiltration (include location privacy)
High (8)		×	×	×	×	Malicious code injection

باتوجه‌به اطلاعات ارائه‌شده در جداول ۳ و ۵، نمره نهایی ریسک اختصاصی به هر کدام از تهدیدات/حملات MEC در جدول ۶ محاسبه شده‌است. باتوجه به این نمره‌ها، می‌توان تهدیدات را اولویت‌بندی کرد. توجه شود حداکثر مقدار برای هر خانه در جدول ۶ برابر با ۷٫۵ است. به‌عبارت‌دیگر، $0 \leq \text{RISK} \leq 7.5$. بر مبنای ارزیابی‌های ارائه‌شده در جدول ۶، پنج تهدید برتر (۲۰ درصد تهدیدات برتر) به‌ترتیب، به‌شرح زیر هستند:

- APTs
- DoS/DDoS
- Spoofing
- Privilege Escalation
- Reduction of Quality (RoQ)

جدول ٦. تهدیدات/حملات MEC و مقدار ریسک (نمره نهایی) آنها جهت اولویت‌بندی‌کردن

Risk	**Threats/Attacks**
	General threats
1.3	Viruses / Worms
2.8	DoS/DDos
1.2	Eavesdropping/Hijacking
0.64	Jamming
2.08	MitM
1	Relay attack
3.5	APTs
1.68	Sybil attack
2.64	Spoofing attack
	Non- Crypt analytic attacks

0.4	Side-Channel Attacks (SCAs)
0.32	Physical damage
0.4	Hardware Trojan (HT)
	Networking/Routing attacks
1.12	Malicious node injection
1.05	Sinkhole attack
1.68	Wormhole attack
2.48	Reduction of Quality (RoQ) attack
0.4	Denial of sleep attack
	Virtualization/VM based Threats
1.68	Service manipulation
2.3	Privilege escalation
1.44	VM manipulation attack
1.84	DNS amplification attack
1.5	VM escape attack
1.44	VNF location shift attack
0.95	Security log troubleshooting failure
	Softwarized Threats
2.08	Software vulnerability
0.8	Data exfiltration
0.88	Malicious code injection

۷) فعالیت‌های آینده

باتوجه‌به آسیب‌پذیری‌های امنیتی متنوعی که در این مطالعه شناسایی شده‌اند، مشخص است که ارائه یک راهکار امنیتی جامع برای کل سیستم عملا امکان‌پذیر نیست. ازاین‌رو، منطقی‌تر این است که این تفاوت‌های پیچیده باید با استفاده از

سازوکارهای برقراری امنیت که متناسب با نیازهای خاص هر مورد استفاده منحصربه‌فرد MEC طراحی شده‌اند، برطرف شوند. ازسوی‌دیگر، برای بهبود امنیت در MEC در حوزه‌های زیر می‌توان فعالیت نموده و زمینه‌های تحقیق فراهم می‌باشد:

- استفاده از هوش مصنوعی (AI)، یادگیری ماشین (ML) و یادگیری عمیق[۹۴] (DL)، ابزارهای موثری برای تحلیل بدافزار و تشخیص ناهنجاری‌ها در MEC و 5G هستند و با شبیه‌سازی رفتار و تله‌گذاری (مثل هانی‌پات)، امنیت سامانه را در برابر تهدیدات جدید تقویت می‌کنند. مطالعه مرجع [۴۵] می‌تواند دانش خوبی را به خواننده درمورد یک روش احراز هویت لایه فیزیکی[۹۵] (PLA) مبتنی بر یادگیری ماشین در مخابرات 6G ارائه دهد که از ویژگی‌های فیزیکی ناهماهنگی[۹۶] I/Q، نویز فاز و اختلالات جابجایی فرکانس حامل[۹۷] (CFO) استفاده نموده‌است.
- یادگیری تقویتی[۹۸] (RL) با الهام از تجربه و بازخورد محیط، امکان تصمیم‌گیری هوشمند و انتخاب شیوه‌نامه‌های امنیتی بهینه را در MEC و دستگاه‌های IoT، بدون وابستگی به داده‌های آموزشی فراهم می‌سازد.
- قابلیت امنیت آگاهی از زمینه[۹۹] در فناوری‌های تلفن همراه با بهره‌گیری از حسگرهای پیشرفته، امکان ارائه خدمات هوشمند و شخصی‌سازی‌شده را فراهم می‌کند. هرچند این کاربردها نگرانی‌های امنیتی برای کاربران به‌همراه دارند اما استفاده از داده‌های زمینه‌ای می‌تواند پیاده‌سازی راهکارهای امنیتی تطبیقی و خودکار را در لبه شبکه MEC امکان‌پذیر کند. چنین سازوکارهایی با استانداردسازی مدل‌هایی مانند «امنیت به عنوان خدمت» (SECaaS)، به تقویت امنیت مبتنی بر زمینه در زیرساخت‌های MEC کمک می‌کنند.
- میکروسرویس‌ها[۱۰۰]، برنامه کاربردی را به بخش‌هایی مستقل و کوچک تقسیم می‌کنند که امکان مدیریت و استقرار جداگانه را فراهم می‌سازند اما تعامل شبکه‌ای را پیچیده‌تر می‌کنند. در MEC، امنیت می‌تواند به شکل سرویس برای این میکروسرویس‌ها پیاده‌سازی شود. رایانش اسمزی[۱۰۱] نیز با مدیریت پویا و مهاجرت سرویس‌ها بین لبه و ابر، امنیت هماهنگ در هر دو بخش را فراهم می‌کند.
- در سال‌های اخیر، بلاکچین بسیار مورد توجه قرار گرفته و در بسیاری از سیستم‌های ارتباطی بکار رفته‌است. به‌ویژه بلاکچین می‌تواند نقش قابل‌توجهی در حوزه اینترنت اشیا (IoT) ایفا کند. بلاکچین می‌تواند نقش مهمی در افزایش امنیت در سیستم‌های MEC ایفا کند اما تاکنون سکوی اختصاصی مبتنی بر بلاکچین برای MEC ارائه نشده‌است.

94 Deep Learning
95 Physical layer authentication
96 Imbalance
97 Carrier frequency offset
98 Reinforcement Learning
99 Context Aware Security
100 Microservices
101 Osmotic Computing

۸) نتیجه‌گیری و پیشنهادها

محاسبات لبه در شبکه 5G، پردازش سریع و کارآمد داده‌ها در شبکه‌های تلفن همراه را به ارمغان می‌آورد. MEC، یک فناوری کلیدی است که این خدمات جدید را با استقرار چندین تجهیز با قابلیت‌های محاسباتی و ذخیره‌سازی در لبه شبکه، نزدیک به کاربران نهایی فعال می‌کند. لذا امنیت، عامل مهمی در تحقق استقرار MEC می‌باشد. در این مقاله، ما ضمن مروری بر معماری 5G و سپس تمرکز بر معماری MEC، تهدیدات، آسیب‌پذیری‌ها و راهکارهای امنیتی ارائه‌شده توسط مراجع علمی را مورد بررسی قرار دادیم. در گام بعد، با ارزیابی تاثیر/شدت و احتمال موفقیت تهدیدات اخذشده بر روی 5G، به تحلیل معیار ریسک پرداختیم. با کمک ریسک‌های به‌دست‌آمده، به رتبه‌بندی تهدیدات پرداختیم. نتایج این مقاله بیان می‌کند پنج تهدید برتر در لبه شبکه تلفن همراه 5G به‌ترتیب عبارتنداز: APTها، DoS/DDoS، Spoofing، Privilege Escalation و Reduction of Quality (RoQ). نتایج این مقاله، به امن‌کردن شبکه 5G و استقرار راهکارهای امنیتی کمک می‌کند.

منابع

A. Reznik, Y. Fang, and S. Ullah, “MEC in an enterprise setting: A solution outline,” ETSI, Sophia Antipolis, France, White Paper, 2018. Accessed: May 16, 2019. [Online]. Available:
https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_ FINAL.pdf .
ISBN No. 979-10-92620-25-2

A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, “AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes,” J. Ambient Intell. Humanized Comput., vol. 14, pp. 4869–4882 ,2023. https://doi.org/10.1007/s12652-020-01770-0

C. Lorenz et al., “An SDN/NFV-enabled enterprise network architecture offering fine-grained security policy enforcement,” IEEE Commun. Mag., vol. 55, no. 3, pp. 217–223, Mar. 2017. DOI: 10.1109/MCOM.2017.1600414CM

Cloud Edge Computing: Beyond the Data Center, OpenStack, Austin, TX, USA, 2018.

“ENISA threat landscape” report, Oct. 2023.

ETSI. (2015). Network Functions Virtualisation (NFV) Security: Report on Use Cases and Technical Approaches for Multi-Layer Host Administration. Accessed: May 16, 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFVSEC/ 001_099/009/01.01.01_60/gs_nfv-sec009v010101p.pdf

ETSI. (2016). Mobile Edge Computing (MEC) Framework and Reference Architecture. Accessed: May 16, 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf

F. Zhang, G. Liu, X. Fu, and R. Yahyapour, “A survey on virtual machine migration: Challenges, techniques, and open issues,” IEEE Commun. Surveys Tuts., vol. 20, no. 2, pp. 1206–1243, 2nd Quart., 2018. DOI: 10.1109/COMST.2018.2794881

G. Li and P. Bours, “Studying WiFi and accelerometer data based authentication method on mobile phones,” in Proc. ACM 2nd Int. Conf. Biometr. Eng. Appl., 2018, pp. 18–23. DOI:10.1145/3230820.3230824

G. Nencioni, R. G. Garroppo and R. F. Olimid, "5G Multi-Access Edge Computing: A Survey on Security, Dependability, and Performance," IEEE Access, vol. 11, pp. 63496-63533, 2023. DOI: 10.1109/ACCESS.2023.3288334

I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, “Network slicing and softwarization: A survey on principles, enabling technologies, and solutions,” IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018. DOI:10.1109/COMST.2018.2815638

I. Farris et al., “Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems,” in Proc. IEEE Conf. Stand. Commun. Netw. (CSCN), 2017, pp. 169–174. DOI: 10.1109/CSCN.2017.8088617

J. Ni, X. Lin, and X. S. Shen, “Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT,” IEEE J. Sel. Areas in Commun., vol. 36, no. 3, pp. 644–657, 2018. DOI: 10.1109/JSAC.2018.2815418

M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, “A PUF based light weight protocol for secure WiFi authentication of IoT devices,” in Proc. IEEE 8th Int. Symp. Embedded Comput. Syst. Design (ISED), 2018, pp. 183–187. DOI: 10.1109/ISED.2018.8703993

M. Pattaranantakul, Y. Tseng, R. He, Z. Zhang, and A. Meddahi, “A first step towards security extension for NFV orchestrator,” in Proc. ACM Int. Workshop Security Softw. Defined Netw. Netw. Function Virtualization, 2017, pp. 25–30. DOI:10.1145/3040992.3040995

Multi-Access Edge Computing (MEC); Terminology, Standard GS MEC 001, Version 3.1.1, ETSI, Jan. 2022.

Multi-Access Edge Computing (MEC); Framework and Reference Architecture, Standard GS MEC 003, Version 3.1.1, Mar. 2022.

Multi-Access Edge Computing (MEC); Study on Inter-MEC Systems and MEC-Cloud Systems Coordination, Standard GR MEC 035, Version 3.1.1, ETSI, Jun. 2021.

N. Islam, S. Das, and Y. Chen, "On-device mobile phone security exploits machine learning," IEEE Pervasive Comput., vol. 16, no. 2, pp. 92–96, Apr.–Jun. 2017. DOI: 10.1109/MPRV.2017.26

O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in device-to-device communications: A survey," IET Netw., vol. 7, no. 1, pp. 14–22, 2017. https://doi.org/10.1049/iet-net.2017.0119

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

P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," Future Gener. Comput. Syst., vol. 83, pp. 629–637, Jun. 2018. https://doi.org/10.1016/j.future.2017.06.023

P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017. DOI: 10.1109/COMST.2017.2682318

P. Ranaweera, A. D. Jurcut, M. Liyanage, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," IEEE Commun. Surveys Tuts., vol. 23, no. 2, pp. 1078 – 1124, 2021. DOI: 10.1109/COMST.2021.3062546

P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018. DOI: 10.1109/COMST.2018.2849509

P. Porambage, T. Kumar, M. Liyanage, J. Partala, L. Lov´en, M. Ylianttila, and T. Sepp¨anen. (2019) Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI. Last accessed May 16, 2019. [Online]. Available: https://www.researchgate.net/publication/330838792 Sec-EdgeAI AI for Edge Security Vs Security for Edge AI.

R. Harel and S. Babbage, "5G Security Recommendations Package 2: Network Slicing," 2016, last accessed 16 May 2019. [Online]. Available: https://www.ngmn.org/fileadmin/user upload/160429 NGMN 5G Security Network Slicing v1 0.pdf

R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196–248, 1st Quart., 2020. DOI: 10.1109/COMST.2019.2933899

R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," Future Gener. Comput. Syst., vol. 78, pp. 680–698, Jan. 2018. https://doi.org/10.1016/j.future.2016.11.009

S. -C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, and C. Su, "A userfriendly privacy framework for users to achieve consents with nearby BLE devices," IEEE Access, vol. 6, pp. 20779–20787, 2018. DOI: 10.1109/ACCESS.2018.2820716

S. Kekki et al. (2018). MEC in 5G Networks. Accessed: May 16, 2019. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," IEEE Commun. Mag., vol. 55, no. 8, pp. 211–217, Aug. 2017. DOI: 10.1109/MCOM.2017.1600899

S. Wang, Y. Zhao, J. Xu, J. Yuan, and C.-H. Hsu, "Edge server placement in mobile edge computing," J. Parallel Distrib. Comput., vol. 127, pp. 160–168, May 2019. https://doi.org/10.1016/j.jpdc.2018.06.008

T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing gadget-free digital services," Computer, vol. 51, no. 11, pp. 66–77, 2018. DOI: 10.1109/MC.2018.2876017

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 Commun.Surveys Tuts., vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017. DOI: 10.1109/COMST.2017.2705720

W. Huang et al., "A New System Risk Definition and System Risk Analysis Approach Based on Improved Risk Field," IEEE Trans. on Reliability, vol. 69, no. 4, pp. 1437-1452, Dec. 2020. DOI: 10.1109/TR.2019.2942373

X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-based Efficient and Incentive Approach," IEEE Trans. on Industrial Informatics, 2019. DOI: 10.1109/TII.2019.2917307

X. Wang et al., "Deep learning-based classification and anomaly detection of side-channel signals," in Proc. Cyber Sensing, vol. 10630. Orlando, FL, USA, 2018, Art. no. 1063006. [Online]. Available: https://doi.org/10.1117/12.2311329

X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in Proc. IEEE Conf. Stand. Commun. Netw. (CSCN), 2017, pp. 181–186. DOI: 10.1109/CSCN.2017.8088619

Y. Jeon, H.-I. Ju, and S. Yoon, "Design of an LPWAN communication module based on secure element for smart parking application," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE), 2018, pp. 1–2. DOI: 10.1109/ICCE.2018.8326112

Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," IEEE Access, vol. 7, pp. 114721–114730, 2019. DOI: 10.1109/ACCESS.2019.2936123

Z. Ezzati Khatab. A. Mohammadi, V. Pourahmadi, A. Kuhestani, "A machine learning-based physical layer authentication with phase impairments," Physical Commun., vol. 68, Feb. 2025. Doi: https://doi.org/10.1016/j.phycom.2024.102545

Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain Meets Edge Computing," IEEE Commun. Mag., vol. 56, no. 8, pp. 33–39, 2018. DOI: 10.1109/MCOM.2018.1701095

Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," Security Commun. Netw., vol. 9, no. 16, pp. 3059–3069, 2016. DOI:10.1002/sec.1243

Z. Zhao, G. Min, Y. Pang, W. Gao, and J. Lv, “Towards fast and reliable WiFi authentication by utilizing visible light diversity,” in Proc. 16th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON), 2019, pp. 1–9. DOI: 10.1109/SAHCN.2019.8824935