Research on Edge Computing Security Defense of Information Energy System

Jian Jiang¹, Jian Li²*, Juan Chen¹

¹Zhongtian Internet Technology Co., Ltd., Nantong, China
²School of Information Science and Engineering, Fujian University of Technology, Fuzhou, China

*Corresponding author: 2502804053@qq.com

Abstract. Mobile Edge Computing (MEC) can effectively solve the problem of heavy backhaul link load and the long delay in traditional networks by further extending the telecom cellular network to other wireless access networks. However, because MEC nodes have abundant computing resources, communication resources, and storage resources, they carry the sensitive data storage, communication applications, and computing services of multiple enterprises. Once the attacker controls the edge nodes, they can use the edge nodes for further horizontal or Vertical attacks will seriously damage the confidentiality, availability, and integrity of applications, communications, and data, and will bring a wide range of new security threats to users and society. At the same time, MEC nodes are often deployed in unattended computer rooms, and there are multiple operators and responsible parties in the safety life cycle, which brings more challenges to physical safety protection and safe operation management. Based on the analysis of the security threats faced by mobile edge computing, the key problems, and challenges faced by mobile edge computing are summarized and expounded because of four different security subjects, namely, device security, application security, data security, and management security, and the existing security solutions are summarized.

Keywords: mobile edge computing, security threats, security principals, solutions

1. Introduction
With the development of new infrastructure and energy Internet, the use of information technology to meet the needs of energy-efficient operation is increasing [1-2]. The cyber energy system (CES) is a new stage of the development of the energy Internet and a new form of application. It belongs to the cyber-physical systems (CPS) and pays more attention to the regulation and processing of energy information. CES deeply couples the information network and the energy network, which can effectively improve the regional coordination, real-time control, and edge synergy of the basic energy network [3-6]. The big data processing system with cloud computing as the core has low computing power, large necessary network bandwidth, serious delay, and traditional distributed control has the disadvantages of low privacy and security of edge devices, the high energy consumption of data transmission, and a high failure rate of communication nodes[7], has been unable to meet the needs of
In 2014, the European Telecommunications Standards Institute [8] (ETSI) integrated edge computing into the mobile network architecture and proposed mobile edge computing. Mobile edge computing [9] refers to the provision of near-end edge computing services on the side close to the source of user business data to meet the basic needs of the industry in terms of low latency, high bandwidth, security, and privacy protection, such as closer to users Real-time and safe processing of location data, etc. Compared with the previously proposed two technologies of mobile cloud computing (MCC) [10] and content delivery network (CDN), MEC’s distributed deployment scheme can achieve a 5G network well. The demand for decentralization of the architecture improves the flexibility of the network. MEC is deployed near the edge of the network. On the one hand, it can reduce the distance to the user, thereby reducing the transmission delay; on the other hand, MEC will sink the computing and storage capabilities to the middle and downstream, through business awareness and context analysis User characteristics provide mobile users with accurate computing services and business services, so that regional businesses can be resolved locally.

While providing users with high-quality services, mobile edge computing is also facing new security challenges. The on-demand adjacent deployment of MEC exposes the server to the edge of the network, objectively shortening the distance between the attacker and the MEC physical facilities, and provides convenience and opportunities for the attacker to access the MEC physical facilities. At the same time, MEC allows providing services for third-party business applications through open interfaces, facilitating attacks by malicious users. Attackers can invade the MEC server through third-party applications, leading to security threats such as illegal access to the MEC server, node intrusion, data leakage, and information tampering [11]. Besides, due to the limited computing resources, storage resources, and energy resources of the MEC server nodes, attackers can uninstall specific MEC service nodes through malicious uninstallation, resulting in exhaustion of resources and the uninstallation service cannot be performed normally. Moreover, because the MEC server has certain data storage capabilities, malicious nodes may illegally obtain users' private data by hacking into service nodes.

For the entire MEC network ecosystem, security issues are difficult to list. However, security is the bottom line and prerequisite of all network services. In the case of limited network resources, it is still necessary to ensure the security requirements of mobile terminal users to uninstall services. In the existing MEC research, the energy consumption and delay caused by task offloading cannot be ignored. The research on the balance of energy consumption and delay has received great attention [12], and security issues are rarely considered. Therefore, based on the analysis of the security risks faced by mobile edge computing, this article explains several key issues and challenges of mobile edge computing and existing security solutions for two scenarios: a single attacker and multiple attackers.

2. Security Threats
Mobile edge computing can provide users with computing, storage, and transmission resource services at the edge of the network. It can sense real-time business needs and location information of users, and provide convenient and accurate services for edge users. However, mobile edge computing faces many heterogeneous terminal users accessing the network through wireless and other methods, involving wireless sensor networks, mobile computing, and other fields, resulting in mobile edge computing facing many new security threats. In mobile edge computing, attackers may attack different infrastructures in the MEC network architecture, such as user equipment, server nodes, network resources or virtual machines, and even the entire edge data center. This situation is similar to the attack scenario on the Internet. Attackers can attack the network infrastructure from "inside" or "outside", posing security threats to mobile edge computing, as shown in Figure 1. This section discusses the security threats MEC may face.
Figure 1. MEC faces security threats

2.1 Infrastructure security threats
Denial of service (Dos): The network infrastructure and virtual infrastructure in the MEC architecture are different from the security threats of cloud computing. The denial of service attack in the MEC environment only involves the service area in the autonomous domain, but still affects the autonomous domain. Or affect the communication and offloading services in the semi-autonomous domain. Because computing nodes are exposed at the edge of the network, they are vulnerable to attacks by attackers. Attackers can use malicious uninstallation to exhaust the computing and network resources of the service host, causing service nodes to fail. For example, an infected zombie host sends local MEC service nodes in the network. A large number of tasks are offloaded, causing network computing power to be paralyzed.

2.2 Security Threats to Capability Opening
To facilitate users to develop required applications, MEC needs to provide users with a series of open APIs to allow users to access MEC-related data and functions. These APIs facilitate the development and deployment of applications, and at the same time have become targets of attackers. If there is a lack of effective authentication and authentication methods, or the security of the API is not fully tested and verified, then attackers may use counterfeit terminal access, vulnerability attacks, side-channel attacks, and other methods to achieve illegal API calls and illegal The purpose of malicious attacks such as accessing or tampering with user data.

2.3 Virtualization security threats
The mobile edge computing platform MEP itself is based on the deployment of virtualized infrastructure and provides an interface for application discovery and notification. Attackers or malicious applications can perform unauthorized access to the service interface of MEP, intercept or tamper with the communication data between MEP and APP, etc., and implement DDoS attacks on MEP. Attackers can access sensitive data on MEP through malicious applications, steal, tamper with, and delete users' sensitive private data.

2.4 Network service security threats
Once malicious attackers control the mobile edge data center, they can obtain control of the edge data center through permission upgrade, steal or tamper with core information, and even provide other partners with false information (such as fake management information, historical data, etc.), which will lead to a selective denial of service attack and selective information tampering on a particular
offload service, thereby launching targeted attacks in a targeted manner.

2.5 Migration security threats

Before the user moves, the MEC server that provides the computing offloading service is not in the new communication range and needs to re-select a new MEC server, which brings about the service area relocation (SAR) problem [13]. This problem may lead to a man-in-the-middle attack. Attackers take advantage of the opportunity of service area relocation to invade edge network devices to conduct eavesdropping or traffic injection attacks, causing user privacy to be violated, or edge devices to provide wrong migration services.

According to the security threats faced by the above five types of mobile edge computing, the key issues and challenges faced by network security subjects are summarized in Table 1.

Table 1 Security threats to mobile edge computing

| Security subject        | basic settings | capability opening | virtualization | network service | migration security |
|-------------------------|----------------|--------------------|----------------|-----------------|--------------------|
| Equipment safety        | √              |                    | √              |                 | √                  |
| Application security    |                | √                  |                |                 | √                  |
| Data security           |                |                    |                |                 | √                  |
| Management security     |                |                    |                |                 |                    |

3. Countermeasures

For device security risks, it is necessary to consider device access security, user identity authentication, and access control, virtual machine/container security, security audits, interception and response to illegal device access, intrusion, remote management security, etc. The main technical means include: building a trusted hardware infrastructure to achieve safe startup and safe firmware upgrades; disabling local maintenance ports such as server physical interfaces; access authentication for physical devices; timely repair of device vulnerabilities; physical machine/virtual machine operation Enhance system security; deploy virtualized firewalls to enhance isolation between virtualized domains, and ensure the correct configuration of the components of the MEC platform.

For application security risks, security measures can be provided in the entire life cycle of application development, online to operation and maintenance, to ensure security audits before applications are launched, to ensure safe isolation between applications, to repair security vulnerabilities on time, and to intercept and respond to illegal applications The ability of access and intrusion restricts the use of platform resources.

Regarding data security risks, formulate identification standards and data classification standards for sensitive data in industrial networks, and clarify desensitization requirements and classification rules. The key data in the industrial network is stored hierarchically, and the data is stored according to specific hierarchical principles. At the same time, encryption processing for sensitive and important data can prevent data centers from being attacked and ensure data security. In the process of data encryption and access, follow the principle of "minimal authorization", formulate a reliable authority strategy, and divide the node authority in edge computing. Each node uses a different key to ensure the independence of the node. After the information of one node is leaked, it will have little impact on other nodes.

For the management of safety risks, corresponding measures can be taken in the establishment of a safety management system, personnel safety awareness education and training, safety assessment, operation inspection and maintenance, emergency response process plan, supply chain safety management, etc., including appropriate authorization of administrators and real-time audits, Auditing suppliers, establishing application security inspection and auditing procedures, promptly pushing upgrade packages based on integrity and signature verification, formulating emergency response plans and regular drills, formulating code development specifications, and requiring software suppliers to follow and formulate safe operations Maintain management procedures, build a team, and provide
tenant-specific business operation and maintenance and security management for the MEC platform.

4. Conclusion
Mobile edge computing, as a data-driven service technology, promotes computing, storage, and local applications to the edge of the network, significantly improving the traditional communication network connection and resource utilization with terminal devices, thereby reducing computing latency and increasing computing success rate. As an excellent practice of CES integration, MEC brings about dual changes in energy technology and industry. At the same time, the potential security risks of its deployment applications also bring new challenges to application development and existing network security regulatory policies.

This article introduces and analyzes the security risks faced by MEC deployment applications from four aspects: equipment security, application security, data security, and management security, and proposes countermeasures, hoping to provide security for relevant organizations and personnel when deploying the MEC platform. Evaluation and deployment of security means provide certain reference and reference. In the future, it is necessary to strengthen the response to potential risks, from innovating safety supervision methods, strengthening technical risk research, and attaching importance to safety assessment, to realize the healthy and orderly development and application of MEC.

References
[1] Liu Yanhong, Huang Xuetao, Shi Bohan. China’s new infrastructure construction: concepts, current situations and problems[J]. Journal of Beijing University of Technology (Social Sciences Edition), 2020, 20(6): 1-12(in Chinese).
[2] Shen Chen, JIA Mengshuo, CHEN Ying, et al. Digital twin of the energy Internet and its application[J]. Journal of Global Energy Interconnection, 2020, 3(1): 1-13(in Chinese).
[3] Lian Xianglong, Zhang Wenhao, Qian Tong, et al. Vulnerability assessment of cyber-physical power system considering cyber nodes failure[J]. Journal of Global Energy Interconnection, 2019, 2(6): 523-529(in Chinese).
[4] Jia Hongjie, Wang Dan, Xu Xianlong, et al. Research on some key problems related to integrated energy systems[J]. Automation of Electric Power Systems, 2015, 39(7): 198-207(in Chinese).
[5] Sun Qiuye, Hu Jingwei, Zhang Huaguang. Modeling and application of we-energy in energy Internet[J]. Scientia Sinica (Information is), 2018, 48(10): 1409-1429(in Chinese).
[6] Hu Jie, Sun Qiuye, Hu Jingwei, et al. Three-dimensional self-mutual-group collaborative optimization method for Information-energy systems[J]. Journal of Global Energy Interconnection, 2019, 2(5): 457-465(in Chinese).
[7] Shi Weisong, Sun Hui, Cao Jie, et al. Edge computing: an emerging computing model for the Internet of Everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924(in Chinese).
[8] Hu Y C, Patel M, et al. Mobile edge computing—a key technology towards 5G[J]. ETSI White Paper, 2015,11(11): 1-16.
[9] Mach P, Becvar Z. Mobile edge computing: a survey on architecture and computation offloading[J]. IEEE Communications Surveys & Tutorials, 2017, PP(99):1-1.
[10] Wang Y, Chen I R, Wang D C. A survey of mobile cloud computing applications: perspectives and challenges[J]. Wireless Personal Communications, 2015, 80(4): 1607-1623.
[11] Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, 78: 680-698.
[12] No Ak J, Kim Y, Lee J, et al. DREAM: dynamic resource and task allocation for energy minimization in mobile cloud systems[J]. IEEE J Sel Areas Commun, 2015, 33(15): 2510-2523.
[13] Ford R, Sridharan A, Margolies R, et al. Provisioning low latency, resilient mobile edge clouds for 5G[C]/2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2017: 169-174.