Hindawi
Security and Communication Networks
Volume 2021, Article ID 8846239, 8 pages
https://doi.org/10.1155/2021/8846239

WILEY | Hindawi

Review Article

A Survey on Secure Deployment of Mobile Services in Edge Computing

Mengmeng Cui,[1] **Yiming Fei**,[2] **and Yin Liu**[3]

[1]*School of Applied Technology, Nanjing University of Information Science & Technology, Nanjing 21000, China*
[2]*School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 21000, China*
[3]*Yunnan Air Traffic Mannagment Sub-Bureau, CAAC, Changshui International Airport, Kunming 650000, China*

Correspondence should be addressed to Yiming Fei; feiyiming@nuist.edu.cn

Received 10 August 2020; Revised 19 October 2020; Accepted 17 December 2020; Published 4 January 2021

Academic Editor: David Megías Jiménez

Mobile edge computing (MEC) is an emerging technology that is recognized as a key to 5G networks. Because MEC provides an IT service environment and cloud-computing services at the edge of the mobile network, researchers hope to use MEC for secure service deployment, such as Internet of vehicles, Internet of Things (IoT), and autonomous vehicles. Because of the characteristics of MEC which do not have terminal servers, it tends to be deployed on the edge of networks. However, there are few related works that systematically introduce the deployment of MEC. Also, secure service deployment frameworks with MEC are even rare. For this reason, we have conducted a comprehensive and concrete survey of recent research studies on secure deployment. Although numerous research studies and experiments about MEC service deployment have been conducted, there are few systematic summaries that conclude basic concepts and development strategies about secure service deployment of commercial MEC. To make up for the gap, a detailed and complete survey about relative achievements is presented.

1. Introduction

In 2013, MEC was first introduced when Nokia Siemens and IBM developed an MEC platform where applications can run directly. Later, MEC was standardized by the European Telecommunications Standards Institute (ETSI) and Industry Specification Group (ISG). Also, European 5G Infrastructure Public Private Partnership regards MEC as a prime emerging technology for 5G networks [1].

In recent years, wearable devices, sensors, and a lot of devices of internet of things (IoT) such as wearable devices become more universal [2]. According to the research of Ericsson, it is estimated that 32 billion terminal devices will be connected to the mobile network by 2030 [3]. Due to the explosive growth of the amount of terminal equipment and data, it is not hard to see that online service providers will face significant challenges in securing reliable and low-latency connections for terminal users [4]. To solve the problems, researchers decide to deploy computation resources, network control functions, and cached data near microbasic stations and macrobasic stations. This model is called mobile edge computing [4]. Usually, edge servers cover specific geographic areas so that users can connect to them easily. A large number of edge servers will be deployed in a distributed manner so that they can cover different geographic areas. Their coverage often overlaps, which may lead to wasting resources.

Because the coverage of MEC is not large enough, operators have to cost more to serve the users. Furthermore, sometimes user requests cannot be processed by the closest edge servers, and how to transfer them to another server is also a problem [5]. On the other hand, problems such as the risk of user data leakage and safety of terminal devices are urgent to be solved.

Because the above problems are caused by service deployment, this article refers to the problems as secure deployment of mobile services in edge computing. Secure deployment of mobile services has been taken into consideration in three aspects as follows.

1.1. MEC Service Deployment. Because edge computing is considered as one of the key technologies to meet low latency, mission-critical, and IoT services requirements in the future, MEC service deployment is required to be flexible and efficient. Also, it is required to be secure and easy to maintain. Services which are provided to users need deploying in the MEC servers themselves. That is why MEC servers can handle users' requests correctly when the MEC server is deployed correctly. If requests are sent to any MEC server, the receiving MEC server will not deploy the service themselves and send it to the neighboring one. Moreover, if there are a lot of neighboring MEC nodes which are running one requested service, the one of them that is chosen must ensure the QoS of the service. We make a model which is named round trip time (RTT) between mobile devices and MEC servers so that we can choose the best destination node. On the other hand, there may be a strain on processing time if a few mobile devices access the same MEC for services. Therefore, the service discovery protocol needs to consider the processing burden on MEC [6].

MEC is an approach complementary to network functions virtualization (NFV) based on a virtualized platform. In fact, while NVF is focused on network functions, the MEC framework allows applications to run at the edge of network. The infrastructure from MEC to NFV or functions on networks is quite similar; thus, in order to enable operators to benefit from their investment as much as possible, it will be helpful to reuse infrastructure management of NFV which hosts VNFs (virtual network functions) and MEC applications on the same platform [7].

MEC service deployment allows operators to run core services near the end-devices. And it enables users and content providers to serve and adjust context-aware services. To meet the requirements of 5G and fill the huge requirements of users and operators in the future, MEC needs to be deployed. Also, the correct deployment of MEC can solve the problem of lack of flexibility [8].

1.2. Computation Offloading. Generally speaking, there are three scenarios for offloading: local execution means the whole computation is done locally and does not transfer to MEC [9]. Full offloading means contrary to local execution, the whole computation is offloaded completely, so partial offloading means a part of computation is offloaded while the rest is done locally [10]. Correct and appropriate service deployment can reduce the pressure of computation offloading. Nowadays, billions of mobile devices are connected to the Internet. Because researchers usually assume that mobile computation offloading relies on a central cloud, it is a huge challenge for limited computation on the central cloud [11]. So computation offloading is a very pivotal technology for MEC [12]. Computation offloading and resource allocation are both parts of the universal system, and they both contribute to user experience, which cannot be guaranteed by the optimization of one single segment [13].

1.3. Data Placement. Because of the rapid growth of MEC services, major service providers now use a lot of geographically dispersed data centers so that the users can get better service experiences. In this way, users can avoid waiting a long time for data transmission [14]. Mobile devices produce a lot of data, which is stored for analysis. However, due to the limited storage of mobile devices, data need to be placed on remote data centers to process further [15]. Generally, data placement is divided into two parts which are random placement and planned placement. In random placement, the sensors are randomly distributed, and in planned placement, the sensors are deployed selectively [16]. The specific requirements of a good strategy data placement are as follows: (1) the scientific workflow structure is complex and datasets are large. Therefore, the data placement strategy should ensure high cohesion within the data center and low coupling among different data centers, thus reducing data transfer time between data centers that combine edge computing and cloud computing. (2) For security reasons, private datasets should be stored in the edge data center. Due to the limited storage capacity of edge data centers, some datasets must be transferred across different data centers. Placing low latency data sets with limited bandwidth and fixed private data sets is a challenge [17].

The organizational structure of the article is as follows: first of all, we introduce the basic concepts and definitions of mobile devices and MEC. Next, we generally overview secure deployment frameworks with commercial MEC and propose a new framework. Meanwhile, we introduce some methods and technologies of deployment. Then, we point out some challenges of secure deployment. Moreover, we provide some solutions to fill these gaps. And then, we discuss some open issues and problems. At last, we make a rough summary of the secure deployment of mobile service.

2. Basic Concepts and Definitions

In this section, we review the basic concepts and definitions of MEC.

2.1. Service Deployment. Usually, service deployment is based on virtualization technology. In other words, a deployed service is a VM or a collection of VMs. The service is composed of functional and nonfunctional requirements for one deployment target [18]. The deployment core of MEC is NFV, software-defined network (SDN), and cloud computing technology. NFV is a way to design, deploy, and manage network services. The main idea of NFV is to decouple the physical network devices from the functionality running on it [19]. Software-defined networks (SDNs) are controlled programmatically. Network state is managed by logically centralized control programs with a global network view and written directly to the switch for using standard API [20].

2.2. Mobile Edge Computing. As shown in Figure 1, data of terminal devices, including but not limited to mobile devices and vehicles, are transferred to MEC originally, then MEC will complete most of the computation tasks, and the remaining unsolvable are transferred to the cloud. The basic idea of MEC is to "sink" the functions of the central cloud

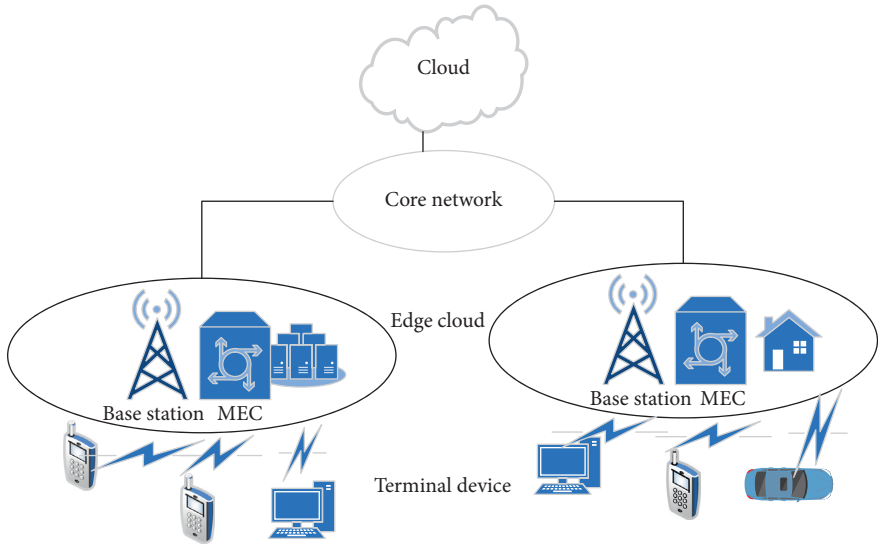

Figure 1: The architecture of MEC.

data center to the network edge which is closer to the mobile end users, and operators deploy MEC near the users to provide necessary computing, storage, and other services for the mobile end users. Though the research in MEC is not detailed and rigorous, some researchers have proposed MEC definitions that an open cloud platform which uses some end-user clients is located on the mobile edge to perform a massive amount of real-time storage (rather than stored primarily in cloud data centers) [21]. MEC can offer a service environment that has the advantages of ultralow latency, high-bandwidth, and direct access to real-time network information. And it is closed to subscribers [22]. Unlike the centralized cloud servers or peer-to-peer mobile devices, the network operators usually manage MEC locally. The generic computing resources within the mobile edge hosts are virtualized and are exposed via application program interfaces (APIs). In this way, both users and operator applications can access it.

3. Secure Service Deployment Framework with Commercial MEC

In this section, we sort out several proposed frameworks about secure service deployment at first. And then, we put forward ours. The relative architectures and their features are listed in Table 1 [32].

3.1. Surveys on the Proposed Framework. Deng et al. [33] proposed a scheme of computation offloading to solve the scalability problems. The utility function of users is to make unloading decisions in turn according to the current interference environment and adjust the number of unloading users according to the estimated delay. Therefore, researchers developed the offloading interaction among multiple users as a sequential offloading decision game to solve the problems of scale ability. Users' utility in terms of experienced wait times and energy consumption is huge. The mobile users make the uninstall decision which is based on the following sequence in the current interference environment and adjusts the offloading users based on the estimated delay. They proposed a way called Nash. A Nash equilibrium is a state of a noncooperative game where no player can improve its utility by changing its strategy if the other players maintain their current strategies. The mobile device users at the equilibrium can achieve a mutually satisfactory solution and no user has the incentive to unilaterally deviate. Dynamic games which are equivalent with perfect information have a pure strategy Nash equilibrium. As the number of users increases, the proposed algorithm offloads the selection task to ensure the user experience. And the network made up of N small cells is shown in Figure 2; mobile devices upload data to MEC servers through nodes which are on the edge networks. One MEC server can provide service for many terminal devices so that operators can save cost-effectively.

Due to computation offloading, extralatency, and network load, Verbelen et al. [34] presented algorithms to partition a software application, composed of a number of components which has four parts in the cloud with different capacities while minimizing the communication cost between the components. They presented a multilevel KL-based algorithm as a fast partitioner. It allows real-time deployment calculations. The solution quality is improved by simulated annealing, but the cost is computation capacity. They used the way which is called computing the graph partitioning problem to assign computation offloading. Then, their goal is to execute all these tasks as fast as possible, thus minimizing the execution time of the slowest node.

Xiang et al. [35] proposed a joint offloading framework, which uses the characteristics of multiple applications to bundle offloading requests of code, thus saving additional energy. By sending code offloading requests in the form of bundles, the time for network interfaces to maintain a high

Table 1: Comparisons of frameworks based on different ways.

Properties	[23]	[24]	[25]	[26]	[27]	[28]	[29]	[30]	[31]
Minimum execution time	Y	N	Y	N	N	N	N	N/A	N/A
Network latency	L	H	N/A	L	L	M	L	N/A	N/A
Transmission delay	M	H	H	N/A	N/A	M	M	N/A	N/A
Preexecution delay	H	N/A	H	L	N/A	N/A	H	L	H
Maximum privacy and security	N/A	N	N	N	N	Y	Y	N/A	N/A
Offloading overhead	H	H	H	N/A	N/A	H	H	N/A	N/A

Y = yes; N = no; H = high; M = medium; L = low; N/A = not applicable.

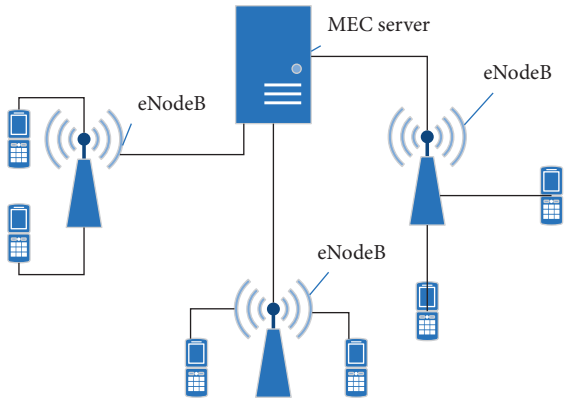

Figure 2: The scenario of multicell MEC.

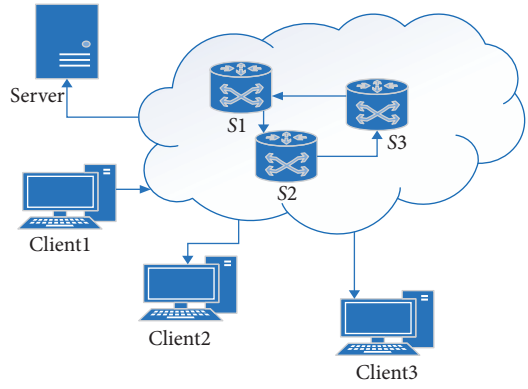

Figure 3: A communication instance of CDN-SDN.

power state is reduced, thus saving energy on mobile devices. The joint offloading problem is reduced to a joint optimization problem aiming at minimizing the response time and energy cost. Although the middleware framework reduces interaction latency, other elements, such as consumption graph modeling, optimal segmentation algorithms, two-step dynamic partitioning analysis, and intensive configuration, consume computing resources for mobile devices. Therefore, the computation-intensive nature of the framework increases the overall execution time of the application, hindering the vision of achieving seamless application execution.

Because many researchers have proposed their own frameworks, further comparisons of some frameworks which are based on different ways are given in Table 1.

3.2. A Framework of Commercial MEC. The idea of content delivery network (CDN) was first proposed in 1998, in which the content would be replicated on several proxy servers that were geographically closer to the user, as shown in Figure 3. As shown in Figure 3, each client will store the content that it originally requested from the server/controller, which will be provided to neighboring clients when the same content is requested. Distributing servers in multiple locations is the most common way to promote high performance and scalability [36]. CDN still faces the problems of limited resources as servers cannot meet the increasing demands of users. The deployment of servers depends on the location, such as in order to find the right location with the required capacity and then invest in the cost of deployment and installation [37].

Now video clips apps and major video websites are popular. As a result, users' habits of watching videos have also changed. Although all major video websites have chosen CDN services to provide users with a good video viewing experience, the current user interface architecture of a mobile communication network still has some inherent flaws. For example, users in the same city or county have the same requests such as watching the same film or downloading a document. All the video content needs to access the CDN service nodes of the video website on the backbone network through the provincial core network exits, which brings huge bandwidth pressure on the backhaul link.

Service providers can set up CDN at the mobile edge so that edge CDN can store popular videos. The differences between traditional CDN and CDN based on MEC are shown in Table 2. By requesting the hot content stored in the edge CDN, the hot content can be sent to users from the edge of the mobile network without the need to transmit the content from the central CDN node through the mobile core network. The hot content caching mechanism should be predefined or support dynamic updates to meet user requests. As shown in Figure 4, mobile devices usually need to transfer data from base station to MEC. With MEC and edge CDN, devices can process data quickly instead of processing data from central CDN or cloud. In this way, data processing will be greatly accelerated and data transfer can speed up.

4. Challenges of Secure Service Deployment

With the secure deployment of commercial MEC, many challenges need to be solved. Table 3 summarizes some challenges and solutions [38].

Table 2: Comparison between CDN based on MEC and traditional CDN.

Comparison	Traditional CDN	CDN based on MEC
Geographical location	Far from users	Closed to users
Receiving and sending resources	Weak ability	Strong ability
Coverage area	Small coverage area	Large coverage area
Kinds of service	Few kinds	More kinds
Cost	Low	High

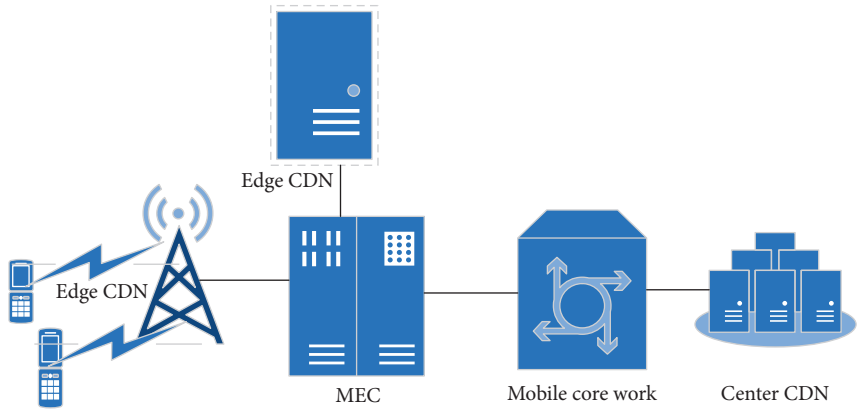

Figure 4: An edge CDN framework based on MEC.

Table 3: Challenges and methods of commercial MEC.

Challenges	Reference	Method used	Contribution
Risk of user data leakage	[42]	A VLAN based on security architecture	Increase protection to prevent accidental data leakage
Secure risk of data transmission	[50]	2D-DWT-1L or 2D-DWT-2L steganography	Enable to hide the confidential patient's data and transfer data secretly
Security of terminal device	[51]	A terminal lightweight anonymous security communication scheme	Support access authentication for massive terminal devices

4.1. Risk of User Data Leakage. In the course of doing business with commercial MEC, sometimes sensitive data must be handed over to supposedly third parties. In this background, it is necessary for researchers to propose a method to detect when the distributor's sensitive data have been leaked and fill this loophole.

Vaidya and Khobragade [39] used an algorithm which is called RSA encryption technology to ensure the security of user data. RSA can ensure coded data through distributed verification. The researchers used the method of reserving the RSA token properties so that they can address the problem of ensuring cloud data storage correction. Considering that the key calculation function belongs to a universal hash function family, researchers choose to store RSA technology, which can be completely integrated with the verification of erasure-coded data. Then, it shows how to verify the correctness of the storage and determine if the server is behaving abnormally.

Yu et al. [40] presented a data leakage prevention model called CBDLP. CBDLP consists of two parts, one is the training phase and the other is the detection phase. During the training phase, the training documents are divided into different clusters. In the detection phase, the documents are matched with the cluster diagram, respectively. So far, a number of specified commercial DLP solutions have reduced the risk of most accidental leaks [41].

4.2. Secure Risk of Data Transmission. For commercial MEC, the information transmission security is crucially important. The hackers take the IP addresses illegally so that they can impersonate other legitimate users to affect the security and stability of communication data transmission. Sometimes, the hackers send a large number of instructions and data to the terminal of the mobile device, which makes the communication network appear to be blocked negatively. Due to data transmission via the wireless network, the hackers analyze the frequency so that they can complete wiretapping work [42]. In severe cases, communication data will be tampered by hackers, causing a negative phenomenon of data loss.

To solve similar problems, Papadimitratos et al. [43] proposed an overview of the secure message transmission (SMT) protocol. SMT is used to establish a security association (SA) between the two terminal communication nodes: the source and the destination. Since the related nodes are chosen to adopt a secure communication scheme, the authentication capability between them is essential. For

example, the trust relationship can be instantiated by knowing the public key at the other end of the communication. However, no terminal node needs to be safely associated with any remaining network nodes. Therefore, SMT does not need to perform encryption operations on these intermediate nodes.

Okaya and Ozdemir also proposed a novel named secure data aggregation (SDA) protocol for fog computing-based SGs (FCSG). Through employing homomorphic encryption, the proposed protocol not only ensures data privacy but also reduces a large of data which is stored in the cloud servers. Moreover, having related servers reduces server response time and creates less data traffic compared to cloud-based smart grids (SGs) [44].

4.3. Security of Terminal Device. At present, most users of mobile cloud services use cloud services without security protection. For example, private data such as user address books, text messages, and memos of mobile terminal devices are directly synchronized with the cloud platform by default. These private data are in the cloud, so that operators can call users' data easily on the platform. With the widespread use of mobile terminal applications, operators can easily capture the user's location information which not only includes the user's closest geographic location but also deduce the user's potential location privacy. It is dangerous for personal privacy.

Researchers proposed a dynamic path quorum system for mobile hoc networks and designed a dynamic path quorum generation algorithm. And they proposed a distributed access control mechanism for mobile hoc networks based on the quorum system, which is different from the traditional one depending on a single node itself. Compared with the access control mechanism, this access control mechanism has the stronger antiattack ability and higher reliability and effectively improve the resource sharing and protection level of the mobile hoc network [45].

5. Open Issues and Challenges

According to the research studies and experiments that have been discussed above, a few crucial open issues on secure deployment of mobile services in edge computing are concluded.

5.1. Privacy Security. Although the hype around MEC tends to encourage people to think that it is a universal panacea, promoters usually ignore the privacy security caused by the MEC. When users use services provided by MEC, their location information may be exposed. For example, the popularity of in-vehicle MEC may lead to misuse of vehicle location information. The service provider may monitor the user's trajectory without being allowed by users [46]. So the privacy security of commercial MEC must be solved urgently. Although many existing studies treat that information security and information privacy threats separately, we believe that only studying information privacy is not enough and there is a lot of related work to be done [47].

5.2. Data Transfer. The evolution of new services and the growth of information on the Internet has caused the origin of ideas, concepts, and paradigms. However, traditional network infrastructure requiring advanced network policies and configuration protocols are inefficient. And it supports significant limitations, high levels of scalability, and high amount of traffic [48]. As known to all, 5G is a key driver of MEC. It means that speed and stability of transfer play an important role in MEC. However, due to different geographical locations, receiving, and sending equipment, high-quality service of MEC is hard to be ensured. In other words, the transfer of data is required to promote the joint optimization of commercial MEC.

5.3. Access Control. Due to the outsourcing feature of edge computing, if there are no effective authentication mechanisms, any malicious users with an unauthorized identity may abuse the service resources at the edge. This leads to a huge security challenge for secure access control systems. For example, virtualized resources of edge server clouds can be accessed and modified by edge devices if they have certain privileges [49].

6. Conclusion

Commercial MEC will play an important role in daily life in the near future. MEC has excellent business prospects. It has a great influence on the society. Operators can combine different industry application scenarios, mature 4G networks, and stronger 5G networks to actively practice the deployment and application of MEC. Predictably, when the commercial MEC framework is completed, it is of great benefit to the city and people.

In this paper, a comprehensive and detailed survey on secure deployment of mobile services in edge computing is presented. Firstly, this paper reviews the basic driving force of conducting the survey about MEC. And then, the related concepts and definitions are introduced. Afterward, this paper provides an overview of frameworks and crucial techniques. Finally, several open issues are enumerated to guide our future research directions. In a word, this survey is presented to promote further progress of commercial MEC.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] N. Abbas, Y. Zhang, Y. Taherkordi, and T. Skeie, "Mobile Edge Computing: a Survey architecture, applications, approaches and challenges," *IEEE Internet of Things Journal*, vol. 5, pp. 454-455, 2018.

[2] X. Xu, X. Liu, Z. Xu, F. Dai, X. Zhang, and L. Qi, "Trust-oriented IoT service placement for smart cities in edge

computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4084–4091, 2020.
[3] A. B. Ericsson, "Ericsson mobility report 2017," 2017.
[4] X. Xu, R. Mo, F. Dai, W. Lin, S. Wan, and W. Dou, "Dynamic resource provisioning with fault tolerance for data-intensive meteorological workflows in cloud," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6172–6181, 2020.
[5] Y. He, J. Ren, G. Yu, and Y. Cai, "D2D communications meet mobile edge computing for enhanced computation capacity in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, 2019.
[6] T. D. Nguyen, E. N. Huh, and M. Jo, "Decentralized and revised content-centric networking-based service deployment and discovery platform in mobile edge computing for IoT devices," *IEEE Internet of Things Journal*, vol. 6, pp. 6142–6175, 2019.
[7] Y. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing: a key technology towards 5G," *ETSI (European Telecommunications Standards Institute)*, vol. 9, 2015.
[8] R. Solozabal, "Exploitation of mobile edge computing in 5G distributed mission-critical push-to-talk service deployment," *IEEE Access*, vol. 6, 2015.
[9] X. Xu, X. Zhang, X. Liu, J. Jiang, L. Qi, and M. Z. A. Bhuiyan, "Adaptive computation offloading with edge for 5G-envisioned Internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 1, 2020.
[10] P. Mach and Z. Becvar, "Mobile edge computing: a survey on architecture and computation offloading," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 1628–1656, 2017.
[11] Y. Zhu, Y. Hu, and A. Schmeink, "Delay minimization offloading for interdependent tasks in energy-aware cooperative MEC networks," *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 15, pp. 1–6, 2019.
[12] C. You, K. Huang, H. Chae, and B. H. Kim, "IEEE transactions on wireless communications," *IEEE*, vol. 16, pp. 1397–1411, 2017.
[13] C. Wang, C. Liang, F. R. Yu, Q. Chen, and L. Tang, "Computation offloading and resource allocation in wireless cellular networks with mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 4924–4938, 2017.
[14] S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, and A. WolmanVolley, "Automated data placement for geo-distributed cloud services sharad," *Microsoft Research*, vol. 16, 2010.
[15] X. Xu, B. Shen, X. Yin et al., "Edge server quantification and placement for offloading social media services in industrial cognitive IoV," *IEEE Transactions on Industrial Informatics*, vol. 16, 2020.
[16] X. Xu, S. Fu, L. Qi et al., "An IoT-Oriented data placement method with privacy preservation in cloud environment," *Journal of Network and Computer Applications*, vol. 124, pp. 148–157, 2018.
[17] B. Lin, F. Zhu, J. Zhang et al., "A time-driven data placement strategy for a scientific workflow combining edge computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4254–4265, 2019.
[18] W. Li, P. Svard, J. Tordsson, and E. Elmroth, "A general approach to service deployment in cloud environments," 2012.
[19] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: state-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, 2015.
[20] N. Handigol, "Where is the debugger for my software-defined network?" 2015.
[21] E. Ahmed and M. H. Rehmani, "Mobile edge computing: opportunities, solutions, and challenges," *Future Generation Computer Systems*, vol. 23, 2016.
[22] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile edge computing: progress and challenges," *Future Generation Computer Systems*, vol. 5, p. 3, 2016.
[23] T. Verbelen, P. Simoens, F. De Turck, and B. Dhoedt, "Aiolos: middleware for improving mobile application performance through cyber foraging," *Journal of Systems and Software*, vol. 85, no. 11, pp. 2629–2639, 2012.
[24] X. Zhang, S. Jeong, A. Kunjithapatham, and S. Gibbs, "Towards an elastic application model for augmenting computing capabilities of mobile platforms," 2010.
[25] S. Kosta, A. Aucinas, P. Hui, R. Mortier, and X. Zhang, "Thinkair: dynamic resource allocation and parallel execution in the cloud for mobile code offloading," 2012.
[26] E. Koukoumidis, D. Lymberopoulos, K. Strauss, J. Liu, and D. Burger, "Pocket cloudlets," *ACM SIGARCH Computer Architecture News*, vol. 39, no. 1, pp. 171–184, 2011.
[27] A. Dou, V. Kalogeraki, D. Gunopulos, T. Mielikainen, and V. H. Tuulos, "Misco: a mapreduce framework for mobile systems," 2010.
[28] D. Kovachev, Y. Cao, and R. Klamma, "Augmenting pervasive environments with an xmpp-based mobile cloud middleware," in *Mobile Computing, Applications, and Services*Springer, Berlin, Germany, 2010.
[29] D. Kovachev, T. Yu, and R. Klamma, "Adaptive computation offloading from mobile devices into the cloud," 2012.
[30] S. Goyal and J. Carter, "A lightweight secure cyber foraging infrastructure for resource-constrained devices," 2004.
[31] D. Fesehaye, Y. Gao, K. Nahrstedt, and G. Wang, "Impact of cloudlets on interactive mobile cloud applications," 2012.
[32] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: fog computing, cloudlet and mobile edge computing," 2017.
[33] M. Deng, H. Tian, and X. Lyu, "Adaptive sequential offloading game for multi-cell Mobile Edge Computing," 2016.
[34] T. Verbelen, T. Stevens, F. De Turck, and B. Dhoedt, "Graph partitioning algorithms for optimizing software deployment in mobile cloud computing," *Future Generation Computer Systems*, vol. 29, no. 2, pp. 451–459, 2013.
[35] L. Xiang, S. Ye, Y. Feng, B. Li, and B. Li, "Ready, Set, Go: coalesced offloading from mobile devices to the cloud," *IEEE*, vol. 7, p. 8, 2014.
[36] J. D. Gagliardi, T. S. Munger, and D. W. Ploesser, "Content Delivery network," *U.S. Patent*, vol. 8, 2012.
[37] J. Chandrakanth, P. Chollangi, and C. H. Lung, "Content distribution networks using software defined networks," *IEEE*, vol. 11, p. 30, 2015.
[38] S. Shahzadi, "Multi-access edge computing: open issues, challenges and future perspectives," *Journal of Cloud Computing*, vol. 12, p. 21, 2017.
[39] C. Vaidya and P. Khobragade, "Data security in cloud computing," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 12, 2015.
[40] X. Yu, Z. Tian, J. Qiu, and F. Jiang, "A data leakage prevention method based on the reduction of confidential and context terms for smart mobile devices," *Wireless Communications and Mobile Computing*, vol. 23, 2018.
[41] R. Rauscher and R. Acharya, "A network security architecture to reduce the risk of data leakage for health care organizations," 2014.

[42] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, "Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain," *ACM Transactions on Internet Technology*, vol. 23, 2020.

[43] P. Papadimitratos and Zygmun, "Secure data transmission in mobile ad hoc networks," *ACM Workshop on Wireless Security*, vol. 9, pp. 41–54, 2013.

[44] F. Y. Okay and S. Ozdemir, "A secure data aggregation protocol for fog computing based smart grids," *IEEE*, vol. 7, p. 7, 2018.

[45] R. Li, X. Dong, X. Gu, W. Zhou, and C. Wang, "Overview of the data security and privacy-preserving of mobile cloud services," *Journal on Communications*, vol. 12, 2013.

[46] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, "Joint optimization of offloading utility and privacy for edge computing enabled IoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2622–2629, 2020.

[47] E. Robert, "The mobile privacy-security knowledge gap model: understanding behaviors," *Destination Area: Integrated Security (IS)*, vol. 4, 2017.

[48] G. A. Mensah, C. O. Johnson, G. Addolorato et al., "Global burden of cardiovascular diseases and risk factors, 1990-2019: update from the GBD 2019 study," *Journal of the American College of Cardiology*, vol. 34, 2020.

[49] J. Zhang, Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: survey and open issues," *IEEE Access*, vol. 6, 2018.

[50] M. Elhoseny, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 3, p. 21, 2018.

[51] L. Chen, Z. Liu, and Z. Wang, "Research on heterogeneous terminal security access technology in edge computing scenario," *2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, vol. 10, p. 7, 2019.