7-1-2023

Edge Computing: Applications and Security Features

India Keene

Haiyan Huang

EDGE COMPUTING: APPLICATIONS AND SECURITY FEATURES

India S. Keene
Amazon AWS
india.keene@gmail.com

Haiyan Huang
Flagler College
hhuang@flagler.edu

ABSTRACT

Edge computing is an extension of cloud computing and is capable of providing storage, data processing, and intelligence at the edge of the network that is closer to the IoT devices and mobile applications. Compared with traditional cloud computing, edge computing can provide scalable, quality services with low latency, low bandwidth cost, low energy consumption, and real-time data processing due to its proximity to the end users. This paper provides a review of edge computing architecture, key technologies, real-world applications, and discusses the security challenges and opportunities related to edge computing.

Keywords

Edge computing, cloudlet, mobile edge computing (MEC), 5G, fog computing, applications, security

INTRODUCTION

As the number of internet-connected devices and mobile applications continues to grow exponentially, technologists have been searching for ways to ensure low latency, high bandwidth, location awareness, and real-time services for all these devices and applications (Ai et al., 2018). In 2016, the number of devices connected to the Internet was estimated to be 17.1 billion. It was estimated the number would exceed 50 billion by 2020 (Cao et al., 2020). Compared to thick clients and server machines, those mobile devices and Internet of Things (IoT) are intrinsically "resource-poor" computational devices with limited processing powers (Satyanarayanan et al., 2009). Resource-intensive, high-performance cloud servers have been utilized to provide storage, analytical, and decision-making services to the mobile devices and IoT sensors. Cloud computing is well known for its capability of pooling computing resources and offering on-demand services to the end-users.

Despite cloud computing technology continues to evolve and improve, latency due to the bandwidth and the distance of data centers has remained as major obstacles for cloud computing to provide timely and effective data processing services to IoT applications. With the traditional cloud computing, all data is transferred to centralized data centers to be processed. Those cloud data centers are usually too distant from the end users to process data in real time. The immense number of IoT devices has made it difficult for traditional big data cloud computing to keep up with the necessary real-time data transmission and processing speed required for those mobile and IoT applications. Additionally, IoT devices collect zettabytes (ZBs) of personal data, which is at risk when being uploaded to the remote clouds. Furthermore, cloud centers can become overwhelmed when it comes to handle the energy consumption required for responding to so many devices (Cao et al., 2020). Edge computing, which is designed to provide data storage and processing at the "edge" of the networks, has emerged as an alternative solution (Satyanarayanan et al., 2009; Satyanarayanan, 2017).

This paper provides a summary of the edge computing architecture and three major approaches. Then it presents several real-world applications of the edge computing technologies to showcase its benefits. Challenges and opportunities associated with the security issues of edge computing are discussed at the end of the paper.

ARCHITECTURE AND MAIN APPROACHES OF EDGE COMPUTING

According to Satyanarayanan (2017) and Cao et al. (2020), edge computing can be described as a new computing paradigm and model that processes data, deploys computing resources, and provides intelligent services at the edge of the networks, closer to sensors or mobile devices where data are produced and gathered. Researchers emphasized that edge computing is not a replacement of cloud computing, rather, it is a complementary extension to cloud computing (Cao et al., 2020), or "an advanced version of cloud computing" (Khan et al., 2019).

Figure 1 shows a typical edge computing architecture that is composed of three layers (Parikh et al., 2019; Cao et al., 2020; Rong et al., 2021; Chen et al., 2022). The device layer includes all types of mobile, smart and IoT devices that collect and consume data. Raw data collected at the device layer is transferred to the edge layer, which consists of edge nodes such as routers, switches, end-user devices and virtual machines. The edge layer sits in between of the device layer and the cloud layer. On the one hand, the edge layer provides real-time data processing and operational services to those devices in the device layer. On the other hand, the edge layer uploads the processed data to the high-performances servers located in the cloud layer, which are responsible for data integration, data warehousing, big data processing, and complex data analytics tasks. Satyanarayanan

(2017) suggested that in edge computing, the proximity of the edge nodes to the devices plays a vital role to deliver scalable, low latency, high responsiveness services to mobile applications and IoT devices.

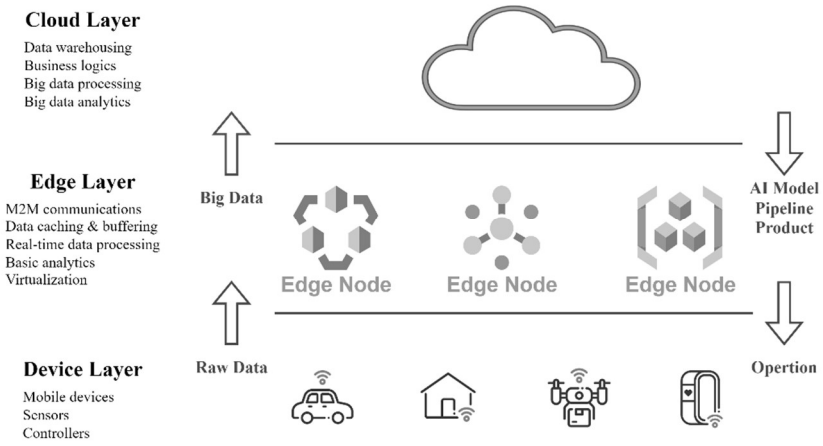

Figure 1. Three-Layer Architecture of Edge Computing

Over the past decade, the published research on edge computing has focused on three main approaches: cloudlets, mobile edge computing (MEC), and fog computing (Shahzadi et al., 2017; Ai et al., 2018; Khan et al., 2019). Ai et al. (2018) provided a comprehensive review about those three edge computing platforms and compared them with respect to organization, driving forces, motivations, and their openness features. Khan et al. (2019) surveyed and analyzed more than 50 published papers on cloudlets, MEC, and fog computing, and raised several challenging issues related to the deployment and adoption of edge computing. Cao et al. (2020) made a side-by-side comparison between cloud computing and edge computing and summarized several edge computing models and key enabling technologies.

Satyanarayanan et al. (2009) defined cloudlet as a trusted, mobility-enhanced, resource-rich computer or clusters of computing devices that are well-connected to the Internet and available for use as services by mobile devices in the close proximity. To enable cloudlet-based edge computing, a mobile device needs to locate and pick an appropriate nearby cloudlet, a cloudlet needs to be flexible because its association with mobile devices will be dynamic, and a virtual machine (VM) handoff technology needs to be set up so that services can be roamed from one cloudlet to another when the mobile devices are on the move (Ai et al, 2018; Babar et al., 2021).

Mobile Edge Computing (MEC) was proposed and developed by ETSI (the European Telecommunications Standards Institute). MEC is designed to allocate computing resources closer the radio access network (RAN) (Shahzadi et al., 2017). The key idea of MEC is to use some end-user clients such as laptops or micro-servers located at the edge of mobile networks to carry out an extensive amount of data storage and processing in real time (Ahmed and Rehmani, 2017; Chen et al., 2022). The introduction of 5G networks allows for MEC to fulfil the speed and network load requirements the traditional cloud computing could not meet (Ahmed and Rehmani, 2017). Industry collaborations between the cloud providers and the major telecommunications companies have been developed to offer MEC based enterprise solutions directly to the customers.

Fog computing was introduced by Cisco, which also founded the OpenFog Consortium to address the demands for scalability and interoperability across different segments of IoT devices and applications (Shahzadi et al., 2017; Khan et al., 2019). Fog computing can be described as a distributed computing infrastructure where computing resources and services are allocated in the most appropriate and efficient places, which can be at any point along the spectrum from IoT, network devices, to the clouds (Vaquero & Rodero-Merino, 2014; Shahzadi et al., 2017). The OpenFog Consortium focuses on developing a system-level horizontal architecture where network devices such as routers can host services as part of the virtualized infrastructure (Vaquero & Rodero-Merino, 2014). Within the virtualized infrastructure, multiple dispersed heterogeneous devices should be able to communicate and cooperate with each other without any issue (Vaquero & Rodero-Merino, 2014; Shahzadi et al., 2017; Ai et al., 2018).

Edge computing can provide quality services with faster response time in comparison with traditional cloud computing. Many applications will benefit from edge computing due to the features of low latency, low bandwidth cost, low energy consumption, real-time data processing, traffic filtering, mobility support, localized security protection, heterogeneity, and scalability

(Satyanarayanan, 2017; Cao et al., 2020; Liyanage et al., 2021). Those applications include but not limit to autonomous vehicles, smart homes/cities, smart manufacturing, environmental monitoring, augmented reality, wearable cognitive assistance, video streaming optimization, emergency management, disaster relief, etc. (Qiu et al., 2020; Alwakeel, 2021; Liyanage et al., 2021). In the next section, this paper provides several examples of the real-world applications to illustrate the key benefits of edge computing.

REAL-WORLD APPLICATIONS OF EDGE COMPUTING

Novetta is an Amazon Web Services (AWS) advanced consulting partner focusing on analytics solutions for government defense and intelligence entities (Heald & Teschke, 2018). One of their most essential functions is to offer support in disaster situations. While the company operates in the cloud, they needed to leverage edge resources to ensure decisions could be made in real time. In disaster situations, the speed of processing is critical to support relief efforts. Novetta uses AWS Snowball Edge, a rugged and shippable computing device equipped with computing power and storage capability. The edge device tracks the location of essential personnel and equipment such as emergency vehicles. It is also used for real time video processing even with reduced bandwidth. Since Novetta is developing resources for government agencies, they must meet the high standards for security the government requires. Snowball edge and the entire Snow Family of AWS products has been standardized to meet these requirements (Heald & Teschke, 2018).

Groupama Assicurazioni, a Paris, France-based insurance company is utilizing IoT and edge to better support their customers (Chaban, 2019). If customers agreed, sensors would be placed in their vehicles, and they would receive a discount on their annual premium. These sensors monitor vehicle speed, breaking, and locations, and will notify the insurance when it believes an accident has occurred. This allows the companies to send out emergency services before anyone calls to report the accident. In the event of theft, the insurance company will be able to track the vehicle. It also helps with fraudulent claims, such as a customer trying to lump in previous damage in a recent accident. Because the sensors can detect which side of the car was impacted by the accident, the insurance company will be able to avoid such fraudulent claims. Groupama claims at least 800 crashes have been avoided, and dangerous driving behaviors have reduced. Due to the large amount of data being captured in real time, edge devices are the best way to process this data, and to provide fast responses in the emergency situations where real-time, low-latency processing is needed. Powered by IBM cloud, Groupama has been effectively using the IoT devices to better serve their clients (Chaban, 2019).

Fugro is an industry leader in geo-intelligence, helping clients to gain insights for marine projects such as offshore wind farms (Microsoft Azure, 2020). Typically, their clients are in the energy sector. Fugro sends oceanographers, meteorologists, and hydrologists out on vessels to collect data from the ocean including water depth and winds. Those scientific data would be collected by sensors on the vessels and then sent via satellite to the on-premises Microsoft SQL server to be stored and processed. While the operation was successful previously, the company was facing issues. Uploading the data from those remote locations was proving to be difficult, and the satellite connections sometime were not sufficient to transfer the substantial amounts of data being collected. The company turned to Azure cloud services to move to the cloud to the edge to address the problem. They first migrated their on-premises database to a traditional cloud database. Then, they employed Azure IOT Edge and Azure SQL edge to use on the vessels for real time processing. Since the change, Fugro is now able to store and process data at sea, whether they are connected to the network or not. Additionally, the company's C# code translated to Azure and developers can update all their systems with a single set of code. With the edge solution, Fugro has reduced the report delivery time from two weeks to eight minutes (Microsoft Azure, 2020).

Industry collaborations between the cloud providers and the major telecommunications companies have been developed to make mobile edge computing accessible. Current collaborations include Verizon with AWS and Azure, T-Mobile with Lumen technologies, and AT&T with Google Cloud. In those collaborations, the telecommunications companies own 5G towers and network, while the cloud providers are providing their computer and storage technologies on the edge network. The edge network is hosted on-premises and can therefore be closer to the end users. The speed of 5G and the computing services being located at the edge allow customers to receive lower latency and higher bandwidth for their applications. With the MEC network, businesses also have the option to host sensitive data in an on-premises environment and still leverage the benefits of the 5G edge (AT&T Business, 2022). For example, ShotTracker, a sensor-based technology providing real time analytics and data to basketball players, coaches, and broadcasters, is able to leverage Verizon 5G and AWS Wavelength to speed up their application response time, giving real time feedback to players and coaches (Garman & Erwin, 2020; McCarthy, 2021). For another example, Tata Consultancy agency has leveraged 5G edge through Verizon and AWS machine learning to speed up their end-of-line quality control process (King, 2019; Jose et al., 2020). AWS wavelength running on Verizon's 5G network allows for AI to examine photos of their devices against stock photos and detect any deficiencies (Jose et al., 2020).

With the development of edge computing and 5G edge, new security challenges arise for the customers, cloud service providers, and telecommunications companies. While traditional security measures remain relevant and applicable, newer concepts such

as three-factor authentication will be needed to provide fully secure solutions deployed at edge computing platforms (Khan et al., 2020; Qiu et al., 2020). Next, the paper explores the major challenges and opportunities of edge computing security.

EDGE COMPUTING SECURITY: CHALLENGES AND OPPORTUNITIES

In both the cloud and the edge models, security is split between the cloud service provider and the company. Edge computing presents unique challenges and opportunities separate from the traditional cloud. Attacks such as DDoS, injection of cloud malware and cryptographic are still at normal in the cloud environments. As the cloud migrates further to the edge, there are additional security concerns to address, for examples, eavesdropping, rogue data center, data tampering, session hijacking, etc. (Parikh et al., 2019; Alwakeel, 2021). Because edge focuses on IoT devices, the lack of security requirements for those devices can make the network vulnerable. The enormous number of devices connected to the edge network carry a ton of personal data. Without the same resources as the traditional cloud servers, it is more challenging to secure the edge network (Sha et al., 2020).

The confidential nature of the data stored at the edge makes edge devices a target for attacks. Compared to the traditional cloud, the impacts are greater if the edge data is compromised. This is further compounded by the limited resources of edge devices, not allowing them to perform intensive security algorithms. By design, the edge network is dynamic and not standardized. Creating security polices for this type of network is challenging (Alwakeel, 2021). Furthermore, the design of the edge network makes backup and recovery more difficult in the case of a system outage or failure. Denial of Service attacks can be targeted towards MEC servers due to their limited capacity. This type of attack would prevent the nodes who need access to the server from gaining it. Man-in-the-middle attacks can be launched on the many connected devices by targeting the infrastructure layer. Therefore, sophisticated edge-centric security designs are needed to provide countermeasures and protect the edge platforms and applications (Sha et al., 2020).

Edge-Centric Approach

All the components of the edge computing environment, including the cloud, edge, IoT devices, and users, are vulnerable to attacks. According to Sha et al. (2020), the best way to protect IoT devices is to do so at the edge layer. While the cloud has more resources than edge, it is located too far from the edge devices to perform security functions efficiently. As discussed, IoT devices do not have the resources needed to run the necessary security functions. Therefore, the edge layer with more resources and being located close to the user is the more efficient and secure way to protect IoT devices. Computation intensive security measures such as homomorphic encryption, and attributes-based controls can be performed at the edge level (Sha et al., 2020). Additionally, the location of the edge devices allows the security to be performed in real time which is necessary or must for edge/IoT applications (Alwakeel, 2021). The location also allows the edge devices to keep up with the mobility of IoT devices. The movement of the devices can be better tracked allowing for continuous connection and protection. Firewalls can be deployed at the edge level to filter attacks to the IoT device. Lastly, because the edge is an extension of the cloud, they are in constant communication with one another. This allows the edge to utilize the more powerful cloud for security support when needed (Sha et al., 2020).

User-centric edge-based IoT security: Relying on users to secure any device/system is a huge risk. Humans are always considered the weakest link in a security structure. This is the same for IoT devices. Users typically do not have the knowledge to secure their own devices. Offloading personal security to the edge layer is a way to solve this problem. A Trusted Virtual Domain (TVD) can be implemented at the edge layer to manage who and what can access the end-user devices. The user-centric approach focuses on allowing the users to define what security policies they want to have in place, then using the TVD, Security Application Virtual Container (SAVC), network enforcer and other resources located at the edge to carry out the security measures (Sha et al., 2019).

Device-centric edge-based IoT security: Rather than customizing the security solution based on the individual users, device centric design focuses on the resources available on each device and deploying the solution accordingly. Because there are so many IoT devices, they all have a different level of resources available. While they are all resource-constrained, some may have more of an ability to handle intense computing. The two proposed models for device-centric security are EdgeSec and ReSIoT (Sha et al., 2020). Both models aim to offload intensive computing from IoT devices to the edge to provide powerful advanced security algorithms and AI protections that cannot be implemented on the IoT devices. EdgeSec uses six major modules that work together to secure the devices (Sha et al., 2020). The ReSIoT method introduces a reconfigurable framework, such as a Security Agent for the devices. The Security Agent may be a wireless router or a gateway device which will handle advanced security computing for the IoT devices (Hsu et al., 2018).

End-to-end security for IoT: IoT devices are heterogeneous in nature, making end-to-end security difficult to implement. Researchers have proposed to deploy security-based middleware at the edge to protect the end-to-end IoT communications. The application would handle security functions such as message authentication and encryption (Mukherjee et al, 2017).

5G Edge Security

Security risks of MEC-enabled 5G applications can come from the device, network, edge, cloud, and operation & management (Qiu et al., 2020). Ranaweera et al. (2022) pointed out that the investigations of security vulnerability and prevention of MEC-enabled 5G technologies need to be managed based on different use cases and scenarios due to the heterogeneous nature of MEC services. Related work on security of 5G edge has highlighted the following aspects: standardization, encryption, monitoring and detection (Alwakeel et al., 2021).

Standardization: All edge nodes need to be equipped with consistent and proper security measures. When there is a single weak link in a system, all the other nodes are also vulnerable. By making sure all nodes have the same algorithms in place, the entire edge system will be more resistant to attack. The standardization efforts should involve multiple players including network providers, application providers, and regulatory agencies (Qiu et al., 2020).

Encryption: According to Ranaweera et al. (2022), it is important to employee the appropriate level of encryption at different layers of the edge architecture, not only to ensure secure data communications between MEC applications, but also to be sensitive to the resource constraints of certain layers. Recently, ESTI cybersecurity committee released two ABE (Attribute-Based Encryption) specifications to be applied in 5G edge (Khan et al., 2020).

Monitoring and Detection: The 2016 DDos attack on DNS servers originated from compromised IoT devices was a sounding alarm to the IoT security. It called for better designed, distributed intrusion detection systems at the edge layer to identify any anomalies in the systems. Sha et al. (2020) suggested that it is important to utilize advanced machine learning algorithms to achieve adaptive and improved intrusion detection results. Moreover, from the user perspective, user behavior should be monitored/profiled to detect unusual activity that may have malicious intents.

CONCLUSION

This paper presents a review of edge computing, with a focus on edge computing architecture and key technologies. Several real-world applications of edge computing are provided in the paper. Besides highlighting the benefits, this paper also explores the unique security challenges related to the design, deployment, and management of edge computing. While edge computing has become a popular topic, many areas are still open for further research. This study serves as a preliminary investigation to the applications and security features of edge computing.

Our future research agenda is to conduct a systematic review about the edge-centric security designs, especially on how to secure the edge layer itself, and how to secure the communications between the IoT devices and the edge, and between the edge and the cloud layer. While machine learning methods have been proposed as mechanisms to detect intrusions at the edge, how to tailor the complex algorithms to work with a relatively small amount of data available at the edge can be a challenging issue. A systematic review of the edge-centric security deigns will shed light on the state-of-art solutions and help identify the research gaps.

REFERENCES

1. Ai, Y., Peng, M., & Zhang, K. (2018). Edge Computing Technologies for Internet of Things: A Primer. Digital *Communications and Networks*, *4*, 77-86.
2. Ahmed, E. & Rehmani, M. (2017). Mobile Edge Computing: Opportunities, Solutions, and Challenges. *Future Generation Computer Systems*, *70*, 59–63.
3. Alwakeel, A. (2021). An Overview of Fog Computing and Edge Computing Security and Privacy Issues." *Sensors*, *21*, 8226. Retrieved from: https://doi.org/10.3390/s21248226
4. AT&T Business. (2022). AT&T Multi-Access Edge Computing. Retrieved in December, 2022, from: https://www.business.att.com/products/multi-access-edge-computing.html
5. Babar, M., Khan, M., Ali, F., Imran, M., & Shoiab, M. (2021). Cloudlet Computing: Recent Advances, Taxonomy, and Challenges. *IEEE Access*, *9*, 29609-29622.
6. Cao, K., Liu, Y., Meng, G, & Sun, Q. (2020). An Overview on Edge Computing Research. *IEEE Access*, *8*, 85714–85728.
7. Chaban, M. (2019, September). How IOT Insurance Is Helping Groupama Reduce Claims and Accidents. Retrieved in December, 2022, from: https://www.ibm.com/blogs/industries/telematics-iot-auto-insurance-data-groupama/
8. Chen, H., Qin, W., & Wang, L. (2022). Task Partitioning and Offloading in IoT Cloud-Edge Collaborative Computing Framework: A Survey. *Journal of Cloud Computing*, *11*(86). Retrieved from: https://doi.org/10.1186/s13677-022-00365-8

9. Garman, M. & Erwin, T. (2020, August). Verizon and AWS Deliver Mobile Edge Computing to Customers in Boston and the Bay Area. Retrieved in December, 2022, from: https://aws.amazon.com/blogs/industries/verizon-and-aws-deliver-mobile-edge-computing-to-customers-in-boston-and-the-bay-area/
10. Heald, K. & Teschke, M. (2018, December). Deploying Machine Learning at the Edge. Retrieved in December, 2022, from: https://www.novetta.com/2018/12/deploying_machine_learning_at_the_edge/
11. Hsu, R., Lee, J., Quek, T., & Chen, J. (2018). Reconfigurable Security: Edge-Computing-Based Framework for IoT. *IEEE Network*, *32*(5), 92–99.
12. Jose, R., Khot, D., Shanmugam, S., & Gopal, S. (2020, October). TCS Enables Intelligent, Real-Time Quality Inspection for a Smart Factory with AWS Wavelength. Retrieved in December 2022, from: https://aws.amazon.com/blogs/industries/tcs-enables-intelligent-real-time-quality-inspection-for-a-smart-factory-with-aws-wavelength/.
13. Khan, R., Kumar, P., Jayakody, D., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196-248
14. Khan, W., Ahmed, E., Hakak, S., Yaqoob, I., & Ahmed, A. (2019). Edge Computing: A Survey. *Future Generation Computer Systems*, *97*, 219-235.
15. King, K. (2019, December). Verizon and AWS Team Up to Deliver 5G Edge Cloud Computing. Retrieved in December, 2022, from: https://www.verizon.com/about/news/aws-verizon-5g-edge-cloud-computing
16. Liyanage, M., Porambage, P., Ding, A., & Kalla, A. (2021). Driving Forces for Multi-Access Edge Computing (MEC) IOT Integration in 5G. *ICT Express*, *7*(2), 127–137.
17. McCarthy, M. (2001). Verizon Ventures' Investment in ShotTracker Fuels Sports Data Growth and Engagement. Retrieved in December 2022, from: https://www.verizon.com/ventures/blog/2021/1/verizon-ventures%E2%80%99-investment-in-shottracker-fuels-sports-data-growth-and-engagement
18. Microsoft Azure. (2020). Azure SQL Edge: A Data Engine Optimized for IoT Workloads on Edge Devices. Retrieved in December, 2022, from: https://azure.microsoft.com/en-us/resources/azure-sql-database-edge-whitepaper/
19. Mukherjee, B., Neupane, R., & Calyam, P. (2017). End-to-End IoT Security Middleware for Cloud-Fog Communication. *Proceedings of 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud),* New York, USA, 151-156.
20. Parikh, S., Dave, D., Patel, R., & Doshi, N. (2019, November). Security and Privacy Issues in Cloud, Fog and Edge Computing. *Procedia Computer Science*, *160*, 734–739.
21. Qiu, Q, Liu, S., Xu, S., & Yu, S. (2020). Study on Security and Privacy in 5G-Enabled Applications. *Wireless Communications and Mobile Computing*. *2020*. Retrieved from: https://doi.org/10.1155/2020/8856683
22. Ranaweera, P., Jurcut, A., & Liyanage, M. (2022). MEC-Enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Computing Surveys*, *54*(9), Article 186, 1-37.
23. Rong, G., Xu, Y., Tong, X., & Fan, H. (2021). An Edge-Cloud Collaborative Computing Platform for Building AIoT Applications Efficiently. *Journal of Cloud computing*, *10*(36). Retrieved from: https://doi.org/10.1186/s13677-021-00250-w
24. Satyanarayanan, M., Bahl, P., Caceres, R., & Davis, N. (2009). The Case of VM-Based Cloudlets in Mobile Computing, *IEEE Pervasive Computing*, *8*(4), 14-23.
25. Satyanarayanan, M. (2017). The Emergence of Edge Computing. *Computer*, *50*(1), 30-39.
26. Sha, K., Errabelly, R., Wei, W., Yang, T., & Wang, Z. (2018). EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security. *Proceedings of the First IEEE International Conference on Fog and Edge Computing (ICFEC)*, Madrid, Spain, 81-88.
27. Sha, K., Yang, T., Wei, W., & Davari, D. (2020). A Survey of Edge Computing-Based Design for IoT Security. *Digital Communications and Networks*, *6*, 195-202.
28. Shahzadi, S, Iqbal, M., Dagiuklas, T., & Qayyum, Z. (2017). Multi-Access Edge Computing: Open Issues, Challenges and Future Perspectives. *Journal of Cloud Computing*, *6*(1). Retrieved from: https://doi.org/10.1186/s13677-017-0097-9
29. Vaquero, L. & Rodero-Merino, L. (2014). Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing. *ACM SIGCOMM Computer Communication Review*, *44*(5), 27–32.