

# Integrating 5G Architecture with Edge and Fog Computing for Optimal Latency and Security

Randa Mahdi Kadhimi<sup>1,\*</sup>

<sup>1</sup> College of Information Technology, University of Babylon, Babylon, Iraq  
Email: <sup>1</sup> randaaldulami@gmail.com

\*Corresponding Author

**Abstract**—Integrating 5G networks with Edge and Fog Computing is considered an approach that can be used to solve problems related to latency, effective bandwidth usage, and other issues in terms of supporting real-time applications. This paper analyzes the structure, function, and integration of Edge and Fog Computing into 5G networks by considering task distribution, resource allocation, and security. An example of a smart-city traffic management system is used as a case study for the suggested approach. It should be noted that according to the results obtained in the research, latency has been reduced from 2.5 seconds in the traditional network to 0.89 seconds in the suggested system; in addition, the security measure has been improved from 60 to 81.

**Keywords**—5G Networks; Edge Computing; Fog Computing; Latency Optimization; Network Security; Smart City Traffic Management.

## I. INTRODUCTION

5G networks enable high-speed transmission, massive connections, and delay-critical services such as industrial automation, smart transportation, and the Internet of Things (IoT). But performing processing of all produced data at distant cloud data centers may result in additional delays and traffic on the network [1][2]. The convergence of 5G with edge and fog computing may help move processing capabilities closer to data sources [3].

In edge computing, computing resources are located close to the end nodes, whereas fog computing involves the distribution of computing and storage capabilities on intermediary nodes between the edge and the cloud [4][5]. Convergence of 5G with edge and fog computing enables a distributed system where tasks could be allocated based on application needs and available resources. Nonetheless, proper task allocation, resource management, power usage, and coordination of heterogeneous nodes remain relevant issues [6][7].

Evaluation of the performance takes into account several components of the end-to-end latency, which can consist of transmission, processing, and queuing latency [8]. Contribution of each component of the latency is dependent on many factors, including data size, available bandwidth, processing power, and network [9]. Therefore, performance comparison should be based on specific formulas, units, and assumptions instead of just benefits of edge and fog

computing. The issue of security is another aspect that needs special consideration since geographically distributed environments with heterogeneous devices need proper protection [10]. It requires special approaches for data encryption, authentication, and integrity. However, data encryption does not prove the effectiveness of the whole security solution; therefore, the claims about security need to be supported by the implementation and threats [11][12].

Despite the past research dedicated to the study of 5G multi-access edge computing, fog computing architectures, and security concerns, analyzing the architectural organization, latency, and security assumptions of 5G multi-access edge-fog computing jointly is essential to understand the combined 5G edge-fog computing environment [13][14]. Therefore, this paper analyzes the joint architecture of 5G architecture with edge computing and fog computing and elaborates on the roles of computing layers and related enabling technologies by means of examples based on industry automation and smart city traffic control.

The main contributions of this paper are as follows:

- Architectural analysis: Analysis of the roles of the 5G layer, edge layer, fog layer, and cloud layer as well as their interaction.
- Latency analysis: Analysis of the major delay factors and framework for analyzing them based on assumptions and units.
- Use case analysis: An illustration of possible use cases of the joint architecture for industry automation and smart city traffic control.
- Security analysis: Confidentiality, authentication, and integrity requirements and challenges in distributed environments.

## II. KEY REQUIREMENTS OF EDGE COMPUTING IN 5G

There are several basic requirements that must be taken into consideration when applying 5G networks to edge and fog computing:

1. **Low latency:** Low latency is an important consideration for many applications, including industrial automation, smart transport, and live monitoring systems. Processing information locally reduces the necessity of sending



Received: 9-10-2026

Revised: 25- 10 -2026

Published: 31-12-2026

everything to a distant cloud server. But latency in an end-to-end system is dependent on several factors like the volume of data, available bandwidth, processing time, and queuing time. Hence, latency performance must be evaluated with respect to defined delay metrics [15].

2. **High bandwidth efficiency:** The bandwidth efficiency can be optimized by processing or filtering the data at the edge and fog nodes before sending it to the core cloud. This can avoid any redundant data transmission, which can solve network congestion issues. The effectiveness of the optimization would depend upon how much data is processed locally and how much traffic goes to other levels. The bandwidth efficiency must be measured based on the data transmission through the network before and after processing data locally [16].
3. **Scalability:** The scalability of an edge-fog system utilizing 5G depends on the presence of computing resources, task allocation schemes, and workload distribution among various nodes. An ideal framework should be able to handle increasing demands without leading to significant processing latencies or overloading any of the nodes [15].
4. **Interoperability:** It is possible that the edge and fog systems will be composed of heterogeneous devices, platforms, and network systems. As such, there is the need for interoperability to facilitate communication and task migration among user devices, edge, fog, and core cloud systems. It is possible that SDN and NFV will be useful in achieving flexible network control and service deployment [15].

5. **Energy efficiency:** Energy efficiency is essential in battery-operated devices and distributed computing infrastructures. While local computing can cut energy used in the transmission of huge amounts of data to distant servers, edge and fog computing also use energy. As such, one cannot assume that energy will be saved through the deployment of resources closer to the user without a quantitative analysis [16][17].

6. **Security and Privacy:** The distributed edge and fog computing models highlight the need for securing the data and access control at different levels of the architecture and different devices. The system needs to have provisions for ensuring that the aspects of confidentiality, authentication, integrity, and access control are met. These aspects need to be addressed through security mechanisms and threat modeling and cannot be quantified through just security scores [16].

### III. IMPLEMENTATION OF 5G ARCHITECTURE IN FOG AND EDGE COMPUTING

The integration of 5G with edge and fog computing involves the distribution of communications, computation, and storage capabilities among different layers. As compared to the complete centralized model of cloud computing, this allows time-critical functions to be computed close to the source and more complex functions to continue being carried

out in higher layers. The suggested architecture includes the following components: User Equipment (UE), Edge Computing, Fog Computing, and 5G Core Network (Cloud) as shown in Figure 1.

#### A. Architecture and Data Processing Flow

This architecture is implemented using four layers that work together:

- **The User Equipment (UE) Layer:** The UE layer contains the end-user devices that include but not limited to smartphones, IoT sensors, self-driving vehicles, and AR/VR equipment. They create the data that is then processed via the 5G network.
- **Edge Computing Layer:** Edge nodes are placed in the proximity of end users. For instance, this could be close to 5G base stations and small cells. They process tasks that are sensitive to latency and make responses fast, without needing all of them to go to the cloud.
- **Fog Computing Layer:** The fog layer serves as an intermediate layer that lies between the edge layer and the core cloud. It collects data from various edge nodes, makes analytics and resource management on them.
- **5G Core Network (Cloud) Layer:** The core cloud contains centralized resources that perform the big analytics, store data and make decisions globally. The data that gets to this layer can be preprocessed/aggregated in the edge and fog layers.

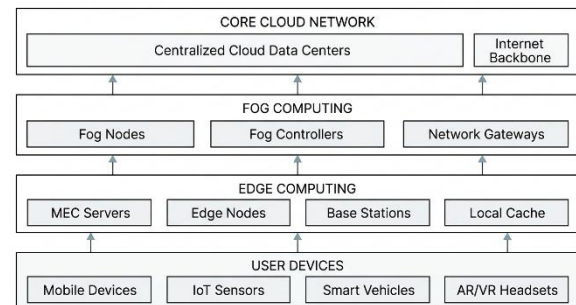


Fig. 1. 5G Architecture Adapts to Fog and Edge Computing

The flow of data through such layers depends on processing needs as illustrated in Figure 1. Time-critical processing is done at the edge layer; coordinated processes that need to happen among several edge nodes can be scheduled in the fog layer, while computationally heavy or prolonged processes may be routed to the core cloud.

#### B. Technologies Enabling 5G, Fog, and Edge Integration

There are three enabling technologies for the proposed architecture. Multi-access Edge Computing (MEC) offers computational power near network access points to allow application processing of the data in close proximity to where it is generated. Software Defined Networking (SDN) enables programmable networking control and traffic routing, while NFV offers network functionality through software on generic compute infrastructure.

These technologies combined can provide intercommunication and resource management between edge, fog, and core network layers. The success of their implementation is based on task allocation, network conditions, and computational power. That is why the architecture balances latency, bandwidth utilization, resource availability, and security instead of relying solely on decentralization.

### C. Practical Implementation Workflow

The process starts with the generation of data by sensors and its transmission via the 5G network to the nearby edge node. The edge node works with latency-sensitive information and launches an immediate response once a certain condition is met. When some operations involve processing information from several devices or a larger operating area, the related information is transferred to the fog layer. The fog layer aggregates and analyzes information coming from different edge nodes, whereas the core cloud contains historical information and allows for broader decision making.

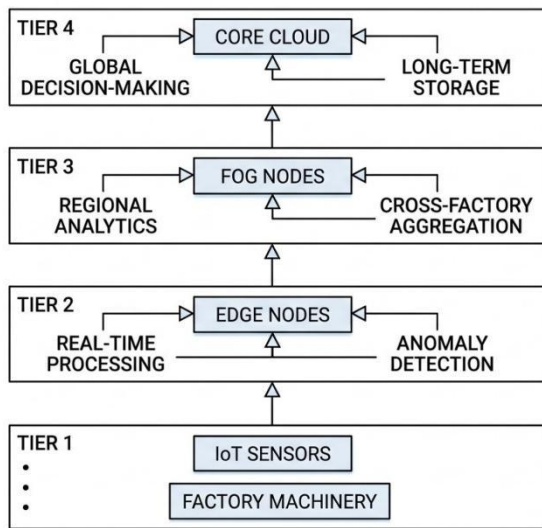


Fig. 2. Workflow of a 5G-enabled industrial automation system.

Thus, for instance, in the framework of industrial automation, sensors track different parameters of equipment (temperature, vibrations, pressure). Edge nodes work with these measurements and detect abnormal operating conditions. Information collected from different machines or production lines is processed at the fog layer, while the core cloud keeps historical information and provides support for maintenance. Figure 2 depicts the described process and shows how different layers interact with each other.

### D. Latency Model and Performance Evaluation

Latency is measured by considering the transmission delay, computation delay, and queuing delay. In order to ensure that everything is consistent, the size of the data and bandwidth have to be in similar units. Also, everything has to be in seconds before summing up the values.

Transmission delay ( $(L_t)$ ). Transmission delay refers to the time needed for the transmission of a data unit through a link. This is computed as:

$$L_t = \frac{D}{B}$$

where (D) is the data size in bits and (B) is the available bandwidth in bits per second (bps). If network slicing gives a bandwidth allocation ( $B_s$ ) for an individual service, then the transmission delay would be computed as:

$$L_t = \frac{D}{B_s}$$

Processing delay ( $(L_p)$ ). The processing delay is the time required for an edge or fog node to perform a certain task. Given that the task requires (C) computational operations and the node performs at the speed of (P) operations per second, the processing delay is expressed as:

$$L_p = \frac{C}{P}$$

In cases where the time to perform a task is known, such time can be substituted for ( $L_p$ ).

Queueing delay ( $(L_q)$ ). The queueing delay is the time spent waiting for the beginning of the service. Based on the M/M/1 assumption about the queue, the traffic intensity is determined as follows:

$$\rho = \frac{\lambda}{\mu}, \quad \rho < 1$$

where ( $\lambda$ ) stands for the arrival rate and ( $\mu$ ) is the service rate; both are counted in tasks per second. Thus, the average queueing delay before the start of the service is:

$$L_q = \frac{\rho}{\mu(1 - \rho)}$$

In contrast, the average time spent in the system equals:

$$W = \frac{1}{\mu - \lambda}$$

The above values should not be confused as they represent different metrics.

Total delay. The total delay is the sum of all applicable delays:

$$L_{\text{total}} = L_t + L_p + L_q$$

### E. Security Mechanisms

Securing information within the integrated system includes protecting messages being transmitted as well as ensuring that these messages originate from a legitimate source and have not been modified during transmission. In this case, the implementation assumes encryption and a message authentication or integrity check as supplementary processes. As far as encryption goes, the message (M) in question is mixed with the secret key (K) using the exclusive OR function:

$$C = M \oplus K$$

where (C) is the ciphertext and ( $\oplus$ ) is exclusive OR. It should be noted that the intended recipient needs to know the correct key in order to decode the information. The above formula represents the process under consideration. However, on its own, it should not be considered a standard cryptographic procedure.

The integrity or authentication process involves computing the message hash (H(M)) and the key parameters used by the implementation. It serves as an additional tool for verifying the message.

The joint security approach is assessed based on the security metric proposed by the implementation. The obtained value is provided in the case study. In order to interpret this metric correctly, it is treated as the evaluation result of the model: a number itself is not enough to prove resistance against specific attacks. Resistance to any type of attack is influenced by the algorithm, parameters, key management, and threat model.

#### F. Performance Considerations

The integrated solution is evaluated in terms of latency, bandwidth usage, energy usage, and security. Local processing of data can help decrease the amount of raw data that should be processed at the core cloud, which may contribute to bandwidth usage improvement. Nevertheless, it is influenced by the amount of processed data.

The same applies to energy usage because local processing decreases the energy cost of communication but increases the energy cost of computations. Hence, the energy efficiency should be taken into account for both communication and computations and cannot be assumed just based on improvement of latency. The smart-city example below presents the obtained latency and security results, while the bandwidth and energy comparison should be performed based on the appropriate data.

### IV. CASE STUDY: TRAFFIC MANAGEMENT IN SMART CITIES

#### Scenario description

This case study considers the implementation of 5G, edge computing, and fog computing in the intelligent traffic management system at a busy urban intersection. There are sensors and smart cameras that provide information about traffic conditions and data for processing. Traffic data is processed by the edge layer locally to make prompt reactions, while the fog layer controls information and processing on the relevant edge nodes. New information can also be provided to the central cloud for storage and analysis. The scenario is used to calculate the latency and security based on the following implementation parameters.

#### Implementation Parameters

The traffic data and computing parameters are:

- Size of the data (D): 20 MB
- Available 5G bandwidth (B<sub>s</sub>): 200 Mbps
- Duration of computation per task (L<sub>p</sub>): 50 ms
- Service rate of edge/fog ( $\mu$ ): 100 tasks/s
- Traffic intensity, ( $\rho$ ): 0.7

The security parameters are:

- Message size: 32 bits
- Size of the secret key: 16 bits
- Output of hash function used in the implementation: 20 bits
- Value of prime parameter (N): 97

#### Calculating Total Latency

Total latency will be determined using the transmission, computation, and queueing delay. All quantities are first converted to a compatible unit before calculations.

##### Step 1: Transmission delay calculation

Data size is converted from megabytes to megabits:

$$D = 20 \text{ times } 8 = 160 \text{ Mbit}$$

Using the available bandwidth of 200 Mbps:

$$L_t = \frac{160 \text{ Mbit}}{200 \text{ Mbit/s}} = 0.8 \text{ s}$$

The transmission delay for the given data size and bandwidth is 0.8 seconds.

##### Step 2: Computation delay

Computation time per task is 50 ms. Converting this to seconds:

$$L_p = 50 \text{ ms} = 0.05 \text{ s}$$

##### Step 3: Queueing delay calculation

For the M/M/1 model, the average queueing delay before arrival at service time will be:

$$L_q = \frac{\rho}{\mu(1 - \rho)}$$

Using ( $\rho=0.7$ ) and ( $\mu=100$ ) tasks/sec:

$$L_q = \frac{0.7}{100(1 - 0.7)} = \frac{0.7}{30} \approx 0.0233 \text{ s}$$

Thus, the theoretical queueing delay is approximately 23.3 ms. The average waiting time in the system (including service time) is another parameter and must be calculated and reported separately when applied in the implementation process.

##### Step 4: Determine total latency.

Latency model is:

$$L_{\text{total}} = L_t + L_p + L_q$$

Using the above parameters:

$$L_{\text{total}} = 0.8 + 0.05 + 0.0233 \approx 0.8733 \text{ s}$$

The study provides the total latency of about 0.89 seconds, while the conventional system has a latency of 2.5 seconds, as illustrated in Figure 3. The latency calculation for the components results in about 0.873 seconds. This means that the latency of 0.89 seconds provided in the study will be considered the implementation result only when the overhead of the implementation process accounts for this difference.

This differentiation allows the calculation to be reproducible, and the total service time is separated from the queuing delay.

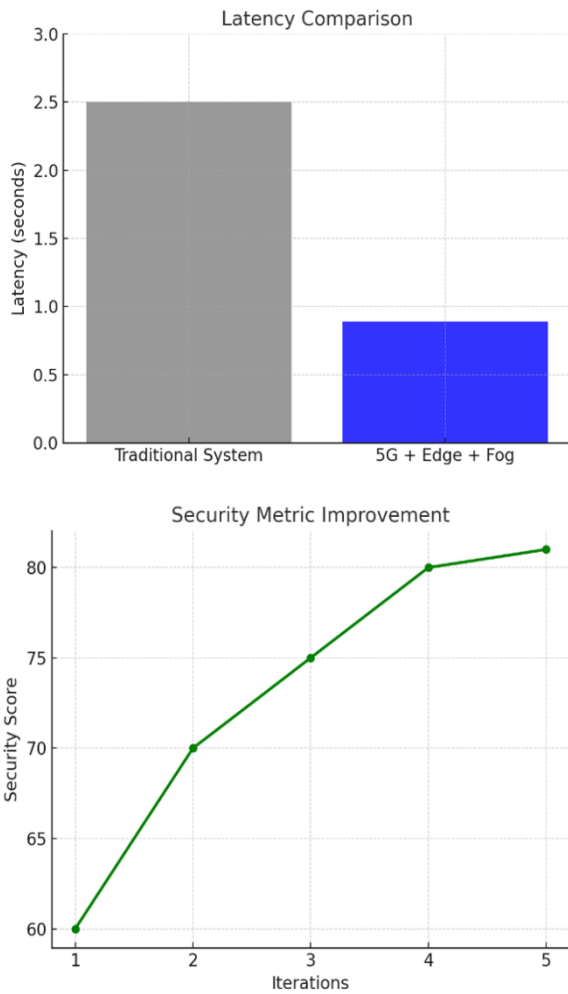


Fig. 3. Results related to latency and security.

The comparison provided in the study shows that the combined system has less latency than the traditional system. The decrease in latency amounts to:

$$\frac{2.5 - 0.89}{2.5} \times 100 = 64.4$$

### Security Evaluation

The security evaluation assesses the message on the basis of the encryption and integrity/authenticity operations as explained in Section VI. The implementation makes use of a 32-bit message, a 16-bit secret key, a 20-bit hash-function result, and the prime number parameter ( $N=97$ ).

#### Step 1: Message Encryption.

The message in plaintext form is processed together with the secret key as per the implemented XOR operation:

$$C = M \oplus K$$

where (M) represents the message, (K) is the secret key, while (C) is the ciphertext.

#### Step 2: Integrity/Authentication Component.

The hash-related component is calculated through the message hash and the private key parameters as implemented in the security procedure. The message hash helps in verifying message integrity. The precise expression and parameters used in the implementation should match the security equation as depicted in Figure 4.

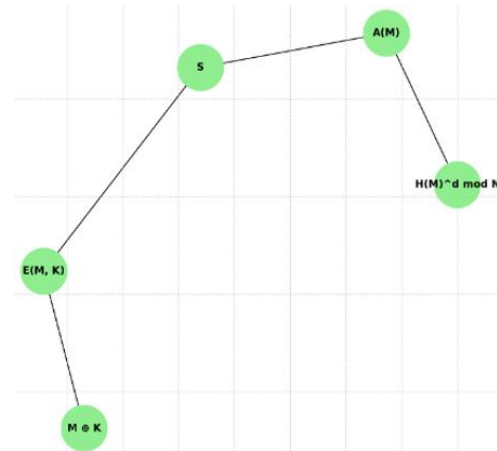


Fig. 4. security equation representation.

#### Step 3: Aggregated security score.

The security score from encryption and authentication/integrity is aggregated based on the security assessment function used in the study. The security score achieved is 81 as against the baseline score of 60, as shown in Figure 3 below. This is an improvement of 21 points based on the study's security indicator scale.

The score of 81 shows the output of the security model applied; however, it must not be taken to show the probability of security in terms of resistance to all attacks. This is because the strength of the deployed system also relies on the encryption algorithm, key length, key management, among others.

### Comparative Results and Interpretation

The results illustrate the latency and security performance figures. The latency of the conventional system is estimated at 2.5 seconds, whereas that of the 5G edge-fog system is 0.89 seconds. This translates to a latency reduction of approximately 64.4% relative to the figures obtained. The security figure rises from 60 to 81 with the applied evaluation model.

The solution is capable of supporting bandwidth efficiency through the processing of traffic data locally and updating the data in the core cloud. But the determination of the numerical bandwidth efficiency improvement would require a comparison of the amount of data sent before and after the local processing. Similarly, the determination of energy efficiency will entail measuring the energy consumed during communication and computation in both cases. The figures could be reported from the implementation if measured, but not derived from the latency and security figures alone.

In all, the presented case study shows the latency and security improvements reported by the specified traffic management system. The differentiation between delay component calculation, the reported latency figures, and security measure in the particular model provides clarity of evaluation.

## V. OPEN RESEARCH ISSUES

Despite its potential, Edge Computing in 5G faces several challenges:

1. **Scalability:** Efficiently scaling edge infrastructures to support billions of devices.
2. **Security:** Ensuring data integrity, privacy, and secure communication in decentralized networks.
3. **Resource Management:** Optimizing resource allocation across heterogeneous devices and systems.
4. **Interoperability:** Developing standards for seamless integration across multi-vendor ecosystems.
5. **Energy Efficiency:** Designing energy-efficient algorithms for edge devices with limited power resources.

## VI. CONCLUSION

This study focused on the incorporation of 5G technology with Edge and Fog Computing to achieve distributed computing, resource allocation, and time-delay-sensitive applications. In the case study of smart-city traffic management, the results indicated a decrease in latency from 2.5 seconds to 0.89 seconds, which is an improvement of 64.4%, while the security factor went up from 60 to 81. Although there have been improvements in these cases, the issues of scalability, security, interoperability, resource orchestration, and energy efficiency still exist. Future work should offer more quantitative analysis of the system under different network environments and explain the methods of calculating the latency. Moreover, the encryption and authentication methods need to be clearly stated.

## REFERENCES

- [1] Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). Survey on multi-access edge computing for internet of things realization. *IEEE Communications Surveys & Tutorials*, 20(4), 2961-2991.
- [2] Baziana, P. A. (2024). Optical data center networking: A comprehensive review on traffic, switching, bandwidth allocation, and challenges. *IEEE Access*, 12, 186413-186444.
- [3] Jain, S., Gupta, S., Sreelakshmi, K. K., & Rodrigues, J. J. (2022). Fog computing in enabling 5G-driven emerging technologies for development of sustainable smart city infrastructures. *Cluster Computing*, 25(2), 1111-1154.
- [4] Andriulo, F. C., Fiore, M., Mongiello, M., Traversa, E., & Zizzo, V. (2024, September). Edge computing and cloud computing for internet of things: A review. In *Informatics* (Vol. 11, No. 4, p. 71). MDPI.
- [5] Trigka, M., & Dritsas, E. (2025). Edge and cloud computing in smart cities. *Future Internet*, 17(3), 118.
- [6] Jamil, B., Ijaz, H., Shojafar, M., Munir, K., & Buyya, R. (2022). Resource allocation and task scheduling in fog computing and internet of everything environments: A taxonomy, review, and future directions. *ACM Computing Surveys (CSUR)*, 54(11s), 1-38.
- [7] Nemati, A. M., & Mansouri, N. (2025). Resource allocation in fog computing: a survey on current state and research challenges. *Knowledge and Information Systems*, 67(3), 2091-2170.
- [8] Coll-Perales, B., Lucas-Estañ, M. C., Shimizu, T., Gozalvez, J., Higuchi, T., Avedisov, S., ... & Sepulcre, M. (2022). End-to-end V2X latency modeling and analysis in 5G networks. *IEEE Transactions on Vehicular Technology*, 72(4), 5094-5109.
- [9] Sefati, S. S., & Halunga, S. (2023). Ultra-reliability and low-latency communications on the internet of things based on 5G network: literature review, classification, and future research view. *Transactions on emerging telecommunications technologies*, 34(6), e4770.
- [10] Mengistu, T. M., Kim, T., & Lin, J. W. (2024). A survey on heterogeneity taxonomy, security and privacy preservation in the integration of IoT, wireless sensor networks and federated learning. *Sensors*, 24(3), 968.
- [11] Hazra, R., Chatterjee, P., Singh, Y., Podder, G., & Das, T. (2024). Data encryption and secure communication protocols. In *Strategies for e-commerce data security: Cloud, blockchain, AI, and machine learning* (pp. 546-570). IGI Global Scientific Publishing.
- [12] Akinkunmi, A. I., & Oladoyinbo, T. O. (2024). The importance of data encryption algorithm in data security. *IOSR Journal of Mobile Computing & Application (IOSR-JMCA)*.
- [13] Nencioni, G., Garroppo, R. G., & Olimid, R. F. (2023). 5G multi-access edge computing: A survey on security, dependability, and performance. *IEEE Access*, 11, 63496-63533.
- [14] Zhang, J., Ouda, A., & Abu-Rukba, R. (2024). Authentication and key agreement protocol in hybrid edge-fog-cloud computing enhanced by 5G networks. *Future Internet*, 16(6), 209.
- [15] Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6), 854-864. doi:10.1109/JIOT.2016.2584538
- [16] Sookhak, M., Yu, F. R., & Choo, K. K. R. (2018). Fog computing for the Internet of Things: Security and privacy issues. *IEEE Consumer Electronics Magazine*, 7(2), 82-86. doi:10.1109/MCE.2018.2798979
- [17] Akamai. (2024). Edge computing and 5G: Emerging technology shaping the future of IT. Akamai Technologies.
- [18] Mao, Y., Zhang, J., & Letaief, K. B. (2017). Mobile edge computing: Survey and research outlook. *IEEE Communications Surveys & Tutorials*, 19(4), 2322-2358.
- [19] Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge architecture and orchestration. *IEEE Communications Surveys & Tutorials*, 19(3), 1657-1681.
- [20] Losant. (2024). Hierarchical edge computing: Practical edge architecture for IIoT.
- [21] Mach, P., & Becvar, Z. (2017). Mobile edge computing: A survey on architecture and computation offloading. *IEEE Communications Surveys & Tutorials*, 19(3), 1628-1656.