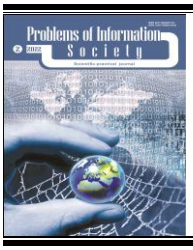

www.jpis.az

13 (2)
2022

# Fog computing technology application in cyber-physical systems and analysis of cybersecurity problems

*Rashid G. Alakbarov[1], Mammad A. Hashimov[2]*

[1, 2]Azerbaijan National Academy of Sciences, Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

[1]t.direktor_muavini@iit.science.az; [2]mamedhashimov@gmail.com

*orcid.org/0000-0002-7566-371X [1], orcid.org/0000-0001-5982-8986[2]*

**ARTICLE INFO**

*http://doi.org/10.25045/jpis.v13.i2.03*

*Article history:*
Received 14 January 2022
Received in revised form
18 Mart 2022
Accepted 19 May 2022

**Keywords:**
Fog computing
Cloud computing
Cyber-physical systems
Fog computing security
Fog computing privacy

**ABSTRACT**

New requirements for modern technologies have become a driving force in the development of information technology. New distributed computing systems are required to handle a large data flow generated by the application of the Internet of Things (IoT) and to ensure their efficient processing. Although cloud computing is an effective technology for processing and storing data generated in a networked environment, it has complications with the real time transmission of large amounts of data due to the low bandwidth of network. To speed up the data processing, fog computing systems have been widely used in recent years. Fog counting systems are one of the proposed solutions for working with IoT devices. Because it can meet the computing needs of multiple devices connected to the network. In these systems, the data is processed at computing nodes located near the data generating devices, which reduces the bandwidth complications of the network channel. In this regard, this article considers the application of fog computing technology in cyber-physical systems. It analyzes the fog technology architecture and its advantages over cloud computing. Cyber security problems arising when using fog technology in cyber-physical systems are analyzed and available protection methods partially solving them are highlighted.

## 1. Introduction

Cyber-physical systems (CPS) connect digital and analog devices, interfaces, networks, computer systems with the physical world. CPS is based on a computer system that processes information in automotive, aviation, energy and other fields. These computer systems are used to perform specific tasks. CPS includes sensors, actuators and similar embedded systems that interact with the real world, as well as sophisticated software. CPS refers to the close interrelationships and relationships between cyber components, such as the sensory systems and physical components forming the basis of the Internet of Things [1].

The main areas covered by CPS are listed below [2, 3]:

- Smart cities: transport, energy distribution, healthcare, environmental monitoring, business, trade, emergency response, waste management;
- Intelligent transport management: operational management of complex traffic flows through real-time data sharing, accident prevention;
- Energy management: Supervisory Control and Data Acquisition (SCADA) systems, smart grid, adaptation and optimization, distribution and consumption of electricity generation;
- Agriculture: precise farming, smart irrigation and more efficient nutrition distribution (fertilization, nitrogen), improved crop production capacity;
- Environment: environmental monitoring in large and diverse geographical areas (forests, rivers and mountains), early detection of natural disasters (forest fires);
- Healthcare: real-time monitoring of patients' health and warning, telemedicine systems for remote delivery of medical services;
- and so forth.

The above-mentioned CPS collects data generated by sensors installed to measure various physical parameters. Since the volume of that data is large to

be handled and tracked, powerful computing resources are required to process it. Cloud technologies with high computing power and memory capabilities are considered to be an effective solution for mentioned data processing.

However, since cloud computing is a centralized computing model, most computing is performed on cloud servers. This means that all information and requests are transmitted in a centralized cloud. Transferring large amounts of data between clouds and data sources is time consuming and expensive. On the other hand, despite the increase in data processing speed, network bandwidth has not increased significantly. Thus, network bandwidth poses problems for cloud computing systems for processing large amounts of data. Currently, edge counting systems are widely used for data sensing and their pre-processing. Consequently, in addition to cloud computing technologies, a new computational paradigm called fog computing is proposed [4]. Fog computing is a computing model performing data processing and application execution at the network boundary, i.e., at computing nodes (as close to the device as possible) rather than in the cloud. The main difference between these two technologies is that the data in the fog computing are processed and analyzed in decentralized fog nodes. Fog nodes can process data without sending it to remote cloud servers. This saves a lot of time during data transmission and ensures real-time responses. Immediate data processing is very important for CPS, especially when decisions or actions need to be made quickly, even a millisecond is of great significance. Thus, fog computing reduces the amount of data required to be sent to the cloud for processing (often because not all data is useful) and accordingly increases the efficiency.

Although fog computing has a number of advantages over cloud computing systems, there are some dangers hindering the application of modern systems when using fog computing. These problems may complicate the successful application of fog computing in CPS. Given that the security is one of the key factors in CPS, especially in critical cyber-physical infrastructures, the identification of cyber security problems of fog technologies and the development of methods to combat them are the most pressing issues today.

In fact, fog computing does not replace cloud computing, it is an improved and expanded version of cloud computing. However, although many ways to address security and data privacy issues in cloud computing are already available, many security and privacy issues related to data and services in cloud computing remain unresolved. Fog computing is based on the computational power of distributed nodes to reduce the overall load of the data center. Since the fog nodes are distributed, centralized control becomes challenging. However, due to various characteristics such as geographical distribution, mobility and heterogeneity, the existing cloud computing security and privacy methods cannot be applied in a fog computing network. This means that new, state-of-the-art security mechanisms are needed to address the security and privacy concerns of fog computing. The goal of this article is to identify future research directions to address various security and privacy issues in fog computing. To this end, the article provides an overview of cyber security problems arising when using fog technology and the methods and tools available to solve them.

## 2. Fog computing technology

The notion fog computing was first used in 2014 by the CISCO Systems employees. Fog and cloud computing runs in an integrated form [5]. Fog computing is closer to the end user, which ensures faster data processing. Thus, fog computing systems are a model of cloud computing systems and consist of multiple computing nodes physically connected directly to devices. The nodes of fog systems are physically closer to the primary data generating sources rather than to the centralized data processing centers. Therefore, they can provide communication with sources faster.

The high computing power of edge nodes allows performing the necessary computing independently without sending large amounts of data to a remote server. Fog computing aims at supporting low latency IoT applications. The main difference between fog and cloud computing is that the cloud is a centralized system, while fog computing has a distributed, decentralized infrastructure. Fog computing systems, on the other hand, intermediate between sensors and remote servers. Fog computing systems determine which data will be sent to the server and which data can be managed locally. Thus, fog computing systems refer to an intelligent system that loads less clouds and provides faster data processing [6].

Sometimes sending data to the cloud for analysis, which requires fast processing, and delays in results delivery can lead to undesirable problems. In some areas (unmanned aerial vehicles, unmanned vehicles,

security cameras, etc.), an immediate and rapid response may be required when driving. Even if decisions are required to be made in the cloud, it is unnecessary and inefficient to send all the data generated to the clouds for processing and storage, since not all of the data generated is useful for decision-making and analysis. Therefore, fog computing is used to quickly control processes in these areas. Fog nodes at network boundaries process and store information generated locally by sensors and devices. This significantly reduces the data transmission over the Internet. This consequently minimizes network latency and provides real-time operations, especially for applications with latency or time constraints [7]. The use of fog computing for driving unmanned vehicles can be the best example. Self-driving cars use thousands of sensors that collect data, and processing of this information in cloud to detect crashes (accidents) and the result delivery can also lead to certain delays. This information should be processed immediately and a decision made instantly. Fog counting systems are used to control such systems. Intel estimates unmanned vehicles to produce 40 TB of data per day. Toyota predicts the sensed data traffic transmitted from cars to the cloud to reach 10 exabytes per month by 2025. Another example is Cloudflare and Akamai, which use content delivery network (CDN) technologies to eliminate network traffic delays. They eliminate network latency by using cached versions of content and hosting them on servers geographically located close to each other. This reduces network latency and provides a closer access point for information [10].

Transferring all data generated from information sources to the data processing center servers is sometimes very expensive, as it requires communication channels with significant bandwidth. Fog computing nodes efficiently handle large amounts of data from sources close to them and transfer only the data that requires additional analysis or long-term storage to the data processing center or cloud. This helps reduce traffic congestion, network bandwidth requirements, and risks when working with confidential information. Restricting the data transmission over the network allows it to be protected from hacker attacks. Applications can be securely used.

Fog computing is expected to replace cloud computing. Although fog computing may theoretically outperform cloud computing, it will evolve with computing clouds. As edge computing technologies develop, so will the cloud. Gartner predicts traditional data processing centers to remain unused by 2025, and 80% of data processing centers to be replaced by infrastructures located closer to the consumer and providing services for them [11].

## 3. Fog computing technology architecture

It should be noted that the fog network does not have a separate architecture and does not replace cloud computing, but complements it being as close as possible to the data source. The hierarchical architecture of the fog computing system is presented in Fig. 1 [3, 12].

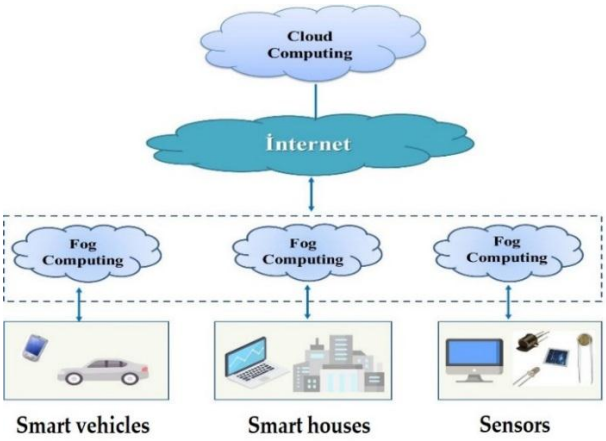


**Fig. 1.** Fog Computing Architecture

**Mobile devices and sensors layer.** This layer is the closest to the end user and the physical environment. It includes a variety of IoT devices, i.e., sensors, cell phones, smart devices, smart cars, smart houses, etc. This layer senses the information about a physical object or event through smart devices and sensors, and then transmits the information collected to a higher layer for processing and storage.

**Fog layer.** This layer is located beyond the boundaries of the cloud computing network. The layer is generally composed of routers, network gateways, computing servers and other nodes. This layer provides a link between the lower layer (mobile devices and sensors) and the cloud layer. Fog-layer computing nodes are capable to process, transmit the data received from mobile devices or sensors to the higher layer and temporarily store the data. Applications used in real-time process analysis and management are performed at this layer. The fog computing system sends them to cloud computing systems to solve the tasks requiring large computing and memory resources. The fog computing system provides a link between cloud computing systems and lower-layer IoT devices.

**Cloud layer.** Numerous high-capacity servers

and memory devices are used at this layer. This layer is provided by servers with high computing and memory capabilities to support the analysis and permanent storage of large amounts of data. The processing result is sent to the fog system via the network. Based on this information, the fog computing system controls the process by manipulating the executive mechanisms.

Fog and Cloud Computing are comparatively analyzed below [13, 14]:

1. Cloud architecture is centralized and consists of large data centers that can be located in different parts of the world, thousands of kilometers away from users. The fog architecture is distributed and consists of millions of small nodes as close as possible to the data generating sources.
2. Fog layer acts as a mediator between the data source and cloud. If there is no fog layer in the system, the cloud communicates directly with data sources, which complicates the process management.
3. Data processing in cloud computing is performed on remote cloud servers. In fog computing, the data processing and storage is performed in real time at the computing nodes located on the edge of the network segment close to the data source.
4. Cloud is more functional than fog due to computing resources and storage capacity.
5. Cloud consists of several large server nodes. The fog contains millions of small nodes and sensors.
6. Fog computing perform analyzes faster because they are located at the network edge, while in cloud computing, servers react late to processes due to being located far away.
7. Delay is less in fog computing and higher in cloud computing.
8. If the Internet is down, the cloud system may crash. Fog computing use different protocols and standards, so the risk of unsustainability is much lower.
9. Fog is a safer system than cloud due to its distributed architecture.

Advantages of fog computing may include [6, 12]:

- short response time to the process (fog system nodes are geographically closer to the sources and can respond instantly);
- high bandwidth of the communication channel (some data is collected at different points and not sent to one center via the same channel);
- impossibility of losing connection (due to numerous alternative communication channels);
- high security (due to the data processing performed by a large number of nodes in the system);
- improved user interface (instant responses and lack of pauses allows users to work comfortably);
- fog computing reduces latency and increases network bandwidth.

Disadvantages of fog counting systems may include [7]:

- ✓ fog computing system is more complex (fog system is an additional layer in the data processing and storage system);
- ✓ additional costs (companies have to purchase peripherals - routers, hubs, gateways);
- ✓ limited scalability (unlike cloud);
- ✓ lack of standard fog computing system architecture;
- ✓ inefficient resource management.

## 4. Cybersecurity problems of fog computing technology

Cloud computing systems are vulnerable to many security threats due to the computing environment and centralized data storage. Its security has become a critical issue limiting its development. On the other hand, its wider edition, i.e., fog, is considered a safer architecture due to the following factors [15]:

1. Collected data is temporarily stored and evaluated at local fog node closest to the data source, thus reducing dependence on the Internet. This complicates the local data storage, sharing and analysis for network attackers to access.
2. There is no real-time data sharing between the cloud and the devices, so it is very difficult for attackers to gain access to any user's personal information.

Fog computing also inherits risks because they inherit many features of cloud computing. Therefore, it cannot be considered completely safe. Some of the security threats that can be used by attackers in fog computing are listed below [16-19]:

• **Malicious Node**: One of the main concerns of fog counting is the presence of fake fog nodes, which can pose a significant threat to data security and privacy. When added to a network, a fake node

infects (disrupts) the entire system by spreading malicious information. This attack can disrupt the operation of the fog network, assemble confidential information, violate the completeness or availability of information, and so forth.

• **Phishing attack:** Users use spam emails or other communication means sent by criminals to capture or destroy important information. It is realized by using the users' interests against them. Here, an attacker can intercept users' confidential information (identity, password) by falsifying users' identification information via infected e-mail and phishing websites.

• **Denial of services (DOS):** Attackers use simple communication protocols to send multiple requests to the node, depleting the fog node resources, thus causing the equipment to stop running. DoS attacks are easier to implement because most devices connected to a fog network are not mutually authenticated. Accordingly, attackers successfully prevent authorized users and devices from accessing the services provided by fog node or even cloud. In short, the attack seriously affects the security of fog and cloud systems. Cybercriminals also perform Distributed DoS (DDoS) attacks, which are very similar to DoS attacks, but performed through more than one computer. In some cases, criminals use both methods at the same time. For example, they first capture target node or nodes through malicious programs, and then perform DoS or DDoS attacks through captured node or nodes.

• **Blackhole Attack:** An unreliable route is created and all data packages are routed to the "black hole". This attack can cause the network to be overloaded and the packages to be dropped. The attacker makes the node look attractive to other nodes during the attack. Thus, all the data flow from any particular node is diverted to the hazardous node, which causes packages to be dropped, i.e., all traffic is stopped and the system believes that the information is received by the other party. It should be noted that a blackhole attack can be organized not only to violate the confidentiality of information transmitted, but also to perform additional attacks (DoS attack, etc.). This leads to more energy consumption.

• **Man-in-the-middle Attack:** One of the most popular attacks in fog computing system is the man-in-the-middle attack. Here, the attacker stands between the fog nodes to snoop to and steal useful information and the authorized users are unaware of this. It is an internal attack and the information from the source node passes through the attacker before reaching the destination, assuming that both the source and the recipient have exchanged information directly. There are two main types of this attack, passive and active. In a passive attack, the attacker is only interested in the information transmitted. Thus, it snoops the packages without changing them, while in an active attack, the attacker manipulates the received packages before directing them to the destination. In the man-in-the-middle attack, a human attack can be performed based on the communication protocols used in the network. Fog devices are often unable to use secure communication protocols due to limited resources. The exact solution to the man-in-the-middle attack is still open, as it is confirmed to be a covert attack on fog computing.

• **Spoofing Attack:** This attack is used by an attacker primarily to gain full access to the fog network and send false information to the network system. Spoofing attacks occur when an attacker appears as an authorized fog device, user, or server to attack a fog system. For example, IP spoofing. In this attack, the attacker may imitate and write the real IP address of other authorized devices, and then send false information to the nodes and devices in the fog network with the obtained real IP address. Devices on the network receive non-original data, which allows attackers to gain full access to the system.

Confidentiality in the collection, processing and transmission of user data through fog nodes is a major concern in fog computing from many points. Confidential information is more difficult to protect since fog nodes are closer to end users to collect sensitive information. None of the users want their information or privacy to be exposed, but no attention is paid to the disclosure of confidentiality under threats or attacks. A person connected to the network can misappropriate and steal confidential information exchanged between users. User privacy includes the followings [20, 21]:

• **Confidentiality of identity.** Fog nodes redirect packages from IoT devices or other fog nodes to other fog nodes or cloud. In this case, the fog node should not be aware of the personal information of users. Anonymity and encryption methods are required to protect users' information and conceal their identities. Therefore, during authentication of fog nodes, the user presents information about own identity (name, phone, home address, passport number, license ID, etc.) to the nodes for verification.

• **Data privacy**. When communicating through fog nodes, users' information may pass into the hands

of outsiders. Such information may include the user's address, personal preferences and political ideology, etc. For example, an online voting system can jeopardize users' political views. The confidentiality of such information is very important.

• **User privacy.** Fog network consists of a large number of IoT devices connected to each other via sensors or wireless communication. The task of IoT devices is to create sensitive data and transmit it to fog nodes for processing. This sensitive information includes personal information, smart home automation information, medical information, business information, etc. and all this information may be stolen by the attacker due to a weak security system.

• **Spatial privacy**. In fog network, the fog node closest to the user is selected. This option is determined by the user's load balance, status, and other criteria. Access to spatial data can be risky for both the user and the fog node. The location of the end user can be easily determined from any fog node, and the location of the fog node can be easily determined from the end user. In addition, spatial data allows us to draw conclusions about a person's social life. For example, smart meter readings violate a user's privacy by indicating when users are sleeping or when they are not at home.

The proposed protection methods to protect data from cyberattacks in Fog Computing environment are listed below [21-24]:

• **Authorization and authentication**. The first safety measure is to identify each node and check that the connected node is genuine. The fog network consists of numerous nodes interacting with different objects at different layers, such as fog to fog, fog to cloud, and fog to IoT devices. The fog network must ensure safe interaction between different devices. This should use the authorization and authentication steps. This is the first step to establish a connection between end user/IoT devices and fog nodes. Authorization is defined as "officially allowed to log in" and Authentication is defined as "confirmation action". The installation phase checks the access rights and identity of the node to be connected to. To access storage and processing services, end users must authenticate with fog node. Because Fog computing is an open network enabling millions of peripheral devices to connect to the network. Hence, it is important to identify each node as a verified one.

• **Decoy Technique**: This is a security method used to authenticate user data available on a computer network. It replaces the original information with the false one, which then passes on to the attackers. When an attacker causes a security breach in the system, it finds a fake data file instead of the original one. This file is known as a decoy file, and the proposed method is called the decoy technique. For security reasons, decoy files are created initially. The system hides the original information, which can only be accessed by authenticated users, and replaces it with a decoy file for intruders by default.

• **Blockchain technology:** This technology has recently been widely used for the secure application of Bitcoin cryptocurrency. The main reason for the success and importance of blockchain technology is that it is decentralized and allows applications to run in distributed way. Obviously, blockchain technology has become a hot topic in recent years, but it is still quite immature in fog computing environment. However, over time, the fog environment safety can be improved by using blockchain technology.

• **Intrusion Detection System (IDS):** An intrusion detection system integrating individual detection components scattered within a fog network should be installed. IDS in Fog computing is used to detect and protect from attacks, including DoS, internal attacks, port scan attacks, flood attacks on virtual machines, man-in-the-middle attacks, hypervisors, and many others. In fog computing, IDS should be deployed at all three architecture layers to track and analyze traffic and behavior of fog nodes, end devices, and cloud servers.

• **Effective encryption methods.** Effective encryption methods solve the privacy problem, because attackers will not be able to decrypt complex encryption algorithms. Recently, homomorphic encryption is gaining more and more attention. Homomorphic Encryption is a cryptographic method enabling to perform computing on encrypted data and maintain confidentiality when processing sensitive data. For example, homomorphic encryption can be used to protect power consumption in Smart Grid systems and to address security and privacy issues in fog computing.

## 5. Conclusion

Cloud computing technologies are widely used in CPS systems to process and store real-time data collected from physical systems and the environment by various sensors. Sensed data often requires rapid processing in terms of solution. For example, data must be processed quickly within seconds and respond to feedback mechanisms. However, the current cloud model is not sufficient to meet these requirements. Using fog computing technologies, it is

possible to improve the quality of cloud services. Thus, the network infrastructure created on Fog computing ensures avoiding the Internet network load as a result of balanced distribution of data between the fog and cloud networks. In this regard, this article examined the prospects for the use of fog computing technologies in CPS, and comparatively analyzed cloud and fog technologies.

The application areas of CPS are of critical importance; hence, special requirements are placed on their safety and reliability. This article analyzed cybersecurity issues when using fog computing systems, and studied the cyber-attacks compromising the fog network efficiency and the user privacy. The available protection methods were explored to prevent these cyber-attacks.

## Acknowledgment

This work supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

## References

1. Alakbarova, I.Y. (2020). The role of cyber-physical systems in Industry 4.0. Problems of the information technology (in Azerbaijani), 2, 91-101. https://DOI.org/10.25045/jpit.v11.i2.09
2. Hong, C. (2017). Applications of Cyber-Physical System: A Literature Review. Journal of Industrial Integration and Management, 2(3), 1-28. https://doi.org/10.1142/S2424862217500129
3. Hashimov, M.A. (2020). Issues of the use of fog technologies in the IoT environment. Problems of the information technology (in Azerbaijani), 2, 80-90. https://doi.org/10.25045/jpit.v11.i2.08
4. Ranesh, K.N., Saurabh, K.G., Andrew, C. (2018). Fog Computing Architecture: Survey and Challenges. arXiv: Distributed, Parallel, and Cluster Computing, 199–223. https://doi.org/10.48550/arXiv.1811.09047
5. Mukherjee, M., Shu, L., Wang, D. (2018). Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges. IEEE Communications Surveys & Tutorials, 20(3), 1826-1857. https://doi.org/10.1109/COMST.2018.2814571
6. Atlam, H.F., Walters, R.J., Wills, G.B. (2018). Fog Computing and the Internet of Things: A Review. Big Data Cognitive Computing Journal, 2(2), 1-18. https://doi.org/10.1109/CSCloudEdgeCom52276.2021.00012
7. Dastjerdi, A.V., Gupta, H., Calheiros, R.N., Ghosh, S.K., Buyya, R. (2016). Fog Computing: principles, architectures, and applications. Internet of Things: Principles and Paradigms. 4, 61–75. https://doi.org/10.48550/arXiv.1601.02752
8. Intel buys driverless car technology firm Mobileye. https://www.bbc.com/news/business-39253422. Accessed on 15 June, 2022.
9. Toyota and Intel headline new car data consortium. https://www.businessinsider.com/toyota-and-intel-headline-new-car-data-consortium-2017-8. Accessed on 15 June, 2022.
10. Meisong, W., Prem, P.J., Ranjan, R., Karan, M. (2015). An Overview of Cloud Based Content Delivery Networks: Research Dimensions and State-of-the-Art. In book: Transactions on Large-Scale Data- and Knowledge-Centered Systems XX, 131-158. https://doi.org/10.1007/978-3-662-46703-9_6
11. The Data Center is Dead. https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead. Accessed on 15 June, 2022.
12. Rahul, N., Urmila, S. (2020). Fog Computing Architecture, Applications and Security Issues. International Journal of Fog Computing, 3(1), 75-105. https://doi.org/10.20944/preprints201903.0145.v1
13. Pengfei, H., Sahraoui, D., Huansheng, N., Tie, Q. (2017). Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues. Journal of Network and Computer Applications, 98, 27-42. https://doi.org/10.1016/j.jnca.2017.09.002.
14. Prakash, P., Darshaun, K.G., Yaazhlene, P., Medidhi, V.G., Vasudha, B. (2017). Fog Computing: Issues, Challenges and Future Directions. International Journal of Electrical and Computer Engineering, 7(6), 3669-3673. https://doi.org/10.11591/ijece.v7i6.pp3669-3673.
15. Aljumah, A., Ahanger, T.A. (2018). Fog Computing and Security Issues: A review," 7th International Conference on Computers Communications and Control (ICCCC), 237-239. https://doi.org/10.1109/ICCCC.2018.8390464.
16. Aleksandr, O., Oliver, L.M., Mikhail, K., Jari, N. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. Sensors, 22(3), pp. 927. https://doi.org/10.3390/s22030927.
17. Deepak, P., Saraju, P. M., Sanjivani, A.B., Graham, M., Rajiv, R. (2019). Fog Computing Security Challenges and Future Directions. IEEE Consumer Electronics Magazine, 8(3), 92-96. https://doi.org/10.1109/MCE.2019.2893674.
18. Yehia, I.A., Ahmad, A.A., Ashraf, J., Valmira, H.O. (2021). FOG computing architecture, benefits, security, and privacy, for the internet of thing applications: An overview. Journal of Theoretical and Applied Information Technology, 99(2), 436-451.
19. Ouns, B., Moayad A., Lewis T., Azzedine B. (2020). Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry. Computer, 53(9), 36-45. https://doi.org/10.1109/MC.2020.2996212
20. Alakbarov, R.A, Hashimov, M.A. (2019). Data Security in Fog Computing. Actual multidisciplinary scientific-practical problems of information security, V Republican Conference, Baku, Azerbaijan, November 29, (in Azerbaijani), 159-162. https://doi.org/10.25045/NCInfoSec.2019.38
21. Ahmed, M.A. (2021). An Overview of Fog Computing and Edge Computing Security and Privacy Issues. Sensors, 21, 8226. https://doi.org/10.3390/s21248226.
22. Mithun, M., Rakesh, M., Lei, S., Leandros, M., Mohamed, A.F., Nikumani, C., Vikas, K. (2017). Security and Privacy in Fog Computing: Challenges. IEEE Access, 5, 19293 – 19304. https://doi.org/10.1109/ACCESS.2017.2749422
23. Neelam, S.K., Mohammad, A.C., (2020). Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review. Scalable Computing: Practice and Experience, 21(3), 515–541. https://doi.org/10.12694/scpe.v21i3.1782.
24. Bushra, Z.A., Munam, A.S. (2017). Fog Computing: Security Issues, Solutions and Robust Practices. Proceedings of the 23rd International Conference on Automation & Computing,1-6. https://doi.org/10.23919/IConAC.2017.8082079.