UDC: 004.735

ANALYSIS OF FOG COMPUTING TECHNOLOGIES

Sadchikova Svetlana Aleksandrovna, Muradova Alevtina Aleksandrovna, Samigov Saddam Murodjonovich
TUIT named after Muhammad al-Khwarizmi, Department of Telecommunication Engineering, Email: a.muradova1982@inbox.ru, +998946126948

Annotation. The article presents an analysis of fog computing technologies. Varieties of this technology, architecture, devices and their application in other areas are considered. A comparison of fog computing and cloud technologies is provided, as well as the advantages and features of each technology.

Keywords: *fog computing, ISO/IEC 20248 standard, cloud computing, Cisco researchers, big data, micro data centers, IoT.*

Аннотация. В статье представлен анализ технологий туманных вычислений. Рассматриваются разновидности этой технологии, архитектура, устройства и их применение в других областях. Приведены сравнение технологий туманных вычислений и облачных технологий, а также преимущества и особенности каждой технологии.

Annotatsiya. Maqolada tumanli hisoblash texnologiyalari tahlili keltirilgan. Ushbu texnologiyaning turlari, arxitekturasi, qurilmalari va ularning boshqa sohalarda qo'llanilishi ko'rib chiqiladi. Tumanli hisoblash va bulutli texnologiyalarni taqqoslash, shuningdek, har bir texnologiyaning afzalliklari va xususiyatlari keltirilgan.

Introduction. Fog computing is a type of horizontal computing architecture used to perform large-scale calculations, store and process data within a network of cloud services and end devices locally and over the Internet. The term “fog computing” originates from the PhD thesis of Professor Jonathan Bar-Magenom Numhauser, published in 2011. In January 2012, Numhauser presented the concept of a new type of computing at the Third International Congress of Silenced Writings at the University of Alcala and published his paper "Fog Computing: An Introduction to the Evolution of Cloud Computing" in the official publication [1].

Fog computing has attracted the attention of a wide audience thanks to the interest of Cisco, which sees it as a new technology that allows for an additional level of interaction between end devices and cloud data centers. On November 19,

2015, Cisco Systems, ARM Holdings, Dell, Intel, Microsoft and Princeton University founded the OpenFog consortium to advance the interests and development of fog computing. The concept of fog computing involves an additional level of working with information both locally and on the global Network, occupying an intermediate position between cloud data centers, end devices and other elements of the data infrastructure. Fog computing, compared to cloud computing, represents another level of data collection and analysis, closer to the user, while edge computing is the point of the described network closest to the end devices [2].

Research object and methods. The fog computing network is represented by two planes (levels) - the control plane and the data plane. For example, in the data plane, fog computing allows computing operators to reside directly at the edge of the network, rather than on servers in data centers. Fog computing in some cases is considered as a quality addition, as well as an alternative to cloud networks. Researchers highlight the following significant advantages of this technology: Low data transfer latency and better connectivity with end devices; Wider geography of networks; Mobility; A very large number of nodes within a network of this type; Improved capabilities for using wireless access technologies; Advanced capabilities for running streaming software and real-time applications; Heterogeneity of computer networks [3].

Fog computing can be considered within the framework of the Internet of Things (IoT), which involves building a network between a large number of devices that people use every day. Such networks may include devices such as mobile phones, wearable health monitoring devices, smart car systems, and augmented reality technology such as Google Glass. SPAWAR, a division of the US Navy, is prototyping and testing a scalable, secure, fault-tolerant network to protect strategic military assets, both fixed and mobile. The software developed by the service, running on network nodes, can quickly restore unhindered control of devices in the event of a loss of Internet connection. Options for using the projected networks for military purposes include, for example, the creation of “smart” swarms of drones.

Research results and their discussion. The ISO/IEC 20248 standard provides a method by which data from objects identified through edge computing using Automatic Identification Data Carriers (AIDC), barcode and/or RFID tag can be read, interpreted, verified and transmitted into the "fog". computing, and then to the periphery, even if the AIDC label has moved. Both cloud and fog computing provide end users with the ability to store and manage data through applications. However, fog computing is “closer” to end users and has a wider geographic

distribution. The very definition of “fog computing” is intended to indicate an additional level of data network architecture, which is located structurally “below” cloud computing, by analogy with clouds and fog, the phenomenon of which can be observed close to the ground.

"Cloud computing" is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than using local services or personal computers. Cloud computing, in some cases, is characterized by greater computing power and maximum density of processed data streams. Fog computing facilitates the operation of information processing and storage services, as well as network services that interconnect between end devices and data centers using cloud technologies; they act as an additional level of information collection and processing. Typically, fog computing is considered as an additional part of the cloud computing infrastructure [4].

Compared to cloud computing, the concept of fog computing is more focused on proximity to end users and their goals (for example, in terms of operating costs, security policies, resource utilization, etc.). This type of computing is also more tightly coupled to the geography of data and its context (relating to computing and IoT resources), reduces latency of data exchange within the network and more economically uses the bandwidth of Internet highways to achieve better quality of experience (QoS). Proponents of fog computing also note improved capabilities for edge analytics and intelligent analysis of information flows within the network of the type described. This makes the user interfaces more efficient and improves network protection against failures, and also allows for a new type of computing in systems for people with disabilities [5].

Fog computing should not be confused with edge computing. Edge computing should be considered as a component, or subset, of fog computing. The difference lies in the fact that edge computing is focused exclusively on local data processing, thus being the final (and closest to the user) link in the ecosystem of “cloud - fog - edge” computing. Fog computing involves not only processing data locally on devices, but also transmitting it to the endpoint. Fog computing can be carried out both in large cloud systems and in big data structures, which is why, in the process of these calculations, there are difficulties in objective access to information. This leads to a decrease in the quality of the results obtained. The impact of fog computing on cloud computing and big data systems may vary. However, all types of fog computing have an inherent limitation in disseminating the results of their operations, a problem that has been solved with the creation of metrics that attempt to improve their accuracy [6].

Scientific research results and conclusion. The main task of fog computing security is to balance the protection of confidentiality, integrity and availability of data, taking into account the feasibility of application and without any damage to infrastructure performance. This is achieved primarily through a multi-step risk management process that identifies fixed and intangible assets, threat sources, vulnerabilities, potential exposure and risk management capabilities. After identifying the critical security issues specific to a particular implementation of the fog computing infrastructure, the necessary security policies are developed, strategies are developed and implemented to reduce the likelihood of risk occurrence and minimize possible negative consequences. This process is accompanied by an assessment of the effectiveness of the risk management plan [7,8].

Fog computing architecture has been officially introduced by Cisco. The fog computing architecture minimizes data transfer overhead, which subsequently improves computing performance on cloud platforms and reduces the need to process and store large amounts of redundant data. The fog computing paradigm is based on the fact that the amount of information required by Internet of Things devices is constantly increasing, and the amount of information (in terms of volume, variety and speed) is also growing due to the ever-expanding number of devices.

The fog computing paradigm can be seen (in a broad sense) as an enabler for many advanced technologies. We can highlight the main functionality provided by fog systems: quick analysis; interoperability between devices; increase or decrease response time; centralized management of IoT devices or control of a specific machine; low bandwidth consumption; efficient energy consumption; device abstraction and many others.

Fog computing is used to improve the usability of the cloud platform and increase its potential. With the advent of widespread applicability of fog and similar technologies such as Edge computing, Cloudlets and Micro-data centers, the number of attacks that can compromise the confidentiality, integrity and availability of information processed is increasing. in them. These issues directly impact the distributed, shared nature of cloud computing. Being a virtualized environment like the cloud, a fog platform can also be affected by the same threats [9,10].

Cisco researchers are using fog computing to improve website performance. Instead of making a round trip for every HTTP request for content, style sheets, redirection, script loading, and image loading, fog nodes can help collect, merge, and execute them. In addition, fog nodes can distinguish users based on MAC

addresses or cookies, monitor and manage user requests, cache files, and determine the state of the local network. Using fog to optimize web services will also lead to website security issues. If user input is not properly validated, the application becomes vulnerable to code injection attacks such as SQL injection. This could result in the entire fog database being compromised or altered information being sent to a central server. Likewise, insecurity in web APIs, session and cookie hijacking (representing the legitimate user), malicious redirects, and drive attacks can compromise the fog and the users within it.

Final conclusion. We can also highlight other areas of application of fog technologies: Virtualized radio access; Collection and pre-processing of speech data; Advanced interaction with AI; Resource management in microcenters; Energy savings in cloud computing; Response to natural disasters and hostile environments.

Although the term fog computing was first coined by Cisco, similar concepts have been researched and developed by other organizations. There are three main technologies and their key differences from fog systems: Edge computing - performs local information processing on the device using programmable automation controllers (PAC). This technology has advantages over fog computing because it reduces the number of points of failure and makes each device more independent. However, the same functionality on end devices makes it difficult to manage and accumulate data in large networks such as IoT. Clouds are the middle part of a three-level hierarchy "mobile device - cloud - cloud". There are four main properties of clouds: it is completely autonomous, it has sufficient computing power but low end-to-end latency, and it is based on standard cloud technology.

Cloud is different from fog computing because application virtualization is not suitable for such an environment as it consumes more resources and cannot operate offline. Micro data centers are small and fully functional data centers containing multiple servers and capable of providing multiple virtual machines. Many technologies, including fog computing, can benefit from micro data centers because the technology reduces latency, improves reliability, is relatively portable, has built-in security protocols, saves bandwidth through data compression, and can accommodate many new services.

List of sources used:

1. Carlos, C., & Maribel, Y.S. (2016).BASIS: A big data architecture for smart cities. *2016 SAI Computing Conference (SAI). IEEE*. 2016-07.
2. Seref, S., & Duygu, S. (2013). Big data: A review. *2013 International Conference on Collaboration Technologies and Systems (CTS). IEEE*. 2013-05.

3. Stojmenovic, I., & Sheng, W. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems*. *IEEE*. 2014-09-29.
4. Yan, Y., & Su, W. (2016). A fog computing solution for advanced metering infrastructure. *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D). IEEE*. 2016-05.
5. Jalali, F., Hinton, K., Ayre, R., Alpcan, T., & Tucker, R.S. (2016). Fog Computing May Help to Save Energy in Cloud Computing. *IEEE Journal on Selected Areas in Communications*. T. 34, #5. Pp.1728-1739.
6. Deng, R., Lu, R., Lai, C., & Luan, T. (2015). Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing. *2015 IEEE International Conference on Communications (ICC). IEEE*. 2015-06.
7. Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing*. T.6, #1.
8. Bierzynski, K., Escobar, A., & Eberl, M. (2017). Cloud, fog and edge: Cooperation for the future. *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). IEEE*. 2017-05.
9. Numhauser, J. (2012). Fog Computing- Introduction to a new Cloud evolution. *Proceedings from the CIES III Congress*, January 2012.
10. Numhauser, J. & Gutierrez de Mesa, J.A. (2013). XMPP Distributed Topology as a Potential Solution for Fog Computing. *6th International Conference on Advances in Mesh Networks, MESH 2013 - Barcelona, Spain*. 2013-08-25. pp. 26-32.