Muratova Polina Vladimirovna
Student
Ural Federal University
Russia, Yekaterinburg
Research advisor: Kovaleva Alexandra

MAINTENANCE OF DATA SECURITY IN THE CLOUD

Abstract: *This study presents the classification of data formats and general provision for data protection in the cloud at each stage. The definition of the term «cloud computing» given by researchers in this field, as well as examples of modern cloud computing are discussed in the paper. The article demonstrates possible variants of work and data protection in a cloud. In the conclusion we present the development of special model of safety for cloud computing.*

Keywords: *data; data security; cloud computing; security of cloud computing; data protection in the cloud.*

Муратова Полина Владимировна
Студент
Уральский федеральный университет
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ В ОБЛАКЕ

Аннотация: *Данная статья представляет классификацию форматов данных и представляет общие положения защиты данных в облаке на каждом этапе. Приведено определение термина «облачных вычислений», данное исследователями в данной области, а также примеры современных облачных вычислений. В статье представлен возможный вариант работы и защиты* *данных в облаке, сделан вывод о разработке специальной модели безопасности для облачных вычислений.*

Ключевые слова: *данные; безопасность данных; облачные вычисления; безопасность облачных технологий; защита данных в облаке.*

Cloud computing has been growing continuously since the 1990s. The concept of cloud computing emerged in the telecommunications industry in the 1990s, when providers began using virtual private networks to transmit data. Cloud computing is basically virtual distributed computing consisting of a data server, i.e. a cluster of servers that remotely distribute services to meet user needs. As the Internet has become an integral part of human life, hardware and software costs have increased. This is also an important point in the development of cloud computing, which has reduced the cost of hardware and software for the client with high flexibility, reliability and minimal time spent [2].

According to the National Institute of Standards and Technology (NIST) [6], cloud computing is defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”. Cloud computing is evolving as one of the most common paradigms in computing, where computing infrastructure and solutions are provided as a service. Mostly Gmail, Office 365, Dropbox are use in cloud computing [1].

Despite the revolution cloud computing has brought challenges in the way computing resources and services are used. The use of such technologies can lead to a catastrophe, as each object can be remotely hacked and controlled by an intruder. Cloud users need to understand the risk of data leakage in the cloud.

As the main purpose of cloud computing is to provide efficient services over the Internet, there are several cloud security issues that prevent its universal adoption, such as cloud storage, which should be protected from unauthorized access, alteration and deletion, thus ensuring data integrity [3]. Classifying cloud computing security issues, reviewing possible threats and methods of data protection in the cloud is important, as cloud computing is one of the most complex computing paradigms available today [4].

There are various important stages in data computing:

1. Transfer of data (transaction)

At this stage, data is transferred from the customer (computing devices) to the supplier (cloud infrastructure) or back. Here the data can be intercepted, which can affect its confidentiality. Encryption is one of the methods used to protect data during transmission.

2. Storage of data

At this stage, the data is stored in the supplier's infrastructure and the supplier is responsible for the security and confidentiality of the data. The supplier should insure the data. In the area of security, confidentiality, integrity and availability are key elements of secure systems. CIA are three important data properties [3]. Confidentiality relates to data privacy, where data is never disclosed to unauthorized persons under any circumstances. Data integrity means ensuring that data stored in the cloud will not be tampered with by unauthorized persons. This also applies when data is transmitted in transit. The availability of data means that whenever the user needs the data, it must be available to them immediately and cannot be denied.

3. Processing of data

At this stage, the data are accessed and processed. In order to develop and implement measures to ensure data security, an authorized person is appointed a structural unit or employee who determines the organizational measures and technical (software and hardware) means of protection. He must use current antivirus protection, block attacks, and ensure the safety of users' workplaces [5].

4. Deletion of data

Another important and often overlooked problem with data is data deletion. After cleaning the storage media, some physical characteristics may be present that allow data recovery. It is the responsibility of the supplier to safely delete the data. You only need to choose a trusted supplier to store data.

Cloud computing is a modern combination of many technologies, making existing problems more complex and demanding.

Reliable, consistent and integrated security models for cloud computing data can be the right stimulus for cloud research. Research on reliable security models is a key factor in the development and deployment of cloud infrastructure.

REFERENCES

1. Raja K, Sabibullah Mohamed Hanifa. Bigdata Driven Cloud Security: A Survey. IOP Conf. Series: Materials Science and Engineering 225. 2017.

2. Mankiran Kaur and Manish Mahajan. An Improved Security Mechanism for Protecting Data in Mobile Cloud Environment. International Journal of Advanced Science and Technology. 2016; № 8: 37-44.

3. Michele De Donno, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone and Manuel Mazzara. Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era. Journal Future Internet. 2019.

4. Security Systems Security and Safety: official website. URL: http://lib.secuteck.ru/articles2/oficial/bezopasnost-personalnyh-dannyh-organizaciya-zaschity-dannyh-pri-ih-obrabotke-v-informacionnyh-sistemah

5. CyberLeninka. Open Access Scientific Digital Library: official website. URL: https://cyberleninka.ru/article/n/metody-povysheniya-bezopasnosti-v-sfere-oblachnyh-tehnologiy/viewer

6. Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Technical Report, 2011.Availableonline:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed on 9 December 2019).