Procedia of Theoretical and Applied Sciences
Volume 8 | Jun 2023
ISSN: 2795-5621 Available: http://procedia.online/index.php/applied/index

CLOUD INFORMATION TECHNOLOGY ANALYSIS

Tojiyev Nuriddin Shukur o‘g‘li
Samarkand Institute of Economics and service, teacher

G‘aniyev G‘iyos G‘ulom o‘g‘li
Samarkand Institute of Economics and service,student

Adilova Dinora Ablaqul qizi
Samarkand State University, student

Abstract: Clouds are the most secure because they are private performed at the stage of creation of encryption and protection tools allows to increase, as well as information of the company will remain in the existing infrastructure. But if the data is in the cloud if not properly secured, the cloud is private or public however, they may be lost or damaged.

***Keywords*:** Cloud, Private Cloud, Public Cloud, Hybrid Cloud, BPaaS, PaaS, SaaS, IaaS.

In recent years, cloud technology or cloud computing has become effective. In some sources, cloud computing is described as a model that allows comprehensive and convenient use of public network computing resources. By now, many experts are of the opinion that the "cloud" surpasses the Internet in terms of its capabilities. The development of cloud computing technology, along with its flexibility and transparency, has become a key factor in creating a universal communication infrastructure that provides efficiency, storage resources, computing resources, data and information [1].

Cloud computing typically provides the user with computer resources and power in the form of an Internet service. In this way, the user is presented with pure computing resources, and the user may not get answers to questions such as what kind of computer is processing his problems, what kind of operating system (OS) is being implemented, and in fact, there will be no need to search for answers to these questions [5].

Currently popular models of cloud computing systems mainly provide three services. Infrastructure as a Service (IaaS) model - infrastructure as a service. In this, physical resources such as servers, network equipment, and data storage devices are provided to users as services. Platform as a Service (PaaS) model - platform as a service. In this case, services are provided to the user through software or web applications. Software as a Service (SaaS) model - applications as a service. It enables users to access and use applications as a service in the cloud and provides services tailored to the user's needs. Consumers do not manage the underlying infrastructure of the cloud, including the network, servers, and operating systems. The end user is solely responsible for the security of access parameters (login, password, etc.) and for following the instructions of the provider for the secure configuration of applications.

At the same time, with the introduction of this technology, the issue of ensuring the security of the information stored in it is also gaining importance. Here we focus on the analysis of existing threats in cloud computing networks and the mechanisms to combat them.

Management and control of cloud computing technologies is one of the main security issues. That is, in this area, a situation has not yet been seen where the elements of the cloud are intact, all resources

Procedia of Theoretical and Applied Sciences
Volume 8 | Jun 2023
ISSN: 2795-5621 Available: http://procedia.online/index.php/applied/index

are accounted for and they are under constant control by virtual machines. This situation is assessed as a high-level threat. In order to increase the level of security reliability, it is necessary to include risk probability management models in the cloud infrastructure. At the same time, there is an increasing demand for strict physical access control to server and network infrastructure based on physical security.

In the first place, the network security model shows security against threats, eliminating them through an inter-network screen [1].

The security requirements of cloud computing are no different from the security requirements of a data center. But the virtualization of the data center and the transition to the cloud environment cause new threats. The processing of large volumes of data is controlled at the physical level, and in the cloud environment they work over the Internet. System-level provisioning of access control restrictions and transparent changes is a key security criterion [3].

Cloud computing servers and local servers use the same operating system and applications. This opens the way for remote hacking or introduction of malicious software for cloud systems. Parallel virtual machines increase the risk of attack. It is important to detect the malicious behavior of protocol-based threats at the level of virtuality. It is necessary to use the security capabilities of local servers by working on virtual machines.

As a basic solution for cloud security, you can get the following:

DOS for a proxy server provides effective protection against this attack;

- Monitoring the integrity of pages for the web server;
- Provide SQL protection for MBBT;
- Use of backup (backup) in data storage devices;
- Restrictions on various uses.

The protection mechanisms listed above have been developed, but they are not integrated into a single environment to provide cloud computing system protection. Therefore, when the cloud is being created, the problem of integrating them into a single system is the impetus to solve the problem.

One of the attacks is Cross Site Scripting, which is based on "stealing" users' passwords, intercepting communication information in the web environment, and similar threats. The defense mechanism against such an attack is the use of clear authentication and encryption at the time of connection (SSL). But this method of protection is very inconvenient and time-consuming for cloud developers.

Interference with the system in managing cloud computing networks causes virtual machines to fail, and by blocking one virtual machine, makes another virtual machine the culprit. One of the most effective ways to ensure cloud security is provided by the Cloud Security Alliance (CSA). This method is based on:

Data storage by encryption.

Security of data transmission. Such technologies are implemented through the most popular algorithms and secure protocols AES, TLS and Ipsec.

Protocols used in authentication protection. It uses LDAP (Light Directory Access Protocol) and SAML (Security Assertion Markup Language) protocols.

Isolation of consumers. For this, the following technologies must be implemented: VPN (Virtual Private Network), VLAN (Virtual Local Area Network) and VPLS (Virtual Private LAN Service).

The main methods of ensuring data protection in cloud computing:

Procedia of Theoretical and Applied Sciences
Volume 8 | Jun 2023
ISSN: 2795-5621 Available: http://procedia.online/index.php/applied/index

- Legal.
- Organizational and technical.
- Economical.

It is important to rely on the above points as the main factor in ensuring information security in cloud computing systems. The issue of information security of cloud computing technologies requires significant improvement and many aspects - priority changes and development. Among the benefits offered by cloud computing, there are currently many security issues that are not well analyzed and are still being discussed.

REFERENCES:

1. Liehuang Zhu • Keke Gai • Meng Li. Blockchain Technology in Internet of Things. Springer Nature Switzerland AG, 2019. – 148 p.
2. Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications. 2013. V. 36. P. 25–41
3. Peter Ghavami. Big Data Analytics Methods: Analytics Techniques in Data Mining, Deep Learning and Natural Language Processing, 2nd edition. Published by Walter de Gruyter Inc., Boston/Berlin, 2020. – 250 p.