CLOUD TECHNOLOGY IN INFORMATION COMMUNICATION SYSTEMS AND ITS SECURITY ANALYSIS

[1]O'rinov Nodirbek Toxirjonovich, [2]Jo'rayev Muhammadjon Durbek o'g'li, [3]Qosimov Shavkatbek Sobirovich

Teacher, Department of Information Technology, Andijan State University[1,2,3]

nodirbekurinov1@gmail.com[1], deejaym2008@gmail.com[2], qosimovdomla8888@gmail.com[3]

ANNOTATION

The current state of the application and development of cloud computing, the main advantages of their use by the state, enterprise and scientific activity are considered. It identifies and analyzes cloud computing information security standards, regulations and guidelines developed by the Cloud Security Alliance (CSA), the European Network and Information Security Agency (ENISA) and the National Institute of Standards and Technology (NIST). It also provides the results of a detailed analysis of issues in the cloud.

Key words: cloud technologies, cloud computing, information security, comparative analysis, disadvantages and advantages of cloud computing.

In recent years, cloud technologies and cloud computing are gaining increasing popularity and efficiency. The latter are defined as models for providing ubiquitous and convenient access through the network to a common pool of computing resources, subject to customization (for example, to communication networks, servers, storage facilities, applications and services) that can be quickly provided and released with minimal operating costs or contacting the provider [1].

Not only large companies that optimize infrastructure costs are showing interest in cloud technologies, but also small firms that are not able to immediately deploy their own structure for data processing. Thus, the main reason for the introduction of such technologies is the economic effect that their use provides. All problems associated with the construction of data centers, the purchase of server and network equipment, hardware and software solutions, as well as ensuring continuity and availability, are shifted to the shoulders of network technology providers. The user only pays for the flexible services provided to him for rent.

Despite the clear advantages of use, cloud technologies require solving problematic issues, the main of which is the degree of trust of the cloud service provider, ensuring confidentiality, integrity, relevance and irrefutability of information at all stages of its existence, business continuity, protection against unauthorized access (NSD) and storing personal data of users transmitted and processed in the cloud. The purpose of this article is to classify and review the major cloud computing technologies, and analyze the current state of use and research in the cloud security industry.

The US National Institute of Standards and Technology (NIST) has proposed a cloud model that consists of five core characteristics, three service models, and four deployment models [1]. Among the main characteristics of the cloud are:

- quality of self-service on demand, when the consumer, without interacting directly with the representative of the service provider, can independently determine and change such computing needs as server time, speed of access and data processing, the amount of stored data, etc. like;

- universality of access using a networkõ, when services are available to consumers through information transmission networks, regardless of the terminal device of client platforms (for example, mobile phones, tablets, laptops and workstations);
- the degree of resource pooling, when a service provider combines resources to serve several consumers using a multi-user model with different physical and virtual resources that are dynamically allocated and redistributed among users in accordance with demand. At the same time, the client does not have the ability to control the location of the resource or does not know the exact location of its location, but is able to indicate the location at a higher level of abstraction (for example, a country, region, or data center). Such resources can play the role of data storage, computing power, memory and network bandwidth.
- sufficient elasticity, when services at any time without additional costs for interaction with the supplier can be provided, expanded, narrowed, as a rule, in automatic mode. For the consumer, such possibilities of the service provider seem to be unlimited and can be provided in any quantity and at any time;
- consumption accounting, when the cloud service automatically manages and optimizes the use of resources by users through measurements at some level of abstraction (for example, the amount of stored data, bandwidth, number of users, number of transactions). Control over resource utilization, the ability to manage resources and the ability to manage resources, and the generation of a consumption report provide transparency for both the provider and the consumer of the service.

In [1], the following service models are also defined using the cloud:

1. Software as a Service (SaaS) is a model where the consumer is given the option of using vendor add-ons that run on the cloud infrastructure. Programs are accessible through different client devices or through a thin client interface or program interface. The consumer does not control or manage the underlying cloud infrastructure, including the network, servers, operating system, storage or even custom add-on capabilities, except for limited custom add-on configuration options, examples of which are Gmail and Google docs.
2. Platform as a Service (PaaS) is a model in which a customer can deploy their own or purchased add-ons on the cloud infrastructure, created using programming languages, libraries, services and tools supported by the vendor. The consumer does not control or manage the underlying cloud infrastructure, including the network, servers, operating system, or storage, but has control over the add-ons deployed and possibly the configuration settings of the environment in which the add-ons run. For example, Google Apps provides online business add-ons that are accessed through an Internet browser, while software and data are stored on Google servers.
3. Infrastructure as a Service (IaaS) - a model in which the consumer is provided with the ability to process, store, access the network and other basic computing resources, where the consumer has the ability to deploy and run arbitrary software, which may include operating systems and programs [2]. The consumer does not control or manage the underlying cloud infrastructure, but has control over operating systems, storage, and deployed add-ons, and possibly limited control over the choice of network components (such as firewalls). The largest players in the infrastructure as a

service market are Amazon, Microsoft, VMWare, Rackspace and RedHat. While some offer more than just infrastructure, they have a common goal of selling basic computing power.

Computing cloud can be deployed as: private, public, public or hybrid [1].

A private cloud is a cloud infrastructure intended to be used exclusively by one organization, which includes several users (for example, departments). A private cloud can be owned, managed and operated by the organization itself or by a third party (or some combination of these). Such a cloud can be physically located both inside and outside the owner's jurisdiction.

A community cloud is a cloud infrastructure designed to be used by a specific community of consumers from organizations with common goals (e.g. mission, security requirements, policy and compliance with various requirements). A public cloud can be jointly owned, operated and operated by one or more community or third party organizations (or some combination of these). Such a cloud can be physically located both inside and outside the owner's jurisdiction.

A public cloud is a cloud infrastructure designed for free use by all users. The public cloud can be owned, operated and operated by commercial, academic (educational and research), or government organizations (or some combination of these). The public cloud is under the jurisdiction of the cloud provider.

A hybrid cloud is a cloud infrastructure consisting of two or more different cloud infrastructures (private, public or public), which remain unique entities, but are interconnected by standardized or private technologies that allow data and application programs to be transferred (for example, using public cloud resources for load balancing between clouds).

Currently, the leading organizations in the field of security in the cloud are the Cloud Security Alliance (CSA), which consists of representatives of the IT industry, as well as two government organizations in Europe and the United States: the European Network and Information Security Agency (ENISA) and the National Institute of Standards and Technology (NIST).

Each of the organizations has created a corresponding document with a classification of all existing information security (IS) problems in the cloud. Let's consider them and make a comparison.

CSA is a non-profit organization founded in late 2008, founded by large IT companies interested in the implementation of cloud technologies: Google, Microsoft, IBM, Salesforce.com, VMWare and others.

The flagship document on security issues in the cloud is the Cloud Computing Critical Areas Security Guide, the first version of which was published in 2009. According to him, the main components of IS requirements in the clouds, which are recommended for consideration and analysis, are the following [3]:

1. Organizational and legal issues of information security;
2. Technical issues of information security.

In addition to information security issues, this document also considers the architecture of building a cloud and provides recommendations and solutions to these problems. In general, information security issues in the cloud are divided into two large groups: the issue of information security management in the cloud

(organizational issues of information security) and information security in the cloud during its use (technical issues of information security). Each of the groups is split into smaller ones, called domains. Domains related to organizational, first of all, are considered with the aim of developing solutions to legal issues, information security policy issues, risk management and standardization. As part of technical issues, issues of implementation and implementation of protection in the cloud are considered.

The European Network and Information Security Agency (ENISA) is an organization whose activities are aimed at "increasing the capacity of the European Union, EU Member States and the business community to prevent, eliminate and respond to network information security problems" [4].

ENISA has prepared and published a document "Cloud computing security and risk assessment" [5], which discusses information security issues in the cloud, their advantages and disadvantages, existing risks, analysis and ways to reduce them, existing threats in the cloud computing environment. According to this document, the following information security risks exist in the cloud:

1. Organizational issues of information security;
2. Legal issues of information security;
3. Technical issues of information security.

To enable cloud computing, the US government commissioned NIST to develop a security and privacy standard for public clouds. Therefore, starting in 2011, NIST published a number of documents that defined cloud computing, considered the issue of information security in the cloud, proposed a security architecture in the cloud, and provided recommendations for assessing and eliminating existing information security risks in the cloud.

The classification of the IS issue in the cloud is discussed in the following NIST documents: "Guide to Security and Privacy in Public Cloud Computing" [6] and "Cloud Computing Brief and Recommendations" [7]. Unlike the considered taxonomies of information security issues in the CSA and ENISA cloud, in the NIST taxonomy, information security issues are not clearly divided into such levels as organizational issues, legal issues and technical issues of information security. In general, they boil down to the following list:

1. Control;
2. Compliance with laws, regulations, standards and specifications;
3. Trust in the service provider;
4. Hardware and software architecture;
5. Identification and access control;
6. Isolation software;
7. Data protection;
8. Availability of resources and data;
9. Response and incidents.

The most complete and structured classification was provided by the CSA organization, but its drawback is the combination of legal and organizational problems of information security. The main advantage of the ENISA classification is the assessment of the likelihood of occurrence of risks associated with

information security, the causes of their occurrence, the relationship with other risks, and their impact on the system and its elements. The disadvantages of the NIST classification include the lack of division of information security problems into three main groups, as was done in the ENISA classification.

Analysis of problematic issues of information protection in the cloud

Most of the problems of protecting user information in the cloud can be solved based on the use of existing methods of cryptographic protection of information, administrative measures on the part of both the cloud service provider and the user, the conclusion of contracts for the provision of services that take into account the individual needs of customers, the adoption of international standards in the industry, the introduction control by the state and the creation of independent experts in this industry.

For example, to ensure the confidentiality and integrity of data stored in the cloud, it is necessary to use digital signature and encryption algorithms that are based on international standards. To prevent unauthorized use of a user profile, existing two-factor user authentication methods can be used.

Nowadays, most providers have their own, sometimes even well-documented, programming interface, but this makes it impossible for users to move from one service provider to another. Practice in such matters shows that only the development of an open single international standard can solve this issue.

The main problems that require further detailed analysis and solution are the following:

a) the problem of privileged users with privileged access to system functions or cloud service administrators. They pose the greatest threat to the security of information in the cloud, and therefore, to reduce the risk of possible destructive actions on their part, it is advisable to conduct independent oversight and control over their actions in the cloud. Statistics show that it is internal users that account for the largest number of security breaches;
b) inconsistency of laws in the field of processing, transfer, storage and protection of information of different states, which is one of the main problems hindering the spread of cloud computing. Solving this problem is key to being able to physically host the servers of the cloud service provider in different countries and regions, as well as for users from different countries to use the same service provider. This problem will most significantly concern transnational corporations;
c) issues of trust in the service provider, which can only be resolved by conducting a security audit of the cloud service provider and verifying that its security system complies with international information security requirements formulated in international standards. Formulation and justification of requirements is one of the important issues;
d) the issues of common vulnerabilities in the cloud are practically the same as in traditional systems, except that a single vulnerability found can be exploited for the entire cloud, but at the same time it can be more easily fixed with a centralized update, as opposed to traditional systems. At this time, its criticality is much greater, because it can easily affect all users of a given service provider, and therefore requires preventive measures and methods of protection;

e) problems of accessibility to services and data by users, their resumption of work after a failure or loss of data should be resolved at the administrative and legal levels. When drafting contracts with the user, the obligations of the parties and the measure of their responsibility should be clearly defined depending on the circumstances of the event that led to these consequences, and the investigation should be carried out by a third independent party. A similar problem exists in traditional systems, but the user has the ability to directly influence the level of redundancy in the system, which makes it possible to more flexibly customize it to the specific requirements of the user and his financial capabilities;

f) the problem of providing access, sharing and blocking access to resources and data in the cloud for users;

g) the challenge of protecting intellectual property in the cloud, in particular software and data.

Advantages and disadvantages of using clouds

The main advantage of using cloud computing, which underlies the technology, is workload balancing, due to which a more efficient use of computing system resources is achieved. The main advantages of the technology include:

- ✓ the ability to access resources in the cloud based on the use of an Internet connection, a regular browser and an undemanding end-user terminal;
- ✓ rapid deployment of proprietary services and / or an increase in the workload on the provider's existing cloud services;
- ✓ support for redundancy, self-recovery and scaling, which allows to increase system reliability and reduce risks in case of software and hardware failures;
- ✓ real-time workload management, including batch operations and background programs that interact with users;
- ✓ real-time monitoring of system load and balance, as well as resource allocation.

In addition to the listed advantages, there are disadvantages and problematic issues that hinder the implementation of cloud computing, namely:

- ✓ impossibility of working with cloud services without a permanent connection to the Internet;
- ✓ Difficult or impossible transition from one cloud provider to another;
- ✓ lack of a single international legal regulation in the field of cloud computing and information processing in the cloud;
- ✓ trust in the user service provider;
- ✓ the issue of protecting user information processed and stored in the cloud.

To ensure the security of information, cloud computing provides the following advantages:

- ✓ specialized staff: a cloud provider, like a large organization, hires information security industry experts to provide security in the cloud, allowing employees to focus exclusively on security, achieving a high level of security that cannot be achieved in a small organization;

- ✓ centralized management, configuration of the security system and its audit;
- ✓ platform resilience: the hardware and software composition of the platform on which the cloud is deployed more evenly than in most traditional computing centers, which allows for better automation of security, testing and bug fixes in platform components;
- ✓ availability of resources: the ability to dynamically scale system resources, as well as redundancy and emergency recovery, which can be used to increase the system's resilience against denial-of-service attacks, as well as to quickly resume serious incidents later;
- ✓ Backup and Resume: A cloud provider can enable higher backup and resume levels than traditional datacenters and provide geographic backup storage.
- ✓ end-customer mobility: thanks to the cloud architecture, customers can use a variety of portable devices with low computing power, Internet access, a browser and / or several installed add-ons, to gain access to basic computing resources;
- ✓ data concentration: using the cloud as the only place for storing and processing data in some cases can improve security than storing data that is dispersed across laptops, embedded devices, or stored on removable media.

The disadvantages of using cloud computing in terms of information security include:

- ✓ Complexity of the system - A shared cloud is usually complex compared to a traditional data center. The large number of components that make up the cloud allows attacks to be carried out at different levels of abstraction. In addition to components for general computing, such as add-on deployment, virtual machine monitors, guest virtual machines, there are also components in data storage that include controls: self-service, resource accounting, quota management, data replication and resumption, service level monitoring, workload management;
- ✓ general multi-user environment: the main disadvantage of public clouds, manifested in the fact that users share resources and components with users that they do not know at a logical level, which allows an attacker, using vulnerabilities inside the cloud, to overcome the mechanism of resource allocation between users and gain unauthorized access to resources. The homogeneity of the software and hardware composition of the platform means that the only flaw will manifest itself in the entire cloud and will potentially affect all users of the service;
- ✓ Internet usage: cloud services, as well as administration and management of cloud services and add-ons settings, use an unsecured Internet network. As an organization moves to cloud computing for internal secure networks and resources, new information threats emerge that need to be addressed. There is also a need for remote administration using an unprotected information transmission channel;
- ✓ loss of control: when using cloud services, the user transfers control over the information to the cloud provider, which carries additional risks to the security of information. The user becomes dependent on the cloud provider and may lose not only logical control over information, but also physical control.

With the totality of the benefits that cloud computing provides, there are many security issues that have not yet been analyzed well enough and are still under discussion.

As shown in the article, the main problem that has not been resolved in the cloud computing industry today is user trust in the service provider. This problem is acute not only for companies and enterprises that use third-party suppliers, but also for ordinary users, whose personal data also needs protection and security guarantees. While in the case of a large enterprise it can protect itself from threats by conducting a security audit of a cloud service provider and analyzing information security risks and threats, and insuring them or creating their own private cloud, then small companies or ordinary users do not have this opportunity. Therefore, it is necessary to implement control mechanisms of cloud service providers at the international level or at the state level in order to conduct a security audit and verify their compliance with international or national standards and the conditions put forward to them.

REFERENCES

1. The NIST Definition of Cloud Computing. NIST Special Publication. 2011. P. 800-145.
2. Dovgal VA Features of realization of safe connection to cloudy services // The Bulletin of the Adyghe State University. Ser. Natural- Mathematical and Technical Sciences. 2015. Iss. 1 (154). P. 128-135. URL: http://vestnik.adygnet.ru
3. Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011. URL: http://www.cloudsecurityalliance.org/guidance/csa guide.v3.0.pdf
4. Catteddu D., Hogben G. Cloud Computing Information Assurance Framework. Technical report, European Network and Information Security Agency. 2009. November. URL: http://www.enisa.europa.eu/activities/risk-management/files/deliverables / a loud- with omputing-information-assurance-framework
5. Catteddu D., Hogben G. Cloud Computing Security Risk Assessment. Technical report, European Network and Information Security Agency. 2009. November. URL: http://www.enisa.europa.eu/activities/risk- management / files / deliverables / cloudcomputing-risk-assessment
6. Wayne Jansen, Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication. 2011.800-144. URL: http://csrc.nist.gov/publications/nistpubs/800-144 / SP800-144.pdf
7. Lee Badger Cloud Computing Synopsis and Recommendations NIST Special Publication 800-146 / L. Badger, T. Grance, R. Patt-Corner, J. Voas. 2012. url: http://csrc.nist.gov/publications/nistpubs/800-146 / sp800-146.pdf