AMERICAN JOURNALS
Open Access,
Peer Reviewed Journals

ANALYSIS OF EXISTING RISKS AND METHODS OF COMBATING THEM IN CLOUD TECHNOLOGIES

Shodiyev Rizamat Davronovich
Professor of Karshi State University

Ergashev Nuriddin Gayratovich
Professor of Karshi Engineering Economics Institute

ABSTRACT

This article provides an analysis of current threats and mechanisms in cloud technologies. In addition, clouds name, computer systems, all of the computers within the same network, are analyzed in clouds to display information within it. Each computer is not considered as an independent unit, but a whole system. In general, the user is provided directly to work directly to work. All network resources available through servers are illuminated.

Modern information technologies often play a major role in the success of all areas. There are a number of means and options that allow us to use full power of cloudy technologies. The concept of cloudy technologies is really important because it can become a turn point of doing business and take it to a completely new level. This means that it can bring income not only for businesses, but also for the state.

KEYWORDS

Cloud, Cloud ACCESS Security, Saas (Virtual-AS-Service, DOS (DENAL-AS-Service, DOS (DENAL-USER), Hypervizor, Cloud Security Alliance (CSA)) and others.

Introduction

Cloud computing security is a set of technologies and strategies that help protect cloud data, applications, infrastructure in organizations as well as meet standards [1].

Identity management, privacy, and access control are especially important for cloud security. Because cloud systems are generally common and are available on Internet sources. Since it is typically used for continuous daily activities from cloud computing and public cloud providers, security measures related to cloud computing as well as vulnerability mitigation should be prioritized [1].

Cloud computing security processes must take into account the security measures provided by the cloud service providers, and organizations must understand the distribution of responsibility between the cloud service provider and the cloud user. In order to prepare for a possible breach of cloud security, it is necessary to ensure the continuity of the business and standardize the processes for the backup of cloud data.

Purpose

Cloud computing security-cloud security belongs to the lower categories of computer security, or network security in the broader category of Information Security. Cloud security is concerned with a set of policies, management tools, or security measures developed specifically to provide data, applications, and infrastructure in the cloud. Cloud Access Security, on the other hand, can be defined as a topic that takes into account where the data in the cloud security context is located and the right to access it through the cloud. Most often, it deals with the provision of an identity management system for cloud users.

Literature Analysis

One of the technologies that we are developing today is Cloud computing. The idea of such calculations was first proposed in 1961 by John McCarthy (John McCarthy). That is, its computing power is provided to users as a service [1].

In 1963 year J.S.R.Licklider began to study the idea of the global existence of a computer network. In his opinion, a global existing network allows a person to access computer programs and information from anywhere in the World [2]. He formulated the oldest ideas of the global computer network. As a result**,** the network space appeared, where today there are cloud services.

Theoretical Basis

Cloud security is a sub-branch of emerging computer or network security that works with cloud content security tools through a variety of management and infrastructure. Cloud-based security, however, has nothing to do with cloud-based security measures and vulnerability management software provided through a cloud-based antivirus or security service. It is segmented into the challenges that cloud security providers and cloud customers face. Cloud providers are responsible for delivering software, platform, or infrastructure as a cloud-based customer service. Cloud service providers need to make sure that their customers' applications and data are protected. At the same time, it is the responsibility of the customer that the service provider takes the right measures to protect the information. Cloud security challenges are divided into three main categories. That is, security and privacy, compliance and legal issues. To ensure data security and its confidentiality, a number of measures such as data protection measures, identity management systems, physical and personal security measures, high level of assurance measures, application-level security measures and data masking measures are used. To ensure compliance, service providers must comply with many data storage regulations, such as the PCI DSS (payment cards industry safety standard), HIPAA(Health Insurance capability and Liability Act), and the Sarbanes-Oksley act. They require regular inspection and reporting procedures. When it comes to legal and contractual issues, there should be agreements between providers and customers on liability, intellectual property and terms of service termination.

Cloud access security. Cloud access security can be defined as the Lower Zone of cloud security. This is due to who is allowed access to this information. Access security is a very important issue in public clouds, where many service providers provide shared services. Identity management systems are mandatory in any cloud. These systems can be either client identification management systems connected to the cloud, or systems provided by the service providers themselves. If one access technology is used between different SaaS (Software-as-a-Service) providers, the user can use the same credentials when accessing all systems. To eliminate the great risk of abuse of access rights by service provider administrators, customers can install event logging monitoring tools.

What is the difference between Cloud Security and Cloud Access Security? Cloud security is an area of computer security that deals with protecting cloud content using a variety of policies, controls, and infrastructures. Cloud security is divided into different sizes, and cloud access security is one of its most important dimensions. Cloud access security is concerned with ensuring cloud content protection. Ensuring cloud access security is critical to ensuring cloud security.Because it eliminates the possibility of unauthorized, unapproved users accessing data in the cloud and compromising the security and privacy of the data stored in the cloud.

When we say threat intelligence to cloud technology is compromised, cloud management and control are understood as the main security challenges. In cloud technologies, all resources are under constant control by virtual machines. This is considered a high-profile threat, it is associated with Cloud Management, serves as a single Information System, and it will need to build its overall protection at a high level.

For this, of course, it will be necessary to apply risk probability management models in the cloud infrastructure. On the basis of physical security, it would be necessary to have strict control over access to the server and network infrastructure. With regard to physical security, network security is in the first place. This model incorporates security against threats and eliminates them through the firewall. The firewall acts as a filter and restricts the use of the data center network. In this case, separate servers, that is, from those that are allowed to be used on the Internet, or servers within the network. Virtualization as a platform plays the main role in cloud computing.

Results and Discussion

We analyze the most common threats to ensure data integrity and security in cloud computing. There are several challenges in deploying cloud servers in cloud computing. The security requirements of cloud computing are no different from the security requirements of a data center. But the virtualization of the data processing center and the transition to the cloud environment cause new threats to appear. Controlling computing power over the Internet is one of the key characteristics of cloud computing. In many traditional data centers, engineers use servers that are controlled on a physical scale, and in a cloud environment, they operate over the Internet. System-level provisioning of access-controlled restrictions and transparent changes is critical protection.

Dynamics of virtual machines. Creating a new car, stop and restarting can be done in a short time. They can interfere with physical servers. Such changes make the system difficulty processing the security integrity. However, the vulnerability of the operating system or apps is uncontrolled in the virtual environments and begins to quickly spread in a certain period of time (for example, backup. In a cloudy computer environment, first of all, correct the system security status, it should be taken into account that its status and storage should not depend on it.

Vulnerabilities in the internal virtual environment. Cloud computing servers and local servers use the same operating system and applications. Remote hacking or malware threats are common to cloud systems. Parallel virtual machines increase the risk of attack. Protocol-based threats and mitigation protocols must detect malicious activity at the virtual level.

Protection of unused virtual machines. When the virtual machine is not active, the risk of damage is greater. Access to stored images on Virtual machines will be enough. On a virtual machine that has not started, it is impossible to start the software security, in general. In this case, not only should internal security be implemented on the virtual machine, but also at the level of the hypervisor(the hypervisor is the computer that manages one or more virtual machines).

Zone security and network restriction. When using cloud computing, the zone network slows down or disappears from sight altogether. As a result, security is not at a high level, and the network part determines the overall security level. In the cloud, virtual machines will have to provide their own security when limiting segments to different levels of reliability.

Attacks carried out through cloud technology and their elimination. Traditional attacks on software this operating system, the vulnerability of network protokols, are considered traditional threats. In order to ensure protection, problems can be solved by installing a firewall, antivirus, IPS and other components[5]. It should be taken into account that such a way of protection should also work effectively in the development.

Functional attacks on Cloud Elements. This type of attack is multipath1i with the cloud due to a common security printzip. On cloud security, the following can be obtained as a solution: when protecting against functional attacks, the following sources of protection should be placed on each cloud partition: DoS for proxy(Denial-of-Service-temporary suspension of the activity of the attacking server), ensuring effective protection from attack, controlling the integrity of pages for the web server, for server applications - applications on-screen, DBMS (Data Base Management System) for SQL(Structured Query Language)Protection, data storage system to give the right back-ups (backup), restrict access, etc. The above listed protections have been produced, but they have not yet been assembled together to provide cloud-based protection. Therefore, at the time of creation of the cloud, integrating them into a single system will be an impetus to the solution of the problem.

Many customers use the browser when connecting to the cloud. One of the attacks is Cross Site Scripting, “stealing” passwords, capturing web sessions, and so on. The only correct and protection from such an attack is mutual authentication with clear authentication and encryption of connections (SSL-Secure Sockets Layer). But such a method of protection is much more inconvenient and time-consuming to the creators of the cloud.

Attacks on the hypervisor. Hypervisor is one of the key elements for virtual systems. One of its main functions is the distribution of resources to virtual machines. An attack on the hypervisor can result in the fact that one of the virtual machines can take advantage of the memory, resources of another virtual machine. It can also capture utarmak traffic, absorb physical resources and stop the virtual machine from running through the server. They recommend the use of the necessary specialized products in the virtual environment in the implementation of standard protection techniques. Integration of host servers with Directory Services Active Directory(a bright database and a suite of services and tools that deploy devices to connect to a specific network), as well as standardize the procedure for using host server management tools. At the same time, denial of Service, which in most cases is not used, for example, virtualization web access to the server.

Attacks on the control system. Many virtual machines used in the cloud require separate system administration. Disrupting the control system in the virtual machines - it causes malfunctions, and by blocking one virtual machine, it makes another virtual machine guilty.

One of the most effective security solutions in the cloud industry, Cloud Security Alliance (CSA), was referred to by the public, in which the following data were analyzed:

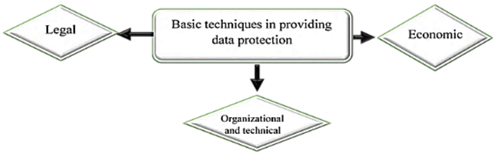
Data storage. Encryption is one of the most effective methods of data protection. The provider, which allows access to the data, must encrypt the client data stored in the data processing center, and when it comes to the use, delete them without a return.

Data security in transmission. The transmission of encrypted data can only be carried out after aytenification. Reading or changing data, their use is carried out through reliable connections. Such technologies are very well-known algorithms and reliable protokollar AES(protected form of information encryption), TLS(ensuring the confidentiality of information), Ipsec(security of the internet protocol).

Autetification. Password protection. When ensuring reliability, attention is paid to tokens and certificates. The provider should act transparently when passing authorization with the identification system. It uses LDAP (Light Directory Access Protokol) and SAML (Security Association Markup Language) protokol.

Consumer insulation.Individual use of Virtual machines and virtual networks. The following technologies should be introduced in Virtual networks. VPN (Virtual Private Network), VLAN (Virtual Local Area Network) and VPLS (Virtual Private LAN Service). Providers often isolate consumer data from each other because of code changes in a single application environment. Such an approach is considered dangerous, it is able to find a way out of a non-standard code and use the data of the client.

Key techniques in securing data protection in cloud technologies.


Legal
Basic techniques in providing data protection
Economic
Organizational and technical

1-picture. Key in providing data protection in cloud technologies techniques.

Legal techniques. Legal techniques include the production of regulatory acts, including ensuring the safety and regulation of information relations between participants and normative - methodical documents, provision of Information Security, etc.

The most important activities of these include:

- timely amendments and amendments to the state legislation, regulations in the field of Information Security;
- elimination of conflicts related to international treaties;
- establishing responsibility for violations;
- limitation of powers in the field of Information Security;
- development and adoption of regulatory and legal acts.

Organizational and technical activities. Such techniques include the following:

- creation and modernization of information security system;
- effective use of tools in production, information protection and control techniques;
- to identify the risks arising from technical devices and applications in ensuring information security;
- certification of information security tools;
- control of personnel behavior in protected information systems;
- formation of system monitoring indicators and information security characteristics;

Economic activity. Economic methods include the following security:

- development of information security plans;
- financing of system improvement works together with organizational rights and

organizational and technical techniques.

Service level adaptation. Currently, legal normative acts, the absence of rules for the regulation of cloud resources, adaptation to the level of Service, are considered one of the most important criteria of cloud computing providers[7]. Unfortunately, at the moment, many providers make the adaptation at the service level so that they receive little responsibility for themselves as a result. Proceeding from this, before using confidential information in cloud computing, it is necessary to choose providers that are well adapted to the level of service.

Set up a cloud security channel up to the system. When communicating with the system in the cloud, the channel is encrypted. When installing security channels, VPN (virtual personal network) technologies are used. Nevertheless, that is, the presence of lower bounce reliability of telecommunications in the network, and the confidence in the channel remains high. Depends on the use of cryptographic tools (encryption, authentication, open-key infrastructure and the Prevention of changing the data being sent). This method is the simplest and most reliable.It protects against MITM (Man in the middle) attacks. But this method only protects the system and channel communication in the cloud. Information passing through the entire system is considered open.

Protection technology. Cloud protection strategy in the IT(Internet technology) industry allows to ensure a very high level. At the same time it is considered to have the highest standards of protection of personal data. ”Cloud computing " allows you to determine the requirements for each structural level, setting the area of participants at all times. Today, measures for the implementation of such requirements are being found. The main emphasis should be on the use of reliable distribution and operation software.

The most common risks in cloud environments are theft of virtual machines from a state of running state, modifications to the network topology of the IT infrastructure using only application parameters, such as direct access to network protections in IT-related attacks. This risk is reduced due to the protection of the virtual environment at all stages of its construction. That is, they are: within the framework of virtual infrastructure, system administration and storage, hardware, system software graph (hypervisor), etc.

Provide customers with hardware and software. Until now, the consumer will not come up with any problems in the approach of software and hardware tools for encrypting IP - streams over SSL protokol at work.Speed, processing can output up to a dozen Mbit/t. Currently, theififikatsiyleş frirme, which provides such services, is considered sufficient. The keys in consumer operating systems and the protection of personal information in the corporate cloud are one of the major challenges in ensuring information security. An electronic lock is installed on the consumer's personal computers. Such locking can be controlled not only by the consumer, but also by the company's information security service. But all this is only available in the private cloud, and the social cloud does not have these opportunities.

Hypervisor, as a software tool, manages hardware resources and allocates resources between guest operating systems. It is therefore the most vulnerable part of the virtual environment. Any broken status of it, the guest will cause a malfunction in the operating system. Taking advantage of the hypervisor brings in its place a variety of opportunities to evil-minded individuals. From a data point of view, such access provides an opportunity to control all information flows that pass through the hypervisor. Such opportunities give the right to general use of the virtual environment, namely: the administrator of the virtual structure will have the right to use any information without restriction.

Therefore, the security of information resources can be solved in a virtual environment. Logical virtual infrastructure does not differ from physical infrastructure. Accordingly, the threats in the first are considered relevant in the second. Then the media should be able to provide virtual infrastructure protection, optimization of hardware resources. The use of information protections for rational purposes in multi-volume virtual infrastructures helps to build at the hypervisor level. The main risk probability in the cloud occurs throughualualization specification, the emergence of new entities - the cloud management system and the systemualualization. Compromising one of them is equivalent to risking cloud security. Virtual machines on physical servers in a Virtual environment can be quite a lot. Virt if a simple antivirus is installed on the operating system of the upgraded server, 100 copies of the antivirus on one physical hypervisor will occur. Each copy will have its own antivirus signature, legal guardian: all this must be updated on time on all virtual machines. This results in a new extra weight being added to the hypervisor, and physical server resources are beginning to be wasted inefficiently.

Conclusions and Suggestions

The above solutions do their job by checking communications between virtual machines and analyzing traffic from attacks occurring at the hypervisor level. Therefore, in the trading market, new products that are produced for theualualization environment begin to appear. Undoubtedly, they work very efficiently and have the most stringent facilities in management.

Regardless of the location of the cloud-based technology, it allows users to collaborate with an ever-growing circle of users. These technologies deliver information in an economical and reliable way and are characterized by Ease of distribution and updating. Cloud-based technologies that allow information to overcome existing barriers, these are geographic, technological, social, etc.

The introduction of cloud technologies not only reduces the cost of purchasing the necessary software, but also increases the quality and efficiency of the production process, as well as the openness of data.

REFERENCES

1. Shodiev, R. D. Methods and Forms to Ensure Understanding in Educational Process. Eastern European Scientific Journal. DOI, 10, 4.
2. Gayratovich, E. N. (2019). USING VISUAL PROGRAM TECHNOLOGY METHODS IN ENGINEERING EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol, 7(10).
3. Gayratovich, E. N. (2021). SPECIFIC ASPECTS OF EDUCATIONAL MATERIAL DEMONSTRATION ON THE BASIS OF VISUAL TECHNOLOGIES. International Engineering Journal For Research & Development, 6, 3-3.
4. G‘ayratovich, E. N. (2022). It Is A Modern Educational Model Based On The Integration Of Knowledge. Eurasian Scientific Herald, 5, 52-55.
5. G‘ayratovich, E. N. (2022). The Theory of the Use of Cloud Technologies in the Implementation of Hierarchical Preparation of Engineers. Eurasian Research Bulletin, 7, 18-21.
6. Gayratovich, E. N., & Yuldashevna, T. O. (2020). Use of visualized electronic textbooks to increase the effectiveness of teaching foreign languages. European Journal of Research and Reflection in Educational Sciences Vol, 8, 12.
7. Ergashev, N. (2021). METHODS OF USING VISUALIZED EDUCATIONAL MATERIALS

IN TEACHING PROGRAMMING LANGUAGES IN TECHNICAL UNIVERSITIES. INNOVATION IN THE MODERN EDUCATION SYSTEM.

8. Ergashev, N. (2020). Didactic fundamentals of electronic books visualization. An International Multidisciplinary Research Journal.
9. Ergashev, N. (2020). Using the capabilities of modern programming languages in solving problems of technical specialties. An International Multidisciplinary Research Journal.
10. Ergashev, N. (2021). ЎКУВ МАТЕРИАЛИНИ ВИЗУАЛ ТЕХНОЛОГИЯЛАР АСОСИДА НАМОЙИШ ЭТИШНИНГ ЎЗИГА ХОС АСПЕКТЛАРИ. Scienceweb academic papers collection.
11. Ergashev, N. (2022, May). FEATURES OF MULTI-STAGE TRAINING OF TEACHERS'CONTENT TO PROFESSIONAL ACTIVITIES USING CLOUD TECHNOLOGY IN THE CONDITIONS OF DIGITAL EDUCATION. In International Conference on Problems of Improving Education and Science (Vol. 1, No. 02).
12. Ergashev, N. (2022, May). THEORETICAL STAFF TRAINING USING CLOUD TECHNOLOGY IN CONTINUING EDUCATION. In International Conference on Problems of Improving Education and Science (Vol. 1, No. 02).
13. Ergashev, N. (2022, May). PROBLEMS OF USING DIGITAL EDUCATION IN PEDAGOGICAL THEORY AND PRACTICE. In International Conference on Problems of Improving Education and Science (Vol. 1, No. 02).
14. Ergashev, N. (2022, May). THEORY OF TRAINING OF PEDAGOGICAL PERSONNEL IN HIGHER EDUCATION USING CLOUD TECHNOLOGIES IN THE CONDITIONS OF DIGITAL EDUCATION. In International Conference on Problems of Improving Education and Science (Vol. 1, No. 02).
15. Ergashev, N. (2022, May). PROBLEMS OF DIGITAL EDUCATION IN PEDAGOGICAL THEORY AND PRACTICE. In International Conference on Problems of Improving Education and Science (Vol. 1, No. 02).
16. Ergashev, N. (2021). METHODS OF USING VISUALIZED EDUCATIONAL MATERIALS IN TEACHING PROGRAMMING LANGUAGES IN TECHNICAL UNIVERSITIES. INNOVATION IN THE MODERN EDUCATION SYSTEM.
17. G'ayratovich, E. N. (2022). The Problem of Training Future Engineer Personnel on the Basis of Cloud Technology in Technical Specialties of Higher Education. Eurasian Scientific Herald, 13, 1-4.
18. Ergashev, N. (2021). ЎКУВ МАТЕРИАЛИНИ ВИЗУАЛ ТЕХНОЛОГИЯЛАР АСОСИДА НАМОЙИШ ЭТИШНИНГ ЎЗИГА ХОС АСПЕКТЛАРИ. Scienceweb academic papers collection.
19. Gayratovich, E. N., & Jovliyevich, K. B. (2023). Theory and Methodology of Software Modeling Using the Web Platform. Eurasian Scientific Herald, 16, 59-63.
20. Ergashev, N. (2023). Bulutli texnologıyalarda mavjud tahdidlar, ularga qarshi kurashish mexanizmları va metodlari. Electron Library Karshi EEI, 1(01). Retrieved from https://ojs.qmii.uz/index.php/el/article/view/273
21. Ergashev, N. (2023). ОЛИЙ ТАЪЛИМ ТЕХНИКА ИХТИСОСЛИКЛАРИ ЎҚУВ МАТЕРИАЛЛАРИНИ ДАСТУРИЙ ВИЗУАЛЛАШТИРИШНИНГ ИЛМИЙНАЗАРИЙ АСОСЛАРИ. Electron Library Karshi EEI, 1(01). Retrieved from

https://ojs.qmii.uz/index.php/el/article/view/270

22. Ergashev, N. (2023). Texnika ixtisosliklari mutaxassislik masalalarini yechishda C++ visual dasturlash tilida klasslardan foydalanish tahlili. Electron Library Karshi EEI, 1(01). Retrieved from https://ojs.qmii.uz/index.php/el/article/view/272
23. Ergashev, N. (2023). Methods of teaching parallel programming methods in higher education. Electron Library Karshi EEI, 1(01). Retrieved from https://ojs.qmii.uz/index.php/el/article/view/271
24. Ergashev, N. (2023). Raqamli ta'lim sharoitida bulutli texnologiyalar yordamida oʻqituvchilarni kasbiy faoliyatga koʻp bosqichli tayyorlashning nazariy aspektlari. Electron Library Karshi EEI, 1(01). Retrieved from https://ojs.qmii.uz/index.php/el/article/view/274
25. ERGASHEV, N. THE ANALYSIS OF THE USE OF CLASSES IN C++ VISUAL PROGRAMMING IN SOLVING THE SPECIALTY ISSUES OF TECHNICAL SPECIALTIES. http://science. nuu. uz/uzmu. php.
26. Ergashev, N. (2022). Ergashev Nuriddin G'ayratovich Oliy ta'lim texnika ixtisosliklarida raqamli ta'lim asosida bo 'lajak muxandis kadrlarni tayyorlash muammosi: oliy ta'lim texnika ixtisosliklarida raqamli ta'lim asosida bo 'lajak muxandis kadrlarni tayyorlash muammosi. E-Library Karshi EEI, 1(01).
27. Ergashev, Nuriddin. "RAQAMLI TEXNOLOGIYALAR MUHITIDA TA'LIMNI RIVOJLANTIRISHNING YETAKCHI TENDENSIYALARI VA ISTIQBOLLARI." International Scientific and Practical Conference on Algorithms and Current Problems of Programming. 2023.
28. Gayratovich, Ergashev Nuriddin. "A MODEL OF THE STRUCTURAL STRUCTURE OF PEDAGOGICAL STRUCTURING OF EDUCATION IN THE CONTEXT OF DIGITAL TECHNOLOGIES." American Journal of Pedagogical and Educational Research 13 (2023): 64-69.