DATA PROTECTION METHODS IN CLOUD SYSTEMS FOR WORKING WITH ELECTRONIC DOCUMENTS

Kamoliddinova Feruza Kamoliddin qizi
Muhammad al Xorazmiy nomidagi Axborot texnologiyalari universiteti
Email: feruza.kamoliddinova@mail.ru

Akbarov Navro‘z Jahongir o‘g‘li
Muhammad al Xorazmiy nomidagi Axborot texnologiyalari universiteti

Abstract: Cloud computing security refers to the broad set of policies, technologies, applications, and controls used to secure virtualized IP, databases, applications, services, and cloud computing infrastructure. Protecting cloud systems is part of computer security, network security, and, more broadly, information security. Data protection is one of the most important aspects in the problem of the security of cloud systems for working with documents. To increase the security of cloud environments, enterprises need to use modern technologies and best practices to protect their data.

Key words: Cloud security, ERMS, cyber attacks, DBMS, SQL, database, Secure Sockets Layer, VPN, password.

Cloud security is only effective when the right methods of protection are in place. The architecture of a cloud-based ERMS must recognize the challenges that arise in managing security. Security management solves these problems with controls security. These controls are in place to protect any weaknesses in the system and reduce the effect of cyber attacks.

Cloud services are highly secure when properly secured, but if neglected, the effect can be completely opposite. The solution is the compliance of the cloud with the requirements of regulatory documents and standards in the field of information security.

Russian legislation does not yet have standards that describe the principle of building information security in cloud technologies. As a result, cloud service providers are forced to choose how to protect information from a huge number of ready-made solutions on the market. But all protections must take into account the peculiarities of cloud technology1.

Let's consider the main types of information threats in cloud systems for working with documents.

In his scientific article identifies five main types of threats to cloud services:

1. Traditional attacks on software. Associated with the vulnerability of the applied network protocols, operating systems, modular components, etc.

To protect against such attacks, anti-virus programs, a firewall (firewall), an intrusion prevention system (Intrusion Prevention System), etc. are used.

2. Functional attack on cloud elements. Such attacks are associated with the layering of the cloud. The main means of defense against such cyberattacks is the protection of the weakest point of the system.

To protect against functional attacks for each layer of the cloud, you need

use special protection tools for each of them: for a proxy - protection against DDoS attacks, for a web server - page integrity control, for an application server - an application-level screen, for a DBMS layer - protection against SQL injection, for a storage system - backup copying and access control1.

3. Attacks on the client. This type of attack is very common in the web space. Such attacks are also typical for cloud systems, since users usually access the cloud through a web browser. These types of attacks include cross-site scripting, password theft, web session hijacking, man-in-the-middle attacks, etc.

As a protection, user authentication is traditionally used here, including effective two-factor authentication, an encrypted connection with mutual authentication2.

4. Attacks on virtualization tools. These include attacks on the hypervisor, on virtual machines when interacting between cloud nodes, as well as attacks on cloud management systems.

Such threats are currently extremely rare, and there are no reports of such real attacks. However, they are worth keeping in mind, as they may appear in the future due to the popularity of cloud virtualization3.

5. Complex threats of cloud services. The reasons for such a threat are improper control of the infrastructure. There are no guarantees that all cloud resources have been calculated and there are no uncontrolled virtual machines in it, no unnecessary business processes have been launched, and the mutual configuration of layers and elements of the cloud has not been violated. This type of threat is associated with the manageability of the cloud as a single information system and the search for abuse or other disruptions to the cloud that can lead to unnecessary costs for maintaining the health of the information system. This type of threat is more complex and it cannot be called a universal method of protection - security methods in this case are developed individually for each cloud.

So, after analyzing various sources on data security in cloud technologies for working with electronic documents, we can distinguish the following effective methods for protecting data in cloud technologies for working with electronic documents:

1.Data encryption. Encryption is one of the most effective methods of protecting information. The provider must encrypt user data from the server side, which is located in the data center. There are several methods for encrypting data when using cloud storage. Server-side encryption - encryption that occurs after the system receives as data, but before the data is written to disk and stored, as well as client-side encryption - encryption that occurs before data is sent to the cloud storage. Such data enters the cloud storage already encrypted, but is also encrypted on the server side.

The question of encryption keys remains important. It is not reasonable to store them on the cloud server, because anyone with access to that server could have access to the key, and thus to the encrypted information. The physical entry of the key is replaced by a request that the cloud server sends to an external source - the key management server

An important component for the implementation of such protection is the separate operation of the cloud server and the key management server: if both are hosted by the same cloud service provider, then all information is again collected in one place. A good alternative is to install a key management server in a local data center or as an outsourced service from another service provider1.

2.Data protection during transmission. Encrypted transmission is a prerequisite for secure data processing. In order to protect data in the public cloud, a virtual private network tunnel is used that connects the client and the server to receive public cloud services. A virtual private network tunnel facilitates secure connections and allows you to use a single name and password to access different cloud resources. As a means of transferring data in public clouds, a VPN connection uses public resources such as the Internet. The process is based on access modes with encryption using two keys based on the Secure Sockets Layer (SSL) protocol2

3.Authentication. Authentication is password protection. For example, they use tokens. A token is an electronic key used to provide information security, as well as to identify a user. The authentication system also uses the concept of one-time passwords. Such passwords may be used for only one authentication session, may be limited to a certain period of time.

After reviewing various literature, we can develop recommendations for users of cloud services to ensure the security and safety of their data:

1.Conduct an analysis of the cloud market. It is important to understand what cloud storage systems exist in enterprises, who uses them, and how. You can trust your data only to reliable and trusted companies that have proven themselves in the market. In order not to make a mistake in choosing, you need to take into account such important factors as the reputation of the cloud service, its duration, customer reviews, as well as its popularity.

2.Determine how the cloud storage provider addresses privacy and security issues. The terms of service agreements are a good starting point for determining the general protections offered by a cloud provider. But this is not enough to ensure the safe storage of files. Cloud service providers frequently update their terms of service and user agreements. Because of this, it is easy to miss minor changes that can have a significant impact on privacy and security.

Most agreements do not cover the details of how the cloud storage provider implements security, what specific protection methods it uses, and what happens in the event of a breakdown or breach. As a result, it is important to clearly define policies and procedures, which will facilitate further negotiations with the provider.

2. Know what means of protection should be applied. Encryption in the cloud is a fundamental requirement. It is important to know how the cloud storage provider uses encryption, including when transferring data between data centers, servers, and storage devices, and who controls the encryption keys, how they are applied to a particular set of data.

An organization using a cloud provider needs to know who has there is access to systems, what other means of protection exist - from DDoS attacks to system errors in applications.

3. Use multi-factor authentication on all devices and systems. The widespread use of multi-factor authentication greatly reduces the risk of gaining access to a system or application to release malware or steal valuable information. Multi-factor authentication can help protect sensitive data from hackers, disgruntled employees, and other insiders who may intentionally or unintentionally put data at risk.

4.Conduct audits and penetration testing of threats. Whether a company is partnering with a third-party security firm or relying on internal staff within its organization, experts believe that threat penetration testing is essential to determine if a system's cloud security measures are in place.

The organization should regularly audit the cloud security capabilities of the system. The audit should include an analysis of the capabilities of suppliers, protection methods should comply with security conditions.

Also, for security reasons, you should review your access logs to ensure that only authorized employees have access to sensitive data and applications in the cloud.

5. Ensure the physical protection of your data. Physical data protection involves minimizing the risks associated with the penetration of unauthorized persons to the computers of the organization. In addition to controlling incoming and outgoing visitors, it is also worth locking the office with a key and be sure to block the computer before leaving.

This, we examined the main methods of data protection in a cloud-based system for working with electronic documents, and also developed recommendations for security measures for users of such systems.

In most cases, security issues should not interfere organizations to use cloud services. By following cloud security best practices, they can further reduce the risk of these threats while enjoying the full benefits of cloud computing.

Organizations large and small spend significant resources developing and improving the security systems for their cloud products. When choosing a cloud service, you need to carefully study all its characteristics, especially when it comes to the issue of reliability.

Currently, methods of protecting information in cloud services need a new approach. Protection should include a whole range of measures implemented through the coordinated work of the provider and user of the services.

To implement the project, even at the stage of its development, it is necessary to involve professional security specialists, with the help of which to develop and provide appropriate software and hardware protection tools, including strong encryption, restricting access to server equipment, reliable logging of work, regulated access based on group policies.

REFERENCES:

1. Aleksandrov K.S. Account for petabytes // Machines and mechanisms. 2013. No. 6. S. 20-27.

2. Murzin F.A., Batura T.V., Semich D.F. Cloud technologies: basic concepts, tasks and development trends // Software products, systems and algorithms. 2014. No. 1. S. 2-22.

3. Berholts K.A. The use of cloud technologies in the electronic document management of commercial organizations // Innovative development. - 2018. No. 10. P. 9-12.

4. Smooth M.V. Application security on cloud computing platforms // Proceedings of BSTU. 2015. No. 9. From 204-207.

5. Gorokhov S.N., Lobanov E.M. Modern technologies for storing electronic documents // Bulletin of the archivist. 2015. No. 1. S. 193-200.

6. Guseev A.V. Prospects for cloud computing and informatization of healthcare institutions // Medical Information Systems. 2011. No. 2. S. 6-16.

7. Denisov D.V. Prospects for the development of cloud computing // Applied Informatics. 2009. No. 5. S. 52-58.

8. Dovgal V.A. Cloud computing and analysis of information security issues in the cloud // Bulletin of the Adygei State University. 2015. No. 2. P. 160-166.

9. Dogwal. EAT. Methods for improving security in the field of "cloud" technologies // Bulletin of the ASU. 2014. No. 4. pp. 170-174.

10. Ivonin P.V. Cloud security in detail // Izvestiya SFedU. 2013. No. 2. S. 35-40.