DOI https://doi.org/10.30525/978-9934-26-459-7-21

# ANALYSIS OF DATA PROTECTION MECHANISMS IN CLOUD ENVIRONMENTS

**Olha Shevchuk[1], Maiia Liuta[2], Mariia Zakharova[2]**
*[1]ISMA University of Applied Science, Latvia*
*[2]Cherkasy State Business-College, Ukraine*
**Corresponding author's e-mail: jenkins00011@gmail.com, maiialiuta@gmail.com, zmaria17mz@gmail.com*

## Abstract

Improving the security of cloud technologies. Analysis of information protection mechanisms in cloud environments and pointing out of their peculiarities. Searching for the most effective mechanism for protecting information, which is stored in cloud environments. Improving the security of cloud technologies will allow more people and organizations, for whom security is very important, to use such technologies. Due to the increase in the number of companies and institutions using cloud environments for the storage and exchange of internal data, there is a need for improved levels of security of this system.

***Key words:*** *cloud technology, information protection, security, mechanism, protocol.*

## Introduction

Cloud computing has become an increasingly popular technology for storing and processing data. However, with the growth of cloud computing, concerns about the security and privacy of data stored in the cloud have also increased. In this context, it is important to analyse the mechanisms for protecting data in cloud environments.

One of the main mechanisms for protecting data in cloud environments is encryption. Encryption is the process of converting plain text into cipher text using an algorithm and a key. Encryption can be used to protect data at rest, as well as data in transit. There are different types of encryption, such as symmetric encryption and asymmetric encryption, and different encryption algorithms, such as AES and RSA.

Another mechanism for protecting data in cloud environments is access control. Access control is the process of granting or denying access to resources based on user identity and permissions. Access control can be implemented using various methods, such as role-based access control (RBAC), attribute-based access control (ABAC), and mandatory access control (MAC).

A third mechanism for protecting data in cloud environments is data backup and recovery. Data backup is the process of creating copies of data to protect against data loss or corruption. Data recovery is the process of restoring data from backups. Data backup and recovery can be implemented using various methods, such as full backup, incremental backup, and differential backup.

It is also important to consider the legal and regulatory aspects of data protection in cloud environments. Different countries and regions have different laws and regulations regarding data protection, and it is important for organizations to comply with these laws and regulations when storing and processing data in the cloud.

Here are some additional points that could be included in the analysis of data protection mechanisms in cloud environments:

− Multi-factor authentication: Multi-factor authentication is a method of authentication that requires users to provide two or more verification factors to gain access to a resource. This can include something the user knows (such as a password), something the user has (such as a smart card), and something the user is (such as a fingerprint). Multi-factor authentication can help to prevent unauthorized access to data in cloud environments

− Data loss prevention (DLP): DLP is a set of technologies and processes used to prevent the unauthorized disclosure or loss of sensitive data. DLP can be used to monitor and control the movement of data within and outside of cloud environments, and to prevent data leakage through various channels, such as email, instant messaging, and file sharing.

− Intrusion detection and prevention systems (IDPS): IDPS are security systems that monitor network traffic for signs of malicious activity, and take action to prevent or mitigate attacks. IDPS can be used to protect data in cloud environments by detecting and preventing unauthorized access, as well as identifying and responding to security threats.

− Security information and event management (SIEM): SIEM is a security management approach that combines security information management (SIM) and security event management (SEM) functions into a single system. SIEM can be used to monitor and analyze security-related data from various sources, such as network devices, servers, and applications, and to provide real-time visibility into security events and incidents.

− Disaster recovery and business continuity planning: Disaster recovery and business continuity planning are processes that organizations use to prepare for and recover from disruptive events, such as natural disasters, cyber attacks, and hardware failures. These processes can help to ensure the availability and integrity of data in cloud environments, and to minimize the impact of disruptive events on business operations.

These data protection mechanisms are detrimental to the security and privacy of data in cloud environments. However, it is important to note that they cannot provide absolute data protection and require a comprehensive approach to data protection that includes various protection mechanisms and security measures.

1. Cloud environments are increasingly being used for data storage and processing, making data protection in the cloud extremely important.

2. There are several data protection mechanisms that can be used to ensure the security and confidentiality of data in cloud environments, including data encryption, access control, data loss prevention, intrusion detection and prevention, and disaster recovery and business continuity planning.

3. Data encryption is one of the primary data protection mechanisms in cloud environments, which can be used to protect data stored in the cloud as well as data transmitted between the user and the cloud environment.

4. Access control is an important data protection mechanism that helps prevent unauthorized access to data and resources in the cloud.

5. Data loss prevention (DLP) is a data protection mechanism that helps prevent the leakage of confidential data from the cloud environment.

6. Intrusion detection and prevention (IDS/IPS) is a data protection mechanism that helps detect and prevent unauthorized access to the cloud environment.

7. Disaster recovery and business continuity planning (DR/BC) is a data protection mechanism that helps ensure that the cloud environment can quickly recover from a disaster or other unexpected event.

8. It is important to use a comprehensive approach to data protection in cloud environments, which includes various data protection mechanisms and security measures, and to regularly update these mechanisms and measures to ensure the maximum level of data protection.

## Conclusions

The analysis of data protection mechanisms in cloud environments is an important task for ensuring the security and privacy of data stored in the cloud. Encryption, access control, data backup and recovery, and compliance with legal and regulatory requirements are some of the key mechanisms for protecting data in cloud environments

## References

1. Bilova T. G. Methods for improving the security of data processing in cloud computing / T. G. Bilova V. O. Yaruta. *Collection of scientific works of Kharkiv National University of Air Forces*. 2015. № 4(45). P. 71–73.

2. Ilkevich N. S. Cloud technologies in education. Educational and methodological manual for students of the Faculty of Physics and Mathematics. Zhytomyr : ZhDU publishing house, 2021. 88 c.

3. Kotyashichev I.A., Birilova E.A. Protection of information in "Cloud technologies" as a subject of national security. *Molodiy scientist.* 2015. No. 6.4. P. 30–34.

4. Fundamentals of cyber security and cyber defense: a textbook / Yu. G. Danyk, P. P. Vorobienko, V. M. Chernega [Second edition, revision. and additional]. Odesa : ONAZ named after O.S. Popova, 2019. 320 p.