UDC 004.056.53

DEVELOPMENT OF DATA PROTECTION METHODS FOR DISTRIBUTED CLOUD SYSTEMS

Ryabova N.
bachelor's degree, Gubkin Russian State University of Oil and Gas (Moscow, Russia)

РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ ДАННЫХ ДЛЯ ДИСТРИБУТИВНЫХ ОБЛАЧНЫХ СИСТЕМ

Рябова Н.М.
бакалавр, Российский государственный университет нефти и газа имени И.М. Губкина (Москва, Россия)

Abstract

This article discusses data protection methods for distributed cloud systems (DCS), including symmetric, asymmetric, and hybrid encryption, multi-factor authentication, and distributed access control systems. Key characteristics of encryption methods are presented, along with an analysis of their advantages and limitations. Notable data breaches in major companies such as Capital One, Facebook, and Uber are described, emphasizing the importance of robust security measures and regular audits. Modern data protection technologies and their applications in the context of increasing cybersecurity threats are explored. The article highlights the importance of a comprehensive approach and the integration of new methods to enhance the reliability of cloud systems.

Keywords: data protection, distributed cloud systems, encryption, multi-factor authentication, access management.

Аннотация

В данной статье рассматриваются методы защиты данных для дистрибутивных облачных систем (ДОС), включая симметричное, асимметричное и гибридное шифрование, многофакторную аутентификацию и распределенные системы управления доступом. Приведены ключевые характеристики методов шифрования и анализ их преимуществ и ограничений. Описаны случаи утечек данных в крупных компаниях, таких как Capital One, Facebook и Uber, что демонстрирует важность надежных мер безопасности и регулярного аудита. Обсуждаются современные технологии защиты данных и их применение в условиях растущих угроз кибербезопасности. Статья подчеркивает значимость комплексного подхода и интеграции новых методов для повышения надежности облачных систем.

Ключевые слова: защита данных, дистрибутивные облачные системы, шифрование, многофакторная аутентификация, управление доступом.

Introduction

With the development of cloud technologies and distributed computing systems, data protection has become increasingly relevant. Modern distributed cloud systems (DCS) provide users with the ability to process and store data on remote servers, enhancing application flexibility and performance. However, these benefits come with new security challenges. Given the high degree of distribution of such systems, ensuring the confidentiality, integrity, and availability of data is a complex task. The goal of this article is to explore modern approaches to developing data protection methods in DCS and to analyze their effectiveness and applicability in various usage scenarios.

The main security threats in distributed cloud systems include unauthorized access, data leakage, and data integrity violations. Various methods are used to prevent these, including cryptographic algorithms, authentication and authorization mechanisms, as well as segmentation and access control strategies. One of the key aspects of data protection is the use of encryption during both data transmission and storage. It is also essential to consider challenges related to encryption key management and security in multi-tenant environments, where the same resources may be used by different users.

The article reviews the main data protection methods in DCS, including symmetric and asymmetric encryption, multi-factor authentication (MFA) mechanisms, and distributed access management systems. The advantages and limitations of these methods are analyzed considering current performance and security requirements.

Main part

Data encryption methods play a crucial role in protecting information transmitted and stored in distributed cloud systems [1]. Various encryption approaches offer different levels of security and performance, allowing the selection of the most suitable method depending on system requirements. Table 1 below presents the characteristics of the main encryption methods.

Table 1

Characteristics of data encryption methods

Encryption Method	Main Algorithms	Advantages	Disadvantages
Symmetric encryption	AES, DES, 3DES	High speed, efficiency with large data volumes	Issues with secure key management
Asymmetric encryption	RSA, ECC	High security level, convenient key transmission	High computational load
Hybrid encryption	SSL/TLS	Combines advantages of symmetric and asymmetric encryption	Complex implementation, infrastructure needs

The table outlines the main data encryption methods, their advantages, and disadvantages. Symmetric encryption is characterized by high speed, making it suitable for handling large volumes of data, but it requires reliable key management methods. Asymmetric encryption provides a high level of security but imposes significant computational loads. Hybrid encryption, represented by algorithms such as SSL/TLS, combines the advantages of both methods, although its implementation can be complex and require developed infrastructure [2].

In modern DCS, data encryption remains the primary method for ensuring confidentiality. Symmetric encryption, using a single key for encryption and decryption, demonstrates high performance and is often applied to secure data during storage [3]. For example, the AES (Advanced Encryption Standard) algorithm is widely used due to its reliability and speed. However, the main issue remains secure key management, especially in distributed systems where keys may be vulnerable to leaks and compromise. To address these issues, distributed key management methods and secure key exchange protocols are implemented.

Asymmetric encryption, which uses a pair of keys (public and private), ensures a higher level of security during data transmission between different network nodes. Algorithms such as RSA and ECC (elliptic curve cryptography) enable encryption with fewer risks associated with key exchange. However, this type of protection requires significant computational resources, which can slow down data processing in real-time and increase latency in system component interaction [4]. As a result, asymmetric encryption is often used to secure communication channels, after which data transmission continues using symmetric encryption.

Hybrid encryption combines the advantages of symmetric and asymmetric methods. This allows asymmetric encryption to be used for key exchange and symmetric encryption for data encryption. The most well-known example of this approach is the use of SSL/TLS protocols, which ensure data protection during transmission over the network. SSL/TLS is applied everywhere, from websites to corporate systems, to protect data from interception and tampering.

Besides encryption, an essential element of data protection in DCS is multi-factor authentication (MFA). MFA includes additional verification layers, significantly reducing the risk of unauthorized access. The combination of a password and biometric data or one-time codes provides more reliable user authentication, especially in distributed systems.

Access management systems also play a crucial role in data protection. Modern methods include using roles and access policies that define which users or nodes can access certain data. The role of access management can be enhanced by using distributed access control systems based on blockchain technology, where information about access rights is recorded in a distributed ledger, preventing unauthorized changes [5, 6].

An important addition to data protection strategies is the use of encryption protocols during data transmission. Protocols such as IPSec and VPN provide secure tunnels for data transfer between nodes, eliminating the possibility of interception and packet analysis. These technologies are particularly relevant for the transmission of confidential data between different regions where communications pass through public networks.

Real cases of data breaches and their consequences

Real cases of data breaches in distributed cloud systems demonstrate the importance of reliable information protection. One well-known example is the 2019 data breach at **Capital One**. An attacker gained access to information of more than 100 million customers due to a vulnerability in the Amazon Web Services (AWS) cloud infrastructure settings. The main cause of the breach was improper access management and firewall configuration, allowing the attacker to exploit vulnerabilities to gain access and extract data [7].

Another notable case was the data breach at **Facebook**. In 2019, it was discovered that the data of millions of users was publicly available on cloud servers managed by third parties. The cause of the breach was insufficient access management and the lack of strict control measures when working with partners, leading to inadequate protection of user data [8].

A significant incident also occurred with **Uber** in 2016, when attackers gained access to the data of 57 million users and drivers. The main reason was the use of vulnerable access tokens and weak account protection in the cloud infrastructure. Uber paid substantial fines and committed to strengthening data protection measures, including the implementation of stricter access management mechanisms and audits [9].

These cases show that even leading companies can fall victim to data breaches due to insufficient protection of their distributed cloud systems. The main lessons that can be learned from such incidents include the need for proper security configuration, regular audits, the use of encryption, and access control at all levels of cloud infrastructure [10].

Conclusion

Data protection in distributed cloud systems requires a comprehensive approach that considers a variety of threats and the specifics of distributed architecture. The reviewed methods, including symmetric, asymmetric, and hybrid encryption, as well as multi-factor authentication mechanisms and distributed access management systems, confirm their effectiveness in various application scenarios. These methods help not only protect data during transmission and storage but also minimize the risks of unauthorized access.

Practical examples of data breaches in major companies such as Capital One, Facebook, and Uber emphasize the importance of proper security configuration, regular audits, and effective access management strategies. These incidents serve as a reminder that even industry leaders can face breaches if their infrastructure is insufficiently protected. The lessons learned from these cases contribute to increased awareness of the need for enhanced security measures.

Future developments in data protection methods should focus on the integration of new technologies such as blockchain and artificial intelligence to automate monitoring and threat prevention. These approaches will help create more secure and attack-resistant distributed cloud systems.

References

1. Poludenny N.I., Chernysheva A.V. Analysis of existing methods of software copyright protection using steganography // Software Engineering: Methods and Technologies for Developing Information and Computing Systems (PIIVS-2020). 2020. P. 91-96.

2. Khramtsovskaya N.A. The InterPares Trust international project // Record Management. 2014. No.2. P. 85.

3. Poltavtseva M.A., Kalinin M.O. Analysis of access control systems in heterogeneous big data systems // Proceedings of the Institute for System Programming of the RAS. 2024. Vol. 35. No.4. P. 93-108.

4. Gavrilenko I.R., Slivinsky D.V. New NDC distribution opportunities and IoT as tools for the development of global GDS distribution systems // Economics and Business: Theory and Practice. 2024. No.1-1(107). P. 44-49.

5. Cherepenin V.A., Smik N.O., Vorobyov S.P. Integration of cloud, fog, and edge technologies for the optimization of high-load systems // Software Systems and Computational Methods. 2024. No.1. P. 1-9.

6. Rafique A., Van Landuyt D., Beni E.H., Lagaisse B., Joosen W. CryptDICE: Distributed data protection system for secure cloud data storage and computation // Information Systems. 2021. Vol. 96. P. 101671.

7. Xiaoyu W., Zhengming G. Research and development of data security multidimensional protection system in cloud computing environment // 2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI). IEEE. 2020. P. 67-70.

8. Gupta I., Singh A.K., Lee C.N., Buyya R. Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions // IEEE Access. 2022. Vol. 10. P. 71247-71277.

9. Sun P.J. Privacy protection and data security in cloud computing: a survey, challenges, and solutions // IEEE Access. 2019. Vol. 7. P. 147420-147452.

10. Sun Y., Zhang J., Xiong Y., Zhu G. Data security and privacy in cloud computing // International Journal of Distributed Sensor Networks. 2014. Vol. 10. No.7. P. 190903.