CYBERSECURITY CHALLENGES IN THE ERA OF CLOUD COMPUTING

Anarbayev Sardorbek Odil o'g'li
Eshonqulov Oybek Shuhrat o‘g‘li
Bahronov Shahzodjon Vahobjon o‘g‘li

Abstract: Cloud computing technology is one of the modern solutions that brought about revolutionary changes in the field of Information Technology. With this technology, users and organizations will be able to store, process and manage their data on remote servers. One of the main advantages of cloud computing is the efficient allocation of resources, reducing costs and providing free access to data at any time, from anywhere. At the same time, with the development of cloud computing technology, new problems and threats are emerging in the field of cyber security. This article will analyze in detail the problems of cyber security that occur during the cloud computing period.

Keywords: Cloud Computing, Information Technology, Data, Problems, Solution, computing, cybersecurity.

Cloud computing systems are used simultaneously by a large number of users and organizations. This makes systems more sensitive to attacks. Cybercriminals use a cloud environment to attempt malicious activities such as data theft, hacking, or system shutdown. In a cloud computing environment, the centralization of data poses a major threat to cybersecurity, as access to the entire system via a single weak point arises. One of the most basic data protection problems in cloud computing is ensuring the confidentiality and integrity of the data. Data is often stored on third-party servers, which increases their risk of falling into the wrong hands. Therefore, the need arises to strengthen data encryption, access control and authentication systems. However, encryption technologies also have their own complexities and limitations, requiring large computational resources to apply them effectively. Another problem that arises in cloud computing is the permanence and reliability of services. Cyberattacks, in particular denial-of-service (DDoS) attacks, can interrupt the performance of cloud services. This causes users to lose access to information and services. For this reason, cloud service providers must constantly strengthen security measures and create quick response systems to attacks.[1]

User identification and authentication are important in cloud computing. In many cases, weak authentication systems allow cybercriminals to illegally access the system. Therefore, it is necessary to introduce modern methods such as two-stage authentication, the use of biometric data. In addition, the fact that users and organizations regularly update their passwords also serves to increase security. Data management and backup systems are also of great importance in cloud computing. The presence of backups in cases of data loss or corruption contributes to the rapid recovery of the system. At the same time, the security of backups should also be ensured, since they can also be a target for cyberattacks. Clear and effective collaboration between organizations and users is necessary to ensure cybersecurity in a cloud computing environment. Cloud service providers must make their security policies accessible and understandable, and users must take the necessary measures to protect their data. At the same time, in the field of cyber security, it is important to constantly educate employees, inform them about new threats and technologies.[2]

Another problem that arises in cloud computing is legal and ethical issues. The storage of data on third-party servers may clash with the legislation of some states. Therefore, it is necessary to determine the location of data storage, as well as comply with the laws governing the rights to access data. This can to some extent hinder the development of cloud computing services globally. New technologies and approaches are being developed to reduce cybersecurity problems in cloud computing. For example, with the help of artificial intelligence and machine learning technologies, the chances of detecting threats in advance and eliminating them are increasing. It is also possible to ensure the integrity and transparency of information using blockchain technology. These technologies serve to further strengthen security in the cloud computing environment. The problems of cloud computing in the field of cyber security and the ways to solve them are constantly changing and developing. Therefore, it is important for organizations and users to be aware of the innovations in this area, constantly updating security policies and effectively using modern technologies. Ensuring cybersecurity requires an integrated approach, taking into account not only technological measures, but also the human factor.[3]

Cloud computing technology is currently one of the most important and widely used approaches in the field of Information Technology. It allows users to remotely manage, store and use their data and applications over the internet. At the same time, the issue of data protection is of paramount importance in cloud computing, since data is often stored on third-party servers and transmitted over the internet. Measures related to data protection are aimed at ensuring not only the confidentiality of information, but also their integrity and availability. One of the basic principles of data protection in cloud computing is data encryption. Using encryption, the data is protected from being read or changed. Data encryption takes place in two main steps: when data is transmitted from the user to the cloud, and when data is stored on cloud servers. At the time of transmission, data is encrypted using secure protocols such as TLS or SSL, which protect them from third-party reading as the data is transmitted over the network. During storage, however, the data is stored encrypted on a disk or in a database. Managing encryption keys requires special attention, as mismanagement of keys can threaten the security of the data. Strong authentication and access control also play an important role in data protection. Users ' access to the system should only be carried out by trusted and approved individuals. For this purpose, two-stage authentication, biometric data or strong passwords are used. Access rights, on the other hand, must be granted in accordance with the principle of minimum necessity, that is, the user is given the rights necessary only for the tasks that he must perform. Regular implementation of control and audit of access rights helps to increase the security of the system. To reduce the risk of data loss or corruption, it is necessary to make backups and store them in a safe place. Backups ensure data recovery and prevent data loss that can result from unexpected technical failures, hacking attacks, or other emergencies. Even when creating backups, it is important to encrypt them and control access to them.[4]

It is also important to regularly update cloud computing systems and close security holes. Software vulnerabilities open the entrance door for cybercriminals, so cloud service providers and users need to constantly update systems and install security patches and updates. These processes can be carried out using automated methods, which reduces errors caused by the human factor. Regular cybersecurity training and awareness of users and employees is also important. Many cyber attacks are carried out through social engineering methods, for example, using phishing or fake emails. Therefore, it is necessary to inform users about such attacks, ensure their compliance with safety rules, identify suspicious behavior and teach them to react. Constant monitoring of all inputs and activities occurring in the system is also an important tool in ensuring security. With Monitoring, suspicious activities, attempts at unknown access or unusual actions in the system are detected. This makes it possible to quickly respond to and prevent security incidents. Monitoring systems can automatically issue alerts and analyze security incidents. When protecting data in cloud computing, it is also necessary to take into account legal and regulatory requirements. Different countries have specific laws and standards for data storage and processing. Cloud service providers and users must meet these requirements, as well as comply with international standards that ensure data privacy. This not only ensures legal compliance, but also increases the trust of customers and users. In addition to applying modern technologies and methods to protect data in cloud computing, it is important to clearly define security policies and procedures and constantly update them. Each organization needs to develop appropriate security measures, taking into account its specific security needs and threats. At the same time, it is recommended to conclude security agreements with cloud service providers and regularly check the level of security of their services. Data protection in cloud computing requires a versatile and integrated approach. In this process, many factors work together, such as data encryption, strong authentication, access control, backups, system upgrades, user training, monitoring, and enforcement of legal requirements. Effective implementation of these measures will help ensure the confidentiality, integrity and availability of information, as well as strengthen protection against cybersecurity threats. To take full advantage of the benefits of cloud computing, it should be remembered that data protection is a process that requires constant and serious attention.[5]

Conclusion: In summary, cloud computing technologies play an important role in efficient resource management and cost reduction, providing great opportunities in the information technology sector. However, along with these technologies, new problems are emerging in the field of cyber security. Data confidentiality, integrity, service permanence, user authentication, data backup, and legal issues are the main issues that arise in cloud computing. To solve these problems, modern technologies, effective security policies and user-to-service cooperation are necessary. Thus, in order to ensure cybersecurity in the cloud computing environment, it is necessary to constantly monitor the news and improve security measures. This is important not only in technological development, but also in ensuring information security.

References:

1. Rakhmatullayev Sh. Problems of cloud computing and cyber security. T.:” University " Press, 2023. – 198 b.
2. Karimov O. Security and cloud computing in Information Systems. T.: Publishing House "Science", 2022. – 210 b.
3. Abdullayev M., Tursunov S. Cybersecurity threats in cloud computing systems. T.: Publishing House” Science and technology", 2023. – 175 b.
4. Rustamova N. Cybersecurity and cloud technologies. T.: Publishing house "Information Security", 2021. – 185 b.
5. Islamov D. Digital security and cloud computing. T.: Publishing house "innovation", 2024. – 200 b.
6. Yusupova L. Data protection problems in cloud computing. T.:” University " Press, 2023. – 190 b.
7. Toraev S. Modern problems of cybersecurity. T.: Publishing House "Science", 2022. – 205 b.
8. Mamatqulov A. Security strategies in cloud computing technologies. T.: Publishing House” Science and technology", 2024. – 220 b.