Challenges and Solutions in Cloud System Security Latest Overview

ABSTRACT

This paper highlights the key security challenges in cloud computing and provides practical solutions to overcome them. We discuss risks such as unauthorized access, data loss, cyberattacks, and regulatory compliance, as well as solutions such as data encryption, access management, and security monitoring. The goal is to help organizations adopt and keep cloud systems secure amid evolving security threats.

LITERATURE REVIEW

Data security in cloud computing is a key focus as it is vulnerable to attacks such as DDoS and hacking, which can lead to data leakage. To combat this, strict security policies and the use of two-factor authentication are required. Proactive monitoring and employee training are also important. Choosing a trusted cloud provider is also crucial. With these measures, the risk of attacks and data leakage can be minimized.

RESEARCH METHODOLOGY

This research involves analyzing literature and secondary data sources related to data security in cloud computing. Theoretical analysis was conducted with the implementation of cloud computing to overcome security challenges. Descriptive analysis method was used to explain and analyze the challenges and solutions in cloud system security. The analysis process is done by linking and comparing data to deeply understand the challenges and solutions in cloud system security. This method helps in identifying alternative challenges and solutions of cloud computing implementation to help organizations in facing security challenges.

ENCRYPTION TECHNIQUES FOR DATA PROTECTION

PRIVACY-PRESERVING MECHANISMS AND REGULATIONS

SECURE DATA LIFECYCLE MECHANISM

AUDIT AND MONITORING

DISCUSSION RESULT

Cloud computing, as a major trend in modern technology, has changed the way IT services are delivered, providing advantages such as flexibility, scalability, and cost efficiency. However, data security in the use of cloud systems is a major concern, with many organizations worried about the potential for unauthorized access and data leakage. Some institutions have adopted blockchain technology and cryptography to enhance the security of their data within the cloud. However, while these technologies can provide an additional layer of security, there are still possible security flaws in the cloud infrastructure itself. Therefore, further research is needed to understand and address the security challenges associated with the use of cloud computing services.

CONCLUSION

Security challenges in cloud computing require effective solutions such as the implementation of strict security policies, the use of strong authentication mechanisms, and cooperation with trusted cloud service providers. Technical solutions such as data encryption, proactive security monitoring, and security training for employees are also important. By identifying these challenges and solutions, this research aims to help organizations adopt cloud computing that is secure and responsive to security threats.

TEKNIK KOMPUTER / FAKULTAS ILMU KOMPUTER / UNIVERSITAS SRIWIJAYA