

Name/ID : ABDELKAREEM YOUSEF MAMDOH SOUBAR/19110022

Subject :IT Seminar

Assignment Title:cloud computing security challenges

Submission Date :26/4/2023

cloud computing, its benefits, and the different deployment models. They then discuss the various security challenges and issues that are associated with cloud computing, such as data breaches, insider attacks, and third-party risks.

the security threats that arise due to the shared infrastructure, multi-tenancy, and lack of control over data and applications. Additionally, the authors examine the security measures that can be implemented to address these challenges and issues, such as access control, encryption, and authentication. They also discuss the need for cloud service providers to comply with various regulatory and compliance requirements.

# Cloud computing security challenges:

1. Data breaches: Data breaches can occur when sensitive information is accessed by unauthorized individuals. In a cloud environment, data breaches can occur due to vulnerabilities in the cloud infrastructure, inadequate access controls, or phishing attacks.
2. Inadequate access controls: In a cloud environment, access to data and applications can be challenging to manage due to the number of users and accounts involved. If access controls are not implemented properly, unauthorized individuals may be able to access sensitive data.
3. Insider threats: Insider threats refer to the risk of malicious or unintentional actions by employees, contractors, or other insiders who have access to data and applications in a cloud environment. Insider threats can include data theft, unauthorized data access, or data destruction.
4. Compliance issues: Compliance issues can arise in a cloud environment when organizations fail to comply with regulations and laws related to data security and privacy. Organizations need to ensure that their cloud providers are compliant with the relevant regulations and that they are following best practices for data security.
5. Data loss: Data loss can occur due to various reasons, including hardware failures, natural disasters, cyber attacks, and human errors. In a cloud environment, data loss can have severe consequences, as data may not be recoverable.

# Countermeasures to mitigate these risks:

1. Strong access controls: Strong access controls, such as multi-factor authentication and role-based access control, can help restrict access to data and applications in a cloud environment.
2. Data encryption: Data encryption can help protect data from unauthorized access by encrypting data both in transit and at rest.
3. Regular security audits: Regular security audits can help identify vulnerabilities in the cloud infrastructure and ensure that security controls are working effectively.
4. Employee training: Employee training can help reduce the risk of insider threats by raising awareness of security best practices and providing employees with the knowledge to identify potential security risks.
5. Disaster recovery and backup: Disaster recovery and backup strategies can help mitigate the risk of data loss by ensuring that data is backed up and can be restored in the event of a disaster.
6. By implementing these measures, organizations can help ensure that their data and applications are secure and available to authorized users in a cloud environment.

# From the paper we read

1. Overview of Cloud Computing: cloud computing and its characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.
2. Cloud Security Challenges: the security challenges faced in cloud computing, including data privacy and protection, lack of transparency, regulatory compliance, insider threats, and multi-tenancy.
3. Cloud Security Issues: the various security issues in cloud computing such as data breaches, data loss, account hijacking, and denial of service attacks.
4. Cloud Security Countermeasures: various countermeasures to address the security challenges and issues in cloud computing, including access control, data encryption, multi-factor authentication, intrusion detection and prevention, and disaster recovery.
5. Cloud Security Standards and Certifications: various cloud security standards and certifications such as ISO/IEC 27001, Cloud Security Alliance (CSA), and Payment Card Industry Data Security Standard (PCI DSS).