Project (Individual) - Fall 2021

CPCS-425 Information Security

Coordinator(s) Dr. Syed Hassan

9065

Razan Mohammed Aljuhani

obtained Marks _____ out of 10

SO	Max	Obtained Marks
2	8	

Printed by : Dr. Rania Molla Tuesday, November 30 2021

Cloud Computing Security

Abstract

Cloud computing has received a lot of attention lately due to its wonderful innovative features that have contributed to improving speed, reducing cost, and scalability. And because cloud computing aims to store and process data, the security of this data must be one of the most important priorities to be taken into consideration, and there is no doubt that any modern technology faces some threats and security challenges. Therefore, this exploratory article aims to discuss cloud computing in terms of security, as it presents how security works in the cloud, challenges, and threats to cloud security, as well as ways to protect against intrusion.

1. Introduction

Cloud computing is considered a new technology that takes advantage of the internet to store, save and manage data of organizations or individuals on servers, and the data can be accessed via the internet. The users of the cloud don't need any physical infrastructure, they rent the usage from a third-party provider. One well-known example is Google cloud which is a collection of public cloud services provided by Google company. The users of Cloud-based storage could save files to a remote database and retrieve them on demand. The Essential characteristics of cloud services used are simple, flexible, Suitable cost, and Dynamic scalability (Butt, 2020).

This technology can be categories into three main service models: SaaS, PaaS, IaaS. First, The Software as a Service (SaaS) is designed for end-users in which providers make applications available to them on the internet. Second, The Platform as a Service (PaaS) helps developers of applications. Third, The Infrastructure as a service (IaaS) serves network engineers who need resources for the development process (Alam, 2021).

Recently, most organizations are already using cloud computing in their business. Moreover, the customer of the cloud has concerns about flaws in cloud computing that stored their data. So, Cloud security is critical including preventing leaks and data theft that leads to trust a vendor that efforts to keep customer's data and make the transactions safe, each of the Cloud providers must increase confidence in their services by aware their customers of the level of security that will protect the user's data from any form of attack. Some methods increase cloud security such as firewalls, penetration testing, tokenization, and virtual private networks (VPN) (Carlin, 2013).

2. Cloud Computing deployment models

Cloud computing has four deployment models, which are private, public, community, and hybrid cloud. Each of them distingue by some characteristics (Butt, 2020).

- **Private Cloud:** It is known as an internal cloud and works by providing computing services via a private network in a place such as Microsoft.

- **Public Cloud:** It is owned by the third-party provider and shared across multiple organizations via the public network such as Gmail.
- **Community Cloud:** it enables a particular group of organizations to work on a single platform and allows systems and services to be accessible for them and share the data such as U.S IBM SoftLayer.
- **Hybrid cloud:** It is the combination of both private and public cloud services such as Amazon Web Services (AWS).

The below table illustrates a comparison between models depending on some security features.

	Scalability	**Reliability**	**Security**	**Privacy**
Public	High	Medium	less	less
Private	less	High	High	High
Community	Medium	Medium	Medium	Medium
Hybrid	High	Medium	High	less

Table 1. Cloud computing deployments

3. Threats and attacks of Cloud Computing

Although Cloud computing is a powerful model that has many advantages which make the Cloud rapidly growing and developing. It is almost daily face various security threats and protection challenges. The categorization is performed based on the CIA Triad threats on cloud components (Butt, 2020).

3.1 Threats

Generally, Cloud computing faced several security threats that violate the basic computer security objectives of confidentiality, integrity, and availability (Butt, 2020).

- **Confidentiality threats** involve made available or control of confidential data of Cloud clients by an unauthorized party, which leads to the external and internal risk of attack.
- **Integrity threats** involve the threats of information transformation, manipulation of data by an unauthorized party, that leads to risk to data quality.
- **Availability threats** include cloud provider non-accessibility, ineffectual, recovery techniques, and physical interruption of assets.

3.2 Challenges

The criminals use several techniques to stay on the victim organization's network as long as possible, for achieving their goals that to access and controls data illegally and use of data for any purpose depends on Hackers goals. Most of the security threats and challenges that are exposed to organizations through Cloud services are related to authentication and public APIs. Here are some challenges of Cloud computing security must be considered (Alam, 2021):

1. Data privacy.
2. Configuration.

3. well-planned cloud security strategy

4. sufficient credential for User Authentication.

5. Access Management for Cloud Security.

6. complete visibility of Cloud Services

7. Secure interfaces and APIs.

8. Experienced workforce.

9. Control over Cloud Infrastructure Security

3.3 Attacks

Attacks on Cloud can be classified into network-based, VM-based, storage-based, and application-based (Butt, 2020).

1. Network-based attacks: are attempts to gain unauthorized access to an organization's network that aims to malicious activity on the data. including Denial-of-Service attack that causes of service or data unavailability.

2. VM-based attacks: The breaches in which an intruder can harm the hypervisor that creates the virtual environment within a virtual machine (VM) host by taking control over it. The cross-VM attacks primarily target the cache memory (Basu, 2018).

3. Storage-based attacks: In this type, the attackers aim to steal the sensitive data stored on storage devices, for example, ransomware malware.

4. Application-based attacks: The applications that use Cloud could face threats and attacks that decrease their performance, and cause data leakage for malicious purposes such as hijackings Service attack (Almorsy, 2016)

.

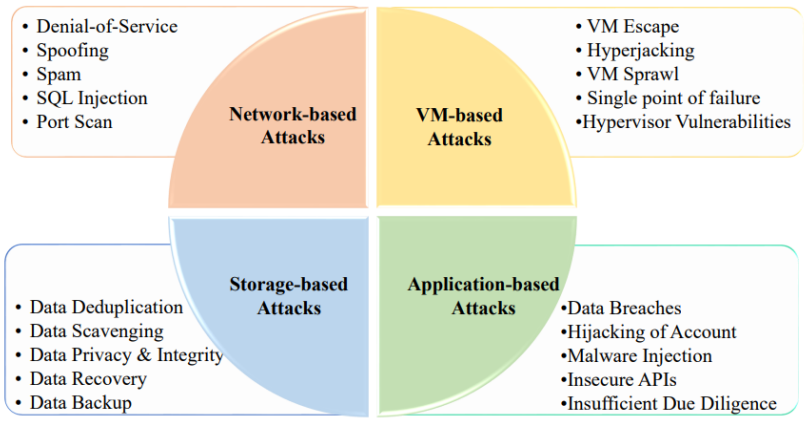

Figure 1. Attacks on cloud components.

Source: (Butt, 2020)

4. Cloud security controls

The Cloud security controls aim to protect data by mitigating or eliminating different types of attacks, they usually belong to four main categories. Frist, Deterrent Controls may act as a warning that an attack will be met with consequences. Second, Preventive Controls detect and handle vulnerabilities. Third, Detective Controls play an important role in monitoring the network to identify security threats. Lastly, Corrective Controls are designed to limit the damage caused by the incident or attack (Alsmadi, 2018).

4.1 Methods of cloud computing security

The risks could be mitigated by using a various method that increase the data security such as (Basu, 2018):

1. Protecting of data using reliable encryption techniques.
2. Deploying of Multi-Factor Authentication (MFA).
3. Establishing of professional data recovery plans.
4. Providing Anti-Phishing training for employees on a regular basis.
5. Monitoring end users' activities.
6. Setting of automated solutions to detect criminals.

4.2 Guidance to Cloud Security

The continued to evolve of cloud services increases the challenges and threats while using cloud services. All the cloud provider and consumer are responsible for data security and must be aware of the security feature updates that allows organizations to grow faster in a safe manner with lower cost. Protecting cloud data requires visibility and control (Basu, 2018).

So, the below points discuss some of the best practices that can leading handle cloud security issues.

- **Understanding cloud usage and risk** by focusing on understanding the current state of the Cloud and determining risks. It mainly goes through four steps. Firstly, the Identification of confidential data, because is the biggest risk is lack or theft of these data. Secondly, determining who can access and share sensitive data. Thirdly, Auditing configurations for identity and access management, network configuration, and encryption, where the IaaS environments consist of important settings can create exploitable vulnerabilities if misconfigured. Lastly, disclosing malicious user behavior by the user behavior analytics (UBA) can monitor for anomalies and mitigate both internal and external data leakage.

- **Protecting the cloud**, after understanding cloud security risks should apply protection techniques to the cloud services. There are several cloud security technologies including applying data protection policies, encrypting sensitive data with secret keys to fully control access, setting limitations of the data sharing by enforcing access control policies across services, and applying advanced Anti-malware technologies to the OS and virtual network to protect the infrastructure of the cloud.

- **Responding to cloud security issues** like any other IT environment, there would face incidents requiring an either automated or planned response.

To begin the cloud security incident response, require additional verification for high-risk access to sensitive date, automatically update web access policies as new services come up, delete malware from a cloud service, and scan files in a cloud storage with anti-malware to avoid ransomware or data theft attacks.

5. Conclusion

Cloud computing has great advantages for improving the performance of organizations. This explosivity essay focused on discussing the security of cloud computing mainly, as it mentioned some security threats and challenges for organizations that use the cloud, also presented the types of attacks that can be exposed, and then discussed some types of security control to ensure the integrity of the data in the cloud, and finally, some guidance was shown that increasing the ability to maintain the safe cloud environment.

References

1. Alam, T. (2021). Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *1*, 108-115.
2. Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), 1379.
3. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 347-356). IEEE.
4. Alsmadi, D., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior*, *85*, 218-226.
5. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.
6. Carlin, S., & Curran, K. (2013). Cloud computing security. In *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments* (pp. 12-17). IGI Global.