# cloud-computing-security-for-multi-cloud-service-providers-controls-and-techniques-in-our-modern-threat-landscape

Conference Paper · August 2022

DOI: 10.5281/zenodo.7084251

Sandesh Achar
Walmart Global Tech

# Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape

Sandesh Achar

Open Science Index, Computer and Systems Engineering Vol:16, No:9, 2022 publications.waset.org/10012673/pdf

***Abstract*****—**Cloud computing security is a broad term that covers a variety of security concerns for organizations that use cloud services. Multi-cloud service providers must consider several factors when addressing security for their customers, including identity and access management, data at rest and in transit, egress and ingress traffic control, vulnerability and threat management, and auditing. This paper explores each of these aspects of cloud security in detail and provides recommendations for best practices for multi-cloud service providers. It also discusses the challenges inherent in securing a multi-cloud environment and offers solutions for overcoming these challenges. By the end of this paper, readers should have a good understanding of the various security concerns associated with multi-cloud environments in the context of today's modern cyber threats and how to address them.

***Keywords*****—**Multi-cloud service, SOC, system organization control, data loss prevention, DLP, identity and access management, IAM.

## I. Introduction

CLOUD computing has become increasingly popular as it offers several advantages over traditional on-premises computing. However, as more organizations move to the cloud, the need for robust security controls has also increased. *Cloud computing security* refers to the set of control-based technologies and policies designed to protect electronic information stored in the cloud. It is a sub-discipline of computer security, network security, and information security, the main goal of which is to protect data and information within the cloud from unauthorized access or theft. To achieve this, organizations employing the cloud in their operations must address the threats inside and outside their cloud infrastructure: security must evolve rapidly in congruence with constantly emerging attack vectors. In this context, organizations must stay up to date with the latest security measures. Some of the most common security measures deployed in cloud computing include data encryption, access control, and identity and access management (IAM). Data encryption protects data at rest, meaning data stored in the cloud [1]. Access control is used to restrict who has access to data and information within the cloud. Finally, IAM ensures that only authorized users can access the cloud.

Organizations must also implement security measures at the application level, such as firewalls and web application security. For instance, web application security is critical, as the web is the main access point for cloud services. Cloud computing security is a complex and ever-evolving field [2], especially given that today's cybercriminals deploy increasingly advanced tactics, techniques, and procedures. However, by implementing the proper security measures, organizations can keep their data and information safe [3]. This paper highlights security controls that businesses and individuals can deploy to secure their cloud infrastructure and information namely, IAM, data encryption, and traffic control.

## II. Identity/Access

Multi-cloud service providers must ensure that their systems and data are secure from unauthorized access and that their customers' data are protected. They must also ensure that their systems are continuously available, and that customer data are not lost or corrupted [2]. Therefore, multi-cloud service providers must implement and maintain strong security policies and procedures to protect their systems and data. They should also have a risk assessment plan to ensure that the system and data on the cloud present no new or unidentified risk to the customer.

Cloud security is a multi-layered approach, beginning with the physical infrastructure and extending to the applications and data that run on the cloud. For multi-cloud service providers, this means composing and adhering strictly to a security plan that covers all aspects of the cloud, from the data center to the application layer. The physical infrastructure which comprises the data center, network infrastructure, and the computers and storage that comprise the cloud is the initial layer of cloud security. This also ensures the security of data center infrastructure for multi-cloud service providers. Next, the application layer protects the applications that run on the cloud: web applications, mobile applications, and API security [4]. For multi-cloud service providers, this also provides for the security of the application development process, including quality assurance and security compliance. The final layer of cloud security is the data layer, in which the data stored in the cloud are protected. The layer features data encryption, data backups, and data recovery methods [5].

Multi-cloud service providers must deploy a comprehensive security program that ensures the security of the data center, the network infrastructure, the servers and storage, the application development process, and the data stored on the cloud.

Sandesh Achar is with Visvesvaraya Technological University, United States (e-mail: sandeshachar26@gmail.com).

Open Science Index, Computer and Systems Engineering Vol:16, No:9, 2022 publications.waset.org/10012673/pdf

Furthermore, multi-cloud service providers must implement an extensive cloud security plan that addresses all areas of the cloud. IAM is a vital part of cloud security for multi-cloud service providers.

IAM includes the management of user accounts, authentication, and authorization. For multi-cloud service providers, IAM also provides the direction of the access control lists (ACLs) for the data and resources on the cloud [6]. It ensures that only authorized users can access the data and resources on the cloud. IAM also helps to prevent unauthorized access: thus, multi-cloud service providers need a robust IAM solution to keep cloud data safe and to ensure uninterrupted business operations. IAM solutions should include the management of user accounts, authentication, authorization, and ACLs for the data and resources on the cloud.

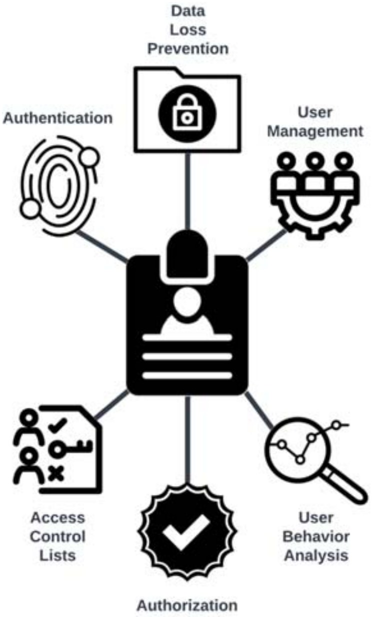

Fig. 1 Identity/access

Data loss prevention (DLP) is a strategy to ensure that sensitive or confidential data are not lost, stolen, or accidentally leaked. It can control access to data, monitor for unauthorized access, and encrypt data at rest or in transit. DLP can also refer to the software and hardware used to implement these security controls. IAM is a process for managing who has access to what data and resources in an organization. These security controls include policies and procedures for authenticating and authorizing users to access data and resources, thereby bolstering the DLP strategy. DLP and IAM are thus interlinked and are important tools for protecting sensitive data. DLP can help prevent loss by encrypting data and controlling access. IAM can help prevent unauthorized data access by authenticating and authorizing users.

## III. Data at Rest/Transit/Encryption

There are three aspects to consider when securing data in the cloud: data at rest, data in transit, and data encryption. When data are at rest, they are stored on a server or hard drive. Organizations can encrypt their data using a tool like BitLocker or FileVault to protect data at rest.

Data encryption makes it difficult for unauthorized users to access data, even if they have physical access to the server or hard drive. When data are in transit, they are being sent from one location to another. Organizations can use a VPN or TLS/ SSL to encrypt their data to protect it during transit. Likewise, data encryption makes it difficult for unauthorized users to intercept and read data as it is transmitted.

Data encryption is the process of encoding data using a key. This security measure helps to protect data at rest and data in transit. Organizations should consider all three aspects of data security when choosing a cloud service provider. Multi-cloud service providers should offer data security features, including data encryption and VPN or TLS/SSL.

Most laptop and desktop computers have built-in security features to protect your data from unauthorized access. Still, there are additional measures individuals and organizations can take to secure files further before storing them in the cloud. Two popular options are BitLocker and FileVault, designed to encrypt hard drives and prevent anyone without the proper credentials from accessing sensitive data. BitLocker is a feature included with certain editions of Windows and is available as an add-on for others. It uses the Advanced Encryption Standard (AES) method to scramble data so that they are unreadable without the proper key. One can set BitLocker to encrypt an entire hard drive or specific partitions or volumes. FileVault is a similar tool included with macOS. It also uses AES encryption to protect data and can likewise be used to encrypt your entire hard drives or just selected volumes. One advantage of FileVault is that it can encrypt a machine's startup disk, which helps to prevent unauthorized access even if someone has physical access to the computer in question. Both BitLocker and FileVault are effective ways to secure data and can help prevent unauthorized access if the computer is lost or stolen. Requiring strong passwords organization-wide is also critical, as well as enabling two-factor authentication to protect information and online accounts.

The human element is the weakest in the cybersecurity chain. Organizations should review the security policy of any multi-cloud service provider they are considering before signing up for service. Moreover, offline data backups should be secured using encryption and restricted access. An increasing concern in cybersecurity and cloud security today is ransomware; offline backups provide protection against such attacks by guaranteeing that data are not lost if malicious actors access and encrypt business data or systems.

Any security policy should account for the following considerations:

✓ What data security features are in place?
✓ How are data security breaches handled?
✓ What data security training is provided to employees?
✓ What third-party security audits have been conducted?
✓ What is the incident response plan for a data security breach?

Organizations should also consider their data security needs

Open Science Index, Computer and Systems Engineering Vol:16, No:9, 2022 publications.waset.org/10012673/pdf

when choosing a multi-cloud service provider. They should ensure that the provider offers the data security features that align with their risk appetite, scale, and business operations. Organizations should also have their data security policies and procedures firmly in place [7]. Likewise, they should consider their data security needs when choosing a multi-cloud service provider, taking care to ensure that the provider offers the data security features they need. Organizations should also have their data security policies and procedures in place.

Data at rest are stored on a physical storage device, such as a hard drive or SSD, and they are typically encrypted to protect it from unauthorized access. Multi-cloud service providers can use encryption to protect data at rest on their servers. Data in transit are typically encrypted to protect it from eavesdropping. In this case, multi-cloud service providers can use cryptographic keys to protect data in transit between their servers and customers' devices. Encryption is done to protect the data from unauthorized access: for example, multi-cloud service providers can use cryptographic keys to encrypt data or digitally sign data to protect unauthorized individuals from accessing their customers' data.

Homomorphic encryption is a type of encryption that allows mathematical operations to be performed on data while it is in an encrypted state. This means that data can be analyzed and processed without requiring decryption, which can be time-consuming and resource-intensive. There are various key management services on the cloud that provide secure storage and management of encryption keys. These services can be used to encrypt data at rest and in transit, as well as to manage and rotate keys regularly. Some of the most popular key management services include AWS Key Management Service (AWS KMS), Azure Key Vault, and Google Cloud Key Management Service (GCP KMS).

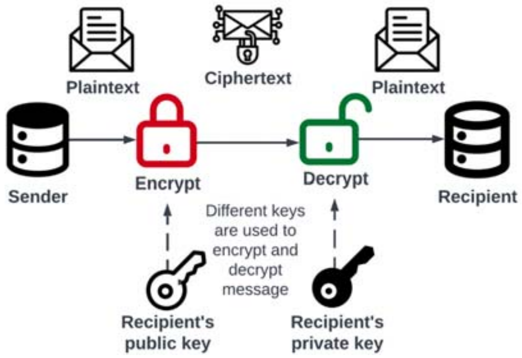

Fig. 2 Data at rest/transit/encryption

## IV. Egress/Ingress Traffic Control

Egress traffic refers to data that leave the cloud environment, whereas ingress traffic is data that enter the cloud. One of the most serious risks with egress traffic is data leakage, which can occur if data are not properly encrypted or there are gaps in the security barrier. To prevent data leakage, multi-cloud providers must ensure that all information is encrypted both in transit and at rest [8]. They must also institute a strong security perimeter, with multiple layers of security. Ingress traffic can also be a security concern, allowing malicious actors to access the cloud environment. To prevent this, multi-cloud providers must have a strong firewall in place, as well as intrusion detection and prevention systems. They also need to ensure that all data entering the environment are scanned for malware and viruses. IP whitelisting mechanisms, cloud ACLs, and firewall configurations should be highly secure to ensure proactively detecting any suspicious activity such as zero-day attacks.

Different types of access policies that can be used to control egress traffic include:

- firewalls
- intrusion detection and prevention systems
- malware and virus scanning
- data encryption

Different security policies that can be used to control ingress traffic include:

- firewalls
- intrusion detection and prevention systems
- data encryption
- user authentication
- access control lists
- activity logging
- data loss prevention

### *Illustration*

Controlling traffic between various cloud service providers can be done via egress/ingress traffic management. This safeguard can stop illegal access or limit access to particular data. For instance, if a business employs several cloud service providers, then it could want to restrict access to particular data or systems to just a few providers. By implementing egress/ ingress traffic management to permit traffic from only specific providers, the business can put this procedure into action. Another example is if a company wants to prevent sensitive data from being accessed by unauthorized people: this protection can be achieved through configuring egress/ingress traffic control to only allow traffic from only specific authorized IP addresses. Configuring egress/ingress traffic control can be a very effective way to secure data in a multi-cloud environment.

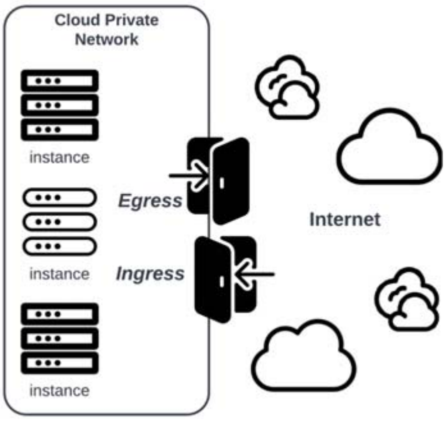

Fig. 3 Egress/ingress traffic control

### *Vulnerability/Threat Control*

One of the critical aspects of cloud security is vulnerability

Open Science Index, Computer and Systems Engineering Vol:16, No:9, 2022 publications.waset.org/10012673/pdf

and threat control. By understanding the vulnerabilities and threats within the different cloud services, organizations can take steps to mitigate and reduce the associated risks. These threats can come from various sources, including internal and external users, malicious software, and hardware failures.

One of the biggest challenges in cloud computing security is that data and resources are often distributed across several servers and locations. This architecture makes it difficult to control access to these resources and ensure that they are adequately protected. Another challenge is that cloud computing environments constantly change, with new users and applications frequently added. In making sure that only people with the proper permissions may access the data and resources, this structure makes it difficult to keep track of all the various entities and permissions. Understanding the dangers and the best defenses against them is crucial for efficiently securing data and providing assistance in the cloud [9]. Data and resources in the cloud can be secured using a variety of technologies and methods. A reliable authentication and authorization system is one of the most important security tools.

Automated and continual vulnerability management capabilities should be enabled in all multi-cloud infrastructures to immediately scan, discover, and remediate all cloud workloads for all kinds of vulnerabilities and unintended exposures. Incorporating best threat modeling practices into organizations software development life cycle is essential to identify and prioritize risk mitigation.

Robust threat modeling security methodologies for various attack vectors such as spoofing, tampering, repudiation, information disclosure, denial of service, malware and ransomware must be implemented in a multi-cloud infrastructure. Designing a process of identifying, evaluating, treating, and reporting on security vulnerabilities in multi-cloud systems and the software will enable organizations to prioritize possible threats and minimize the attack surface.

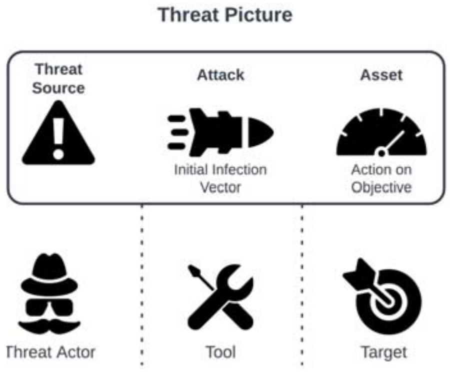

Fig. 4 Threat control

*Auditing*

Auditing in cloud computing security is the process of monitoring and assessing the safety of cloud-based systems and services. It helps organizations to ensure that their data and applications are secure and compliant with security policies and industry regulations. Auditing can be performed manually or through automated tools and through third party auditors.

Organizations should regularly engage a compliance team to perform system and control (SOC) audits on cloud infrastructure to ensure that authenticated network and host vulnerability scans are performed routinely. Issues identified during audit including inconsistencies with system security policies are assessed for remediation. In addition, audits can help verify that cloud-based systems and services comply with security policies and industry regulations.

Several types of audits can be performed on cloud-based systems and services [11]. These include security audits, compliance audits, and performance audits. Security audits assess the system's or service's security and identify potential vulnerabilities. Compliance audits assess whether the system or service complies with security policies and industry regulations. Finally, performance audits assess the system's or service's performance and identify areas where improvements can be made [12].

Organizations should consult with their cloud service providers to determine the best approach for conducting audits of their systems and services. Providers typically have experience performing systems audits and can guide the best strategy for an organization.

The audit aspect of cloud security applies to multi-cloud service providers in the same way it applies to any other organization. The main difference is that multi-cloud service providers must manage and monitor multiple cloud environments, which can be challenging. Multi-cloud service providers must clearly understand the security controls in each cloud environment and map those controls to their organization's specific needs and objectives. They also need to monitor activity across all their cloud environments and quickly identify and respond to security incidents.

To ensure effective security identification and response, multi-cloud service providers must have strong, easily understood security policies and procedures and ensure that all employees are trained on these policies and procedures [14]. A robust security monitoring system is also necessary to provide visibility into all cloud environments. Auditing is essential to cloud security, and multi-cloud service providers must ensure that they do it often and do it well. By taking the time to understand the security controls in each cloud environment, monitoring activity across all of their settings, and having solid policies and procedures in place, they can help to ensure that their organization is protected.

## V. Factors to Consider in Cloud Security

Several principal factors must be considered when developing a cloud computing security strategy. These include the data and resources that must be protected, the required security level, and the available budget. The kinds of data and resources that need to be covered will vary depending on the business and the industry: for example, a healthcare organization is beholden to different security requirements than those of a retail organization. Likewise, the level of security required will also vary depending on the business and the industry.

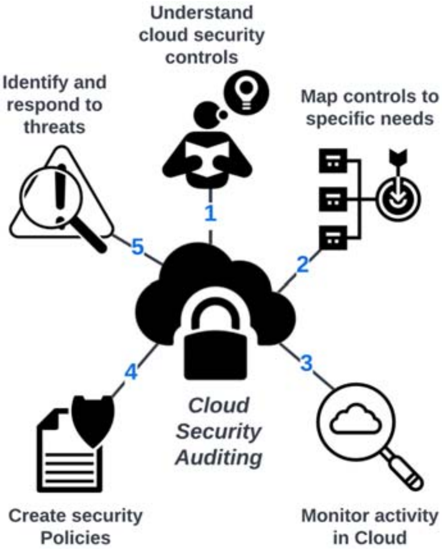
Understand cloud security controls
1
Map controls to specific needs
2
3
Monitor activity in Cloud
4
Create security Policies
5
Identify and respond to threats
Cloud Security Auditing

Fig. 5 Auditing

In some cases, compliance with regulations may require a certain level of security. In other cases, the business may prefer a certain level of protection [10]. The available budget will also play a role in the cloud computing security strategy. In some cases, the cost of the security measures may be prohibitive. In other cases, the price may be worth the investment to protect the data and resources.

Small and midsize business organizations can adopt many of the already developed internal tools rather than paying for expensive cloud native services in many cases. Adopting open-source solutions is also feasible, such as the `detect-secret` module to prevent any accidental commits of any secret tokens, passwords, or private keys in source control. Prowler is another open-source security tool that enables security assessment, audits, incident response, continuous monitoring, forensics readiness, and many security controls covering various compliance frameworks.

The cloud computing security strategy should be reviewed and updated regularly [11]. This regular quality assurance review ensures that the plan remains effective in protecting data and resources from unauthorized access, disclosure, or destruction according to the dominating cybercriminal tactics, techniques, and procedures.

A good cloud computing security strategy can help protect data and resources from various threats. However, it is essential to remember that no security measure is perfect and that there is always a risk of data or resources being compromised. The best way to protect against these risks is to have a comprehensive cloud computing security strategy that considers all the different threats and the best ways to protect against them [13].

## VI. Conclusion

As the use of cloud computing continues to grow, so does the need for security in the cloud especially for those organizations making use of multiple cloud services. The security of cloud computing is a shared responsibility between the customer and the cloud provider. The user is responsible for securing their data and applications, whereas the cloud provider is responsible for securing the infrastructure. By working together, the user and cloud provider can ensure the security of the cloud. There are many benefits to using cloud computing, but security is often a concern [15]. However, by understanding the shared responsibility model and following best practices, the cloud can be a secure place for businesses to store and process data.

Cloud security for multi-cloud service providers is a complex and ever-evolving issue. Despite the benefits, service providers must be aware of the unique security challenges that come with this type of distributed environment. To keep data and applications safe, service providers must carefully plan and implement security measures at each stage of the multi-cloud journey [16]. With the proper security measures in place, multi-cloud service providers can enjoy the benefits of this setup while keeping data and applications safe. Multi-cloud infrastructures must also enforce frequent system key rotation.

Multi-cloud service providers must take security seriously and implement robust security controls, maintaining vigilance in providing security services and educating their customers on the importance of safety. Multi-cloud service providers are responsible for providing security services to their customers and educating them on the importance of security.

Finally, a public cloud provider may not be as strict about security as the business itself, which could leave holes in the protection provided by the company. Conversely, a company may have more control over security in a private cloud environment, but cloud expenses will grow. It may seem like the ideal compromise, but a hybrid approach—half public, part remote—has its own set of issues, including regulatory enforcement across contexts.

## References

[1] Basu, Cloud computing security challenges & solutions-A survey, Annual Computing and Communication Workshop and Conference (CCWC) 2018.

[2] Verma, Cloud computing security issues: a stakeholder's perspective., SN Computer Science, 1(6), 1-8, 2020.

[3] Alsmadi, Sharing and storage behavior via cloud computing: Security and privacy in research and practice., Computers in Human Behavior, 85, 218-226, 2018.

[4] Mondal, Cloud computing security issues & challenges: A review. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE., 2020.

[5] G. Kumar, A review on data protection of cloud computing security, benefits, risks and suggestions. PDF. United International Journal for Research & Technology, 1(2), 26, 2019.

[6] Garg, Emerging trends in cloud computing security: A bibliometric analyses. IET Software, 13(3), 223-231, 2019.

[7] Rupra, A cloud computing security assessment framework for small and medium enterprises. Journal of Information Security, 11(4), 201-224, 2020.

[8] Goumidi, Vehicular cloud computing security: A survey. Arabian Journal for Science and Engineering, 45(4), 2473-2499, 2020.

[9] Raj, An exploration on cloud computing security strategies and issues. In Inventive Communication and Computational Technologies (pp. 549-562). Springer, Singapore., 2020.

[10] El-Yahyaoui, A verifiable fully homomorphic encryption scheme for cloud computing security. Technologies, 7(1), 21, 2019.

[11] Gan, Dynamical propagation model of malware for cloud computing security. IEEE Access, 8, 20325-20333, 2020.

[12] L. Hasimi, Cost-effective solutions in cloud computing security. In Developments in Information & Knowledge Management for Business

Applications (pp. 177-202). Springer, Cham., 2021.

[13] Subramanian, Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42, 2018.

[14] Balani, Cloud computing security challenges and threats. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-4). IEEE, 2020.

[15] Mondal, Cloud computing security issues & challenges: A review. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-5). IEEE., 2020.

[16] Muheidat, Mobile and cloud computing security. In Machine Intelligence and Big Data Analytics for Cybersecurity Applications (pp. 461-483). Springer, Cham, 2021.