South Asian Journal of Engineering and Technology Research Article

Open Access Full Text Article 102(2020) 1-4 DOI: 10.26524/sajet.2020.2.1

Information security controls for multi-cloud and microservices

Alok Kumar[a]
[a]Modern College of Arts, Science and Commerce, Pune

Corresponding author.
Correspondence: Alok Kumar
E-mail:alok13737@gmail.com

Article info
Received 3th May 2020
Received in revised form
10 June 2020 Accepted
13 June 2020

Keywords
Security, Information science, multi cloud, microservices

Abstract
The current study, provides the information security control process involved in multi-cloud and micro services. In recent years, there has been great demand to provide two layer securities in almost all sectors with the use of information technologies. Hence the present study highlights on the information securities and their importance.

1.Introduction

The Department of spatial information's main work offers accurate information and timely spatial information to the other governments. The spatial information is available to public users. It provides government and public services. The department of spatial information developed several web services that provide information from several internally developed web services and applications. These web applications and services are denoted as DSI online spatial delivery system (OSDS). The DSI plans to migrate all web services and applications into the cloud environment. The DSI plans to organize a Risk and Security workshop to analyze the risks, security problems and possible methods to mitigate the risks. This security workshop analyzes possible security methods that will be required to Multi-cloud and Microservices approach (1). Below information security controls of the Multi-cloud and Microservices approach have been discussed.

2.Information Security Controls for Multi-Cloud

Some information security control methods are required to Multi-cloud approach for protecting sensitive data. The security controls protecting the cloud environment and it can reduce vulnerability attacks and fraudulent activities. It should be implemented to secure cloud environments. Below information security control methods have been described for the Multi-cloud approach (2,3).

3. Protect Data using Encryption

Encryption is cryptographic functions and it is one of the information security control. Unencrypted data on cloud leads to loss of data by unauthorized users. The cloud service provider should encrypt to storing sensitive data in the appropriate place in the cloud. The encryption methods prevent servers and protecting valuable information from intruders or hackers. Encryption keys provide robust security to protecting information in the cloud environment. Encrypt sensitive data by strong encryption keys. The cloud service provider must be maintained encryption keys and this cloud service provider is responsible to keep encryption keys. The cloud service provider provides encryption tools and management services. From a prospective, you have the choice of how to manage the data security in the various cloud based systems and platforms as well as the microservices-based systems. Depending on your needs, you need to design a comprehensive set of Information Security Controls for different network environments. The requirements for the security controls that will be implemented are often both cloud-based and/or microservices. It is important to keep in mind the basic approach while designing an information security control:

4.Security Control Purpose

Security Controls for Infrastructure

The current and the future trend in the IT industry is for organizations to adopt a multifaceted approach towards the infrastructure-based security controls. There are a variety of techniques to be applied for the information security controls that are required for the system architectures. It includes the use of the security policies that are needed to secure the data that is accessed by the network. At the same time, the management of the policies also comprises a range of other security measures that secure the network by making it difficult for attackers to take access to the data that is present on the network. Also, there are a number of security controls that are required to secure the information about the procedures that are related to the security of the application layer protocols. These measures make it possible for the users to have a better level of access to the various network layers. Lastly, a variety of techniques are needed to secure the device interface, which can include the proper setting of the cryptographic keys.The organization must implement encryption tools and services. This helps to protect services and applications in a cloud environment. Encrypted data ensures anyone cannot access and alter data. The encryption methods are required to implement in the Multi-cloud approach and it effectively mitigates security issues and securely protecting sensitive information (2-4).

5.Implement Two Factor Authentication

The Two Factor authentication is one of the security mechanisms. This ensures secure credentials. The traditional password does not provide effective security in the cloud environment, but Two-Factor authentication offers robust security to protect the cloud environment. It provides an extra layer of protection in the Multi-cloud approach. This reduces cybercriminals from gaining access to sensitive data. It can prevent any type of attacks and it effectively prevents web services. The two-factor authentication security method required to Multi-cloud approach to mitigate security risks (3-5).

6.Implement Security Monitoring strategy

The cloud service provider should establish a security monitoring strategy in the cloud environment. It supervises physical and virtual servers to regularly analyze applications, data. It continuously monitoring possible threats in the cloud. It can analyze and monitor potential threats with the appropriate action. It helps to control security risks and threats. This security control required a Multi-cloud approach to reduce security issues.

7.Improve Cloud Service Provider Security Practices

The cloud service provider requires more security practices and awareness about security threats and attacks. The cloud service provider security practices make sure the securing of the platforms. If any security attacks happen the cloud service providers are responsible to takeappropriate action so the cloud service providers must well know about security attacks and remedial actions. Some services the cloud vendors are responsible for given that consist of access management, encryption software tools, and multi-factor authentication. Must improve cloud service provider security practices that required to Multi-cloud approach.These information security control methods are required to Multi-cloud approach that helps to protect web services and applications against unauthorized users (6-8).

8.Information Security Controls for Microservice

Some information security controls are required to Microservice approach for mitigating security risks and threats. The information security controls applied in the Microservice approach that efficiently

protecting data on a cloud against security threats. Below information security controls have been discussed for the Microservice approach.

9.Establish a Distributed Firewall

The cloud security administrator should establish a distributed firewall in the cloud environment. It does filtering traffic from internet networks and the internet. The firewall provides safeguard to servers against unwanted traffic. The distributed firewall applying firewall policies and provide an additional layer of protection against cyber-attacks. The cloud security administrator should install a firewall on a cloud that helps to block unwanted traffic and it provides high security to avoid unauthorized access. The distributed firewall security control is required to Microservice approach to reduce vulnerability attacks (9).

10.Establish Identity and Access Management System

Cloud computing is a technology that gives organizations the ability to access files and other information from anywhere they have an internet connection. This process of data and storage access is referred to as Identify and Access Management in Cloud Computing (IACAC). The IACAC allows organizations to use their own IP network, which can be easily linked into their cloud, to access files and information from anywhere on the planet, regardless of their geographical location.The Identity and Access Management System is a security control used to manage all applications and services and it ensures security. The identity access management's main function is authenticated devices, users, or services and to grant access rights or dent rights to access resources and data. The Identity and access management system has some effective features that include resource-level access control, high security, and a single access control interface.Identity access management can improve security for critical applications. The single access control provides an access control interface for cloud platforms. This interface can be used in every cloud service. Resource level access control grant access permissions to only authorized users from accessing data or resources at different granularity levels. It provides multi-factor authentication, access control, etc. Identity and access management must be required for the Microservice approach for authentication and access control purposes in the cloud.

11.Intrusion Detection and Prevention System

The intrusion detection and prevention system is a security control method that helps to resolve security issues in the cloud. The Intrusion detection system (IDS) is to monitor and analyze the traffic to detect malicious activities. It can be able to identify possible attacks and it takes appropriate steps to block malicious attackers. The intrusion detection system mainly focuses on monitoring traffic, detect a range of cyber threats, and analyze server activities. When vulnerability activities are detected, the intrusion detection and prevention system take necessary action to prevent services and data from malicious attacks. Must use an intrusion prevention system (IPS) tool for protecting the system. The intrusion prevention system provides possible solutions to prevent servers and services from malicious activities. IDS and IPS security controls are required for the Microservice approach.

12.Use Encryption

The encryption provides additional level security to sensitive data. The cloud service provider must encrypt data before persisting it. Use strong encryption algorithms that include RSA, AES, and DES algorithms. They make secure transmission and safer. The encryption mechanisms use effective encryption keys to protecting data and other resources in the cloud. Must keep and maintain encryption keys. Encryption is supported to protect sensitive information against cyber attackers. Encryption data the cybercriminals cannot access servers and main data storage. Encryption data cannot read and access by any peoples. Encryption provides safeguard to sensitive data that effectively protect the information in the cloud. It

ensures protect data contents and other resources in the cloud. Encryption information security controls are required to Microservice approach for protecting data and other resources in the cloud.These information security control methods are required to Microservice approach to mitigate security risks in the cloud.The information security control methods and possible solutions have been discussed to mitigate security risks. These security control methods are required to Multi-cloud and Microservice approach to minimize security attacks and protecting web services and applications (10-13).

References

1. M.Kretzschmar, M.Golling and S. Hanigk, (2011).Security Management Areas in the Inter-cloud. 2011 IEEE 4th International Conference on Cloud Computing, 762-763.
2. B.S.Farroha and D.L. Farroha, (2012).Architecting dynamic cyber defense for a secure multi-tenant cloud services environment. MILCOM 2012 - 2012 IEEE Military Communications Conference, 1-6.
3. S.M. Mohammad, Security and Privacy Concerns of the 'Internet of Things' (IoT) in IT and its Help in the Various Sectors across the World (April 4, 2020). International Journal of Computer Trends and Technology (IJCTT) – Volume 68 Issue 4 – April 2020. Available at SSRN: https://ssrn.com/abstract=3630513
4. M.A. Dave, (2013).Data Storage Security in Cloud Computing: A survey.
5. D.A.Fernandes, L.F.Soares, J.V.Gomes, M.M.Freire, P.R., Inácio, A.Bates, B.Mood, J.Pletcher, H.Pruse, M.Valafar and K. Butler, (2014). Security in cloud computing. International Journal of Information Security, 13, 95-96.
6. M.Anwar and A. Imran, (2015).Access Control for Multi-tenancy in Cloud-Based Health Information Systems. 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, 104-110.
7. M.Gangappa and B. Suseela, (2016).A Novel CP-ABE on Cloud Information Storage using CA &AA. International Journal of Research, 3, 1010-1016.
8. P.Carvallo, A.R.Cavalli, W.Mallouli and E. Rios, (2017).Multi-cloud Applications Security Monitoring. GPC.
9. B.S.Ajinath, H.S.Sunil, K.S.Digambar, B.P.Anandkumar and V.S. Nalawade, (2018).Optimizing Information Leakage and Improve Security over Public Multi- Cloud Environment. Journal of emerging technologies and innovative research.
10. S.S.Kondekar and B.M.Patil (2019).Multi Cloud Storage of Data with Cost Efficiency Using Data Centric Security. International Journal of Research, 6, 525-534.
11. S.M. Mohammad, Surya Lakshmisri , "SECURITY AUTOMATION IN INFORMATION TECHNOLOGY", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 2, pp.901-905, June 2018, Available at :http://www.ijcrt.org/papers/IJCRT1133434.pdf
12. C.E.Exceline and J. Norman, (2020). Biometric based Multi-Authority Inner Product Encryption for Electronic Health Record. EAI Endorsed Trans. Pervasive Health Technol., 5, e1.
13. S.M. Mohammad, "STREAMLINING DEVOPS AUTOMATION FOR CLOUD APPLICATIONS", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.6, Issue 4, pp.955-959, October-2018, Available at :http://www.ijcrt.org/papers/IJCRT1133443.pdf