WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Systematic Review Of Security Challenges in Devsecops For Cloud

***HARSHITHA N***

**DayanandaSagar College Of Engineering**

A B S T R A C T

Cloud computing has become a boon in the current century where most companies use cloud services to support their demands. Cloud computing on the other hand will allow you to pay how much you use its services. Once upon a time storing data on a regular basis took a lot of time and also a huge space to maintain files or data and accessing this stored data was also a hectic process. guard with a huge maintenance cost in your pocket to always safeguard your data, all you need is to get in touch with a cloud storage provider saving you both money and space with a hassle-free service anytime within a few taps on your mobile phone you are good to go. This paper is to inform IT Professionals and also software organizations why such security is important and what all challenges are faced while providing security for cloud storage through a new concept called as DevSecOps.

Keywords:security,DevSecOps, Cloud computing, Storing data, Software

## 1. Introduction

Security in simple terms means the quality or a state of being secure. The safety measures that are taken by an individual or is given to a person or a place so that one is not exposed to any attacks or is in harm's way. To be much more precise there are four types of security and they are listed as debt, derivative, equity, and hybrid security, whereas in IT security they are network security, internet security, endpoint security, cloud security, and application security.IT security or information technology security or cybersecurity protects computers, programs, networks, files, or data from unauthorized access or from malicious attacks which are intended for exploitation. Similarly, Cloud security will help to secure the usage of software-as-a-service (SaaS) applications and also the public cloud. For cloud security purposes cloud access security broker (CASB), cloud-based unified threat management (cUTM) and secure internet gateway (SIG) can be used. Cloud security is defined as a set of policies or controls or procedures that have to be followed and technologies that work together to protect cloud-based systems, infrastructure and data. These security protocols or measures are set up to safeguard cloud data, protect customer's privacy, support regulatory compliance and also setting up authentication rules for individual users and their devices.

## 2. Importance of cloud security

Cloud security is one of the main aspects which has to be prioritized when a cloud computing application is created and is made available to the users. If it is done it enhances the dependability of the application provided and the customer relationship trust will be well maintained which acts as a boon for the organization and also the IT professionals. From a business perspective, if the customers are satisfied and are highly reliant on your application, your organization will turn out to be one of the safest and topmost trustworthy organizations in the current market. Being a world-class cloud service provider, which offers best in class security which has its own personalized customization for your clients, one can easily boast its security offers with these benefits listed below: -

- Centralized security: As in cloud computing how applications centralize their data, cloud security also has its own centralization for increased protection of data. In a cloud-based business or an organization we can see a lot of networks and a huge number of devices connected to these networks, it becomes very difficult to manage and deal with this kind of network. We cannot manage endpoints especially while dealing with BYOD (Bring Your Own Device) or Shadow IT (projects managed outside IT department).

● Reliability: In association with the above benefit discussed by offering an amazing cloud service with a top-notch security measure we can gain results in ultimate cloud service dependability. With these security measures in place, the customer and also the security provider can access data and its applications present in the cloud on any device whatsoever and at any place present. Nowadays more n more organizations have realized and are moving from their traditional data storage methods to modernized cloud services. Due to this, there is a race between organizations that provide such cloud services and the urge to provide the safest and most reliable technology usability by the agile systematic approach giving them the competitive edge. It is essential for such organizations that they must have confidence in the security provided by them and all systems, applications and their data are protected from data leaks, theft, deletion and corruption.

● Reduced administration: From a business perspective lesser the number of expenses the greater fruits of profit can be reaped. This means no more manual security configurations no more warehouses with guards, and that being replaced by 24/7 security updates in any part of the world which is much more cost-effective and a massive drain on resources can be averted easily. Thanks to cloud services all security administrations are managed, maintained and updated all in one place with the least cost and are highly time-efficient. As cloud reception develops, an ever-increasing number of basic applications move to the cloud too, requiring cloud security apparatuses. We already know that Cloud security is the act of ensuring cloud-based information, applications, and framework from cyberattacks. Cloud specialist organizations don't generally give sufficient inclusion, so extra devices, as CWPPs (Cloud Workload Protection Platforms), CASBs (Cloud Access Security Brokers), CSPM (Cloud Security Posture Management), SASE (Secure Access Service Edge), or ZTNA (Zero Trust Network Access) may be important. These are some of the cloud security policies through which one can create their own security standards. The means needed to get cloud information differ dependent on the kind and affectability of the information, the cloud design number and sorts of clients approved to get to the information and that's only the tip of the iceberg.

## 3. DevOps

DevSecOps is the combination of security in data processing and DevOps[4].It is One of the latest innovations in the advancement of current programming is DevOps technology.This well-known philosophy involves hosting the turn of events and operational movement on a table.DevOps is frequently associated with a skillful organization. the techniques of the executive, since both systems are equipped with quick and efficient means of transport.DevOps is a promotional system to overcome any barriers between development (Dev) and operations, highlighting correspondence and coordination,integration, quality confirmation and mechanised shipping with an evolution group.

From the above definition, it would be possible to separate that the fundamental target of the DevOps practice is to improve the link between the turn of events and the task office and for these offices to occur in cooperation for the achievement of a product item Since the methodology is like the practical procedure, where the different partners of a company are strongly associated.

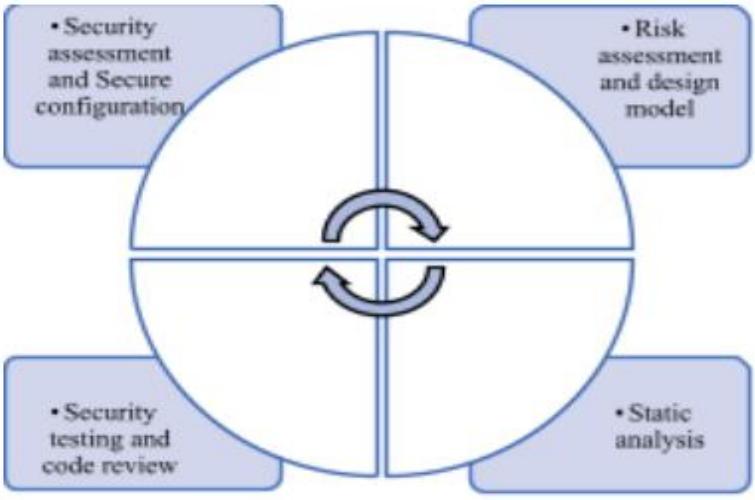
Example: Amazon Web Services (AWS) created tremendous DevOps skills.

## 4. DevSecOps

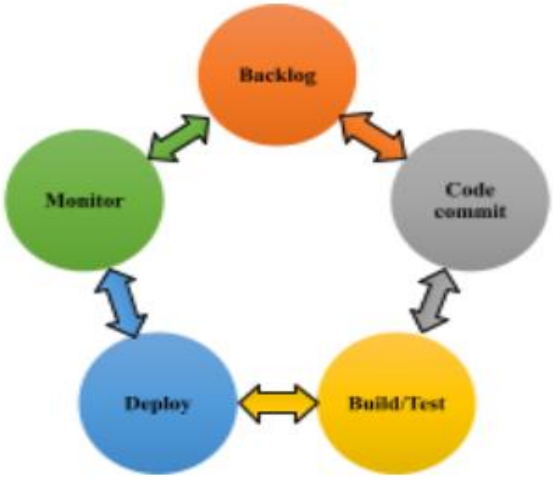
DevSecOps is a combination of security in information technology development and DevOps.Preferably, this is handled without reducing the confidence or speed of the designers or expecting them to let their toolchain development environment.If you want a simple definition of DevSecOps, "it is short for development, functioning. With the growth of the Sec(security) towards DevOps, a reflection on the coordination of security is manufactured.
The rather clear purpose of introducing an expanded security center into DevOps mechanisms is to ensure that any product or data handled in its course of events is secure as well as exercise.

Advantage of DevSecOps
- Security teams will be able to distinguish themselves by their increased speed and agility.
- The ability to respond rapidly to changes and wants.
- Teamwork and communication are more well-coordinated. • Detection and rectification of code flaws at an earlier stage
- Early detection of code flaws.

Disadvantages of DevSecOps
- Because DevSecOps cannot pinpoint the specific location of a problem in the source code, developers must hunt for errors themselves.
- DevSecOps might not be the answer to your problem.
- Companies should rely on DevSecOps for any and all minor issues.




Security and developers shifting




DevSecOps - SSDLC

## 4 Challenges faced while providing security

A functioning group of experts, planners, designers and C-level staff distinguished a list of around 25 security threats, which were then investigated by security experts who positioned them and limited them down further to the 11 most important cloud security challenges: -

**4.1 Data breaches:** Content security policies have increased the security layer which helps to identify and the types of attacks that carry out data breaches in the cloud. Through these attacks data theft, defacements of websites were done for the distribution of malware. To tackle this issue precise definition of the data that is stored was done and data encryption was implemented.

**4.2 Service misconfigurations and inadequate control change:** When the service providers offer us several features that help us meet our requirements in the application and adjust these services to suit our needs, recently in march 2020 google cloud had a similar issue in their cloud service, through research experts found out the bug where if a socket connection was used to escalate their access in cloud services a misconfiguration of data type was found as the root cause of this potential bug. This enabled the attacker to gain access to a limited scope deployment server which enabled the attacker to access the data and modify the data that was stored.

**4.3 Lack of cloud security architecture and strategies:** There are numerous organizations currently jump in to produce their cloud services in the market. Most of these low-level organizations have used open-source codes and platforms in building out their cloud services. This provides a poor security architecture since most of these open-source codes wouldn't have tackled their security issues and have passed on providing cloud services with a weak security firewall.

**4.4 Unsatisfactory identities, credentials, accesses and key management:** One of the common cybersecurity threats are linked to IAM (Identity and Access Management). Authentic credential safety, IAM scalability modifications and weak passwords/access keys without a multifactor authentication leads to poor data protection and permits easy access to attackers to steal or manipulate valuable data.

**4.5 Account hijacking/seizing/block:** As discussed in the previous challenge account seizing occurs due to the leakage or disclosure of valuable information. This compromises the cloud service which is provided and impacts maintaining the security of the cloud service provided. Phishing is also another attack that causes one's account to be blocked or seized and the root of this attack to occur is the use of open-source code with a poor security architecture. We must remember that here the login details entered by the user are already with the attacker and a simple password reset to the cloud account won't solve this issue.

**4.6 Insider threats:** This is a risk that is found within the cloud service provider's organization when an official or an employee decides to leak or disclose the data that is stored by the customer to another peer or an organization. This causes the customer to lose the trust he/she has in the organization thus leading to the downfall of the cloud service organization. The customer whose data is leaked without his/her consent can legally take action by filing a lawsuit on this particular cloud service organization.

**4.7 Insecure interfaces and APIs:** The user interface through which the customers use the cloud services is the most exposed component since it is easier for attackers to steal authentication access of this particular customer. If a secured network connection is provided for all the users accessing the cloud services this issue/challenge can be tackled since firewalls will protect the users.

**4.8 Weak control plane:** This challenge is seen from the cloud service provider when they have a weak cloud administrative consoles to save the data from the user. This causes loss of data that is stored and this leads to loss of organization reputation and revenue.

**4.9 Meta-structure and Appli-structure failures:** When the protocols and mechanisms used to develop the security platform and all the other layers are not followed by the programmers while creating the application for cloud services leads to a poorer response can be seen in finding out the loopholes in the application and all the issues that affect in the smooth functioning of the application

**4.10 Limitations on cloud usage visibility:** When un-authentic login is performed using an unauthorized application which is not permitted by the technical support of the organization and such login access was left unchecked individuals who have been granted access have stolen the data and credentials which is nothing but another cyber-attack. This unauthorized access must be shown clearly before being granted access to the organization's security authorities and should be able to trace out the login and block this particular attack from this and any other source in the future.

**4.11 Abuse and evil/wrong use of cloud services:** When an attacker disguises as a customer and wants a cloud service and has been granted access to the cloud service, this is a huge threat for the cloud service provider as well as all the other customers who are currently using these services. If this ever happens to an organization it is considered as a compromised state of the cloud service provider I. e this organization is unfit to provide cloud services.

## 5 Security measurements to be taken

The primary test of a survey of safety is its quantifiability. While this point has been talked about for more than 20 years now. The underlying issue of measuring security is as yet troublesome. Similarly, as with any estimation approach, a bunch of measures or measurements, just as scales, are required. The measurement of security is hard based on nine reasons: -

1. We can't test all security requirements.
2. Environment, abstraction, and context affect security.
3. Measurement and security interact.
4. No system stands alone.
5. Security is multidimensional, emergent, and irreducible.
6. The adversary changes the environment.
7. Measurement is both an expectation and an organizational objective.
8. We're overoptimistic

Considering these listed measurements, we have to be able to analyze the source of the security issue that has caused an issue to the cloud service which is provided. We must also bear the fact that we must be able to improvise and improve our security on future challenges that are yet to be faced by the cloud service organization.

## 6 Security review criteria

A security estimation needs to explore an execution dependent on a predefined set of standards. The examination objective of this investigation is to extricate pertinent models that could be utilized for an audit of a DevSecOps execution. As recently examined, the survey of safety execution is certainly not a minor undertaking, and in this manner, a pattern and cycle for the extraction of estimation rules should have been created and continued in the extraction cycle.

## 7 Benefits of providing security to cloud services: -

- Cost – Reduction
- Data security and integrity
- Reliability
- Efficiency
- Risk and Threat management
- Protection against DDoS attack
- Regulatory compliance
- Flexibility

7 Demerits or disadvantages of cloud security: -

- Server Downtime or loss of access to data
- Migration of cloud vendor
- Costly services for storage space
- Vulnerability in the case of an attack
- Internal technical problems
- A strong internet connection is a must

## 8 Conclusion

Currently, we have discussed providing security which is very much required for cloud computation and all the risks or challenges that we are facing and yet to face we must focus on the advantages of cloud security since most of the demerits are nullable unless there is a hardware issue, we must strive forward for the betterment of the services which we are providing and all the promises which are made to customers and to the organization to which have professed our faith too. Providing security to this huge platform is a never-ending cycle of the betterment of our services and also a challenging task where one has to undertake optimistically and there is a huge opportunity to upgrade and grow as an organization and also in person. In this year 2021 majority of the security issues are resolved within an hour and only the cyber-attacks which are happening currently are taking time within one to seven working days to be completely resolved. All the data that is lost if an occurrence of a cyber-attack the customer or the user can reclaim all the data that was stored on the cloud. Almost all the data which was restored will be uncorrupted and no traces or paths of the attacker will remain in the digital footprint of these data. Even though there are over 300 million hacking attempts per day we can still trust the cloud services due to the amount of firewall and security which are present in the DevSecOps

References

[1] Munir, Kashif & Palaniappan, Sella pan. (2013). Secure Cloud Architecture.
Advanced Computing: An International Journal. 4. 9-22. 10.5121/acij.2013.4102.

[2] Mathison, "Security Challenges and Solutions in Cloud Computing"
5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST2011) , Daejeon, Korea,
31 May -3 June 2011.

[3] Priyanshu Srivastava and Rizwan Khan. "A review paper on Cloud computing". Srivastava, Priyanshu, and Rizwan Khan. "A review paper on cloud computing." International Journal of Advanced Research in Computer Science and Software Engineering 8, no. 6 (2018): 17-20.

[4] Mr. Pavan B, Mr. Kishore H, Prof. Sunitha M "IOT-BASED BIG DATA STORAGE SYSTEMS IN CLOUD COMPUTING" E-ISSN: 2347-2693 A Research paper on Cloud Computing Vol.-6, Issue-9, Sep 2019 published on September 2019

[5] Harvard Myrbakken, Ricardo Colombo-Palacios "DevSecOps: A Multivocal Literature Review" A review paper on DevSecOps published by www.researchgate.com in 2017.

[6] Adrian Lane "Enterprise DevSecOps" A research paper published on December 10, 2019.

[7] Zaydi, Mounia & Bouchaib, Nassereddine. (2020). DevSecOps PRACTICES FOR AN AGILE AND SECURE IT SERVICE MANAGEMENT. International Journal of Information and Decision Sciences. 23. 134-149.

[8] Zissis, Dimitris & Lekkas, Dimitrios. (2012). Addressing cloud computing security issues. Future Generation Comp. Syst. 28. 583-592. 10.1016/j.future.2010.12.006