Research and Reviews: Journal of Global Research in Computer Science

ISSN: 2229-371X

The Repercussions and Remediation's of Misconfiguration in Cloud

J. Israelin Insulata*

Department of Computer Science and Engineering, Arasu Engineering College, Kumbakonam, India

Short Communication

Received: 26/08/2021
Accepted: 09/09/2021
Published: 16/09/2021

***For correspondence:**
J. Israelin Insulata, Department of Computer Science and Engineering, Arasu Engineering College, Kumbakonam, India

E-mail: info2intelligent@gmail.com

Keywords: Cloud; Misconfiguration; Cloud infrastructure; Cloud Security

ABSTRACT

Cloud provides numerous benefits for working environment. But, for the secure handling of data, the cloud users should be aware of how to safeguard their data against the general issues of misconfigurations which leads to openness of cloud data to hackers or malicious users. The incorrect configuration of cloud infrastructure is the only one biggest problem fronting the security groups and the managing teams. Configuration of cloud is quite complex process. But, it should be done correctly inorder to avoid the security risks. The cloud infrastructure misconfiguration is the biggest menace to cloud security. But, this threat can be avoidable before the risk happens and also rectifiable after the risk occurs. This article explains clearly about the repercussions and remediations of misconfigurations in cloud

INTRODUCTION

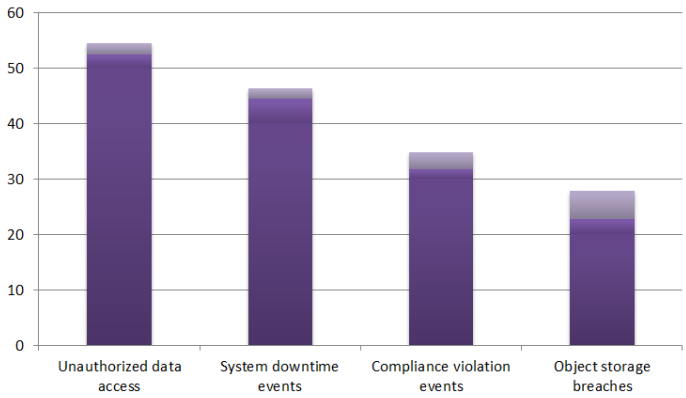
The National Security Agency of United States reported about reduction of vulnerabilities in cloud. They have submitted a list of 4 main vulnerabilities in cloud and Misconfiguration took first position in that list. Configuration is the most tedious process in any diversified networks. Distributed computing models require a dynamic, complex infrastructure set up and maintenance. In order to preserve the consistency of the system, configuration management is necessary. That is, preserving the security features and assertiveness by management of changes.

Because of the escalating needs of the distributed systems, management of configuration is the ballooning domain in research to provide a most secure realm for user to work within. Oppenheimer declared that the most problematic issues in configuration come to light while defining how the modules should communicate with one another [1].

According to the findings of North American Network Operators Group (NANOG), 700 incorrect configurations occur per month. These incorrect configuration occurrences are indescribably high. Moreover, these incorrect configurations may lead to some other misconfigurations which increase the security risk. Misconfigurations cause a greater impact on security of the users and the whole system. If diverse modules of systems to be controlled by diverse groups, then the efficient configuration of cloud infrastructure becomes a conundrum.

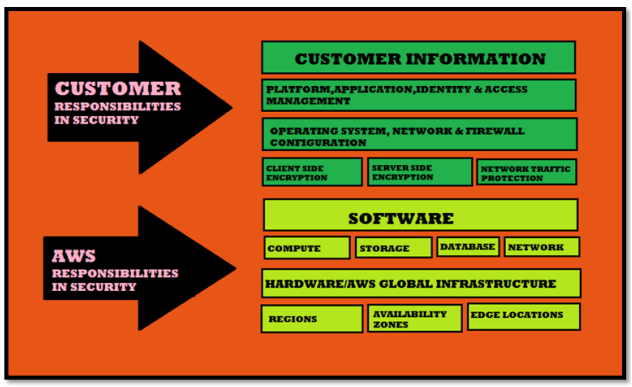
A real-time example for this misconfiguration repercussion can be unknown exposure of US military data. In May 2017, the security firm Up guard revealed that more than 60,000 government military files exposed by the defense contractor on Amazon S3 bucket. Within few months, another similar issue happened which was discovered by the Up guard. On noticing these kinds of incidents, the US National Security Agency gave warning in January 2020. The NSA warned the Organizations to hone in on safeguarding the cloud services and infrastructure.
If powerful security measures are not present, then adversaries can easily do information theft. These kinds of attacks are possible in the case where the Organization allows unrestricted access. Digital attackers can easily abuse the network of their target and can easily hack the data. Moreover, the bitter truth regarding misconfigurations is 'it is quite difficult to detect such misconfiguration (Figure 2) [2].

Figure 1. Misconfigurations comparison chart.



The above figure represents the comparisons over misconfigurations in cloud. From the comparison chart, it is obvious that, the unauthorized data access ranked top. This unauthorized data access is due to the unrestricted data access policies of the Organization. System downtime is an outcome from the system, when the system fails to function because of the unexpected event. Migration of applications to public cloud does not give assurance for security and cannot provide the regulatory compliance. The three types of data breaches are: i) physical ii) electronic iii) skimming. Loss or thefts of information, unauthorized data access, sending personal data via e-mail to wrong person are the best examples for object storage breaches (Figure 2) [3].

Figure 2. Responsibilities of CSP and customers for security in cloud.



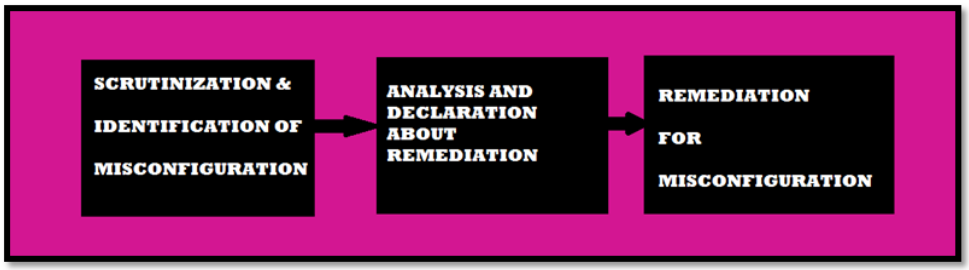
Even though this traditional model exists, still now there is no full stop for the dubiousness of responsibilities between Cloud Service Provider and the Organization. In 2018, the report given by IBM X-Force revealed that 424% hike in data fissures due to human-flaw incorrect configuration. It is clear that the human flaws are the important causes for incorrect configuration.

Remediation

To avoid misconfigurations, Organizations should impose restrictions in accessing data from cloud. Data Owner can set access policies based on user's role, attribute or identity. That is, restrictions to data access can be implemented using Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) and Identity Based Access Control (IBAC) schemes. By implementing these kinds of restrictions, there will be no data breaches and the cloud data will be more secure.

RBAC: Based on the user's role such as Manager or Employee, access permissions can be assigned to heighten the security of cloud data. If role based access control scheme implemented fairly, security of cloud data will be very high.
ABAC: Based on the attribute of every user like User-Employee-Designation-Age, access permissions will be assigned to every user. Attribute based access control scheme is an efficient technique to preserve security of cloud data.
IBAC: Based on the identity of every user like user id-password, access permissions can be assigned to every user. This identity based access control schemes are easy to follow and efficient in working (Figure 3) [4].

Figure 3. Supportive remediation.



Supportive Remediation is the general approach. In this supportive remediation, a tool is used to scrutinize the cloud infrastructure and that tool notifies about the issues identified. Then, the team member goes through the list of issues and declares whether remediations required or not. Next, team member gives remediations either manually or by making arrangements for automation.

Structured Remediation joins extra features with supportive remediation. Here, rules for describing about the problem can be given by the tool along with the structured solution. The advantages of this structured remediation are quick and correct response. But, scalability issue arises in this remediation.

Standard Implementation is the most extensive of all the remediations. Whenever problems arise, the pre-established standard scrutinizes, identifies and notifies about the occurred issues. Then, it generates quick, automated response. The benefits of this approach are: There is no human interference and more scalability. These benefits make this approach, a best one.

The other solutions include crippling administration interface, crippling of debugging, crippling the default accounts and passcodes, making sure about a fine application architecture, building the server in the way that it prevents unauthorized access, periodical scanning and auditing [5].

CONCLUSION

There are plenty of ways to prevent or rectify the misconfiguration issues in cloud. However, this paper focuses on the important, efficient and convenient approaches for the remediations of misconfigurations. By enforcing such techniques, data security can be highly assured. The repercussions and remediations are clearly explained in this paper. It showcases that repercussions of misconfigurations are high but there are numerous remediations also available. Even a minor mistake in configuration can have much impact on security of cloud data. Eventhough many

remediations are available, prevention of misconfiguration is always better than finding remediations of misconfiguration.

REFERENCES

1. Stephen C, et al. Devolved management of distributed infrastructures with Quattor. LISA. 2008;8:175-189.
2. Zhang J, et al. Encore: Exploiting system environment and correlation information for misconfiguration detection. ASPLOS. 2014;24:687-700.
3. Bleikertz S, et al. Security audits of multi-tier virtual infrastructures in public infrastructure clouds. Comput Sci. 2010; 8: 93-102.
4. Torkura KA, et al. Csbauditor: Proactive security risk analysis for cloud storage broker systems. IEEE. 2018.
5. Priebe C, et al. Cloudsafetynet: Detecting data leakage between cloud tenants. Comp Sci. 2014;7:117-128.