

Cloud Security | Review Paper

IT16178700 D.I.K. Rajapakshe

Software Engineering, Sri Lanka Institute of Information Technology

Abstract- With the advance of technology therein cloud service in the technical world. Security and privacy are very important in cloud services. People use it to save their personal and other data. There are types of cloud security in cloud service. Moreover, explaining in there is cloud security really a concern and how secure should you make your application. Considering cloud security, it was more important because every year users facing worldwide cloud breaches.

Index Terms- Cloud breaches, Cloud security, Cloud service

I. INTRODUCTION

Cloud computing is the world biggest computer system resource including save data, retrieving data, access and manipulating data in anywhere. Considering the cloud computing failures there are popular security breaches in the past. As an example, there are significant breaches facing in LinkedIn, Sony and iCloud. In 2012 6.5M LinkedIn users were hacked by hackers who got their usernames and passwords from LinkedIn database and published to public sites. After that in 2014, Sony experienced the most aggressive cyber-attack in history wherein their financials, movie project and much more was published publicly by hackers. This made a huge impacted on the business path in their company. Moreover, in 2014 iCloud service from Apple faced a similar hack wherein private images of users from their database were made public. These popular companies breach in security. Cloud security must be advanced and need to be used. There is cloud computing in the world. It is a very important thing wherein cloud service. However, users can make their data secure with the instruction of cloud security. They are giving users to instruction on how to keep safe their data. But users without having good knowledge of the IoT they are facing spam. Therefor may hackers can hack user data.

Then we consider what is the cloud security, It is a use of latest technology and techniques and program to secure your applications which is on the cloud or the data which is hosted on the cloud and the infrastructure which is associated with the cloud computer whatever security techniques or technology that you are using to secure your application should be updated as frequently as possible because every day new threads are coming up. Every day there is the new workaround to the problem. You should be able to tackle these problems or these workarounds and hence you should upgrade your security as frequency as possible.

In additionally there in sort out a few differences between Cloud Security and Traditional IT Security.

<u>Cloud Security</u>	<u>Traditional IT Security</u>
Third-Party Data Centers	In-House Data Centers
Low Upfront Infrastructure Investments	High Upfront Costs
Quickly scalable	Slow Scaling
Efficient Resource	Utilization Lower Efficiency
Reduced Time to Market	Longer Time to Market
Usage-Based Cost	Higher Cost

In the cloud computing having three type of cloud security. There are private, public and hybrid. What are the different between a public, a private and a hybrid cloud in infrastructures? In the private cloud have highly confidential files there can store on the cloud platform. There are two type ways of thinking a private infrastructure either after private servers or private infrastructure on user own premises or they can look up for servers dedicated servers by their crown provider that all comes under the private infrastructure.

In the public cloud infrastructure user would basically use website setup public facing. If users have a products page where they have application which can be downloaded by the public that can be hosted on the public cloud because there is nothing that has to be secret over there. If can be use in websites things like that is not confidential and seeing public, it can be hosted on your public cloud.

The third infrastructure is the most important infrastructure which is the hybrid infrastructure this is the setup that most companies go for that where in users have private files of highly confidential files and a website as well highly recommended to go for hybrid infrastructure which is kind of both worlds you get the security or the comfort of the private infrastructure and the cost-effectiveness of the public cloud is well. Hybrid cloud is basically if user want their highly confidential be stored on their own promises and their website being posted on their public cloud this infrastructure would be hybrid cloud infrastructure.

There is research result whether cloud security really makes sense. In Figure 3.1 shows Gartner research on companies who are making plan to move the cloud or who has not moved to the cloud most of them facing was security and privacy concerns.

Therefore, we want to concern how secure should user make their application. What are the extended to which you should make an application secure? Cloud security is a mixture of art and science. It is a science because user have to come up with new technologies and new techniques to protect this data and protect their application because they have to be prepared with the technical part but it is art as well why because they should create their techniques or they should create their technologies in such a way that their user experience is not hindered.

As an example, suppose you make an application and for making it secure after every three or five minutes if will ask the user for a password from a security point of view it seems okay but from the user point of view it actually hindering the user's experience. Therefor should have that artist in user that they should understand when to stop or till where should we extend their security techniques and creative as to what security techniques can be implemented.

As an example, there is two-step authentication user get that when they are logging into their Gmail account. Therefor if they know their password that is not enough, they should have an OTP as well to log into their Gmail account. This might be hindering with user exercise to some extent, but it is making their application secure as well. So, users should have a balance between their signs and the art path that they are applying on cloud security.

II. CONCLUSION

More than half of the companies believe that a certified and knowledgeable qualified cloud security executive will contribute a lot in securing business online in the world. The review describes the biggest cloud security breaches, which are held in day-to-day trading life. Companies can save themselves from these attacks either by hiring a cloud security expert or by adopting a suitable Cloud Access Security Broker provider. Talking about finance, both will cost the same in today's date and most of having a reasonable cost. As a solution would suggest you go for Cyber Security Service Provider because they render a package of security solutions through an automated software in there. It will provide more functionalities in comparison to an individual person without timely. Rest you need to observe the level and standard of security required in user's organization and then, go for any decision.

III. APPENDIX

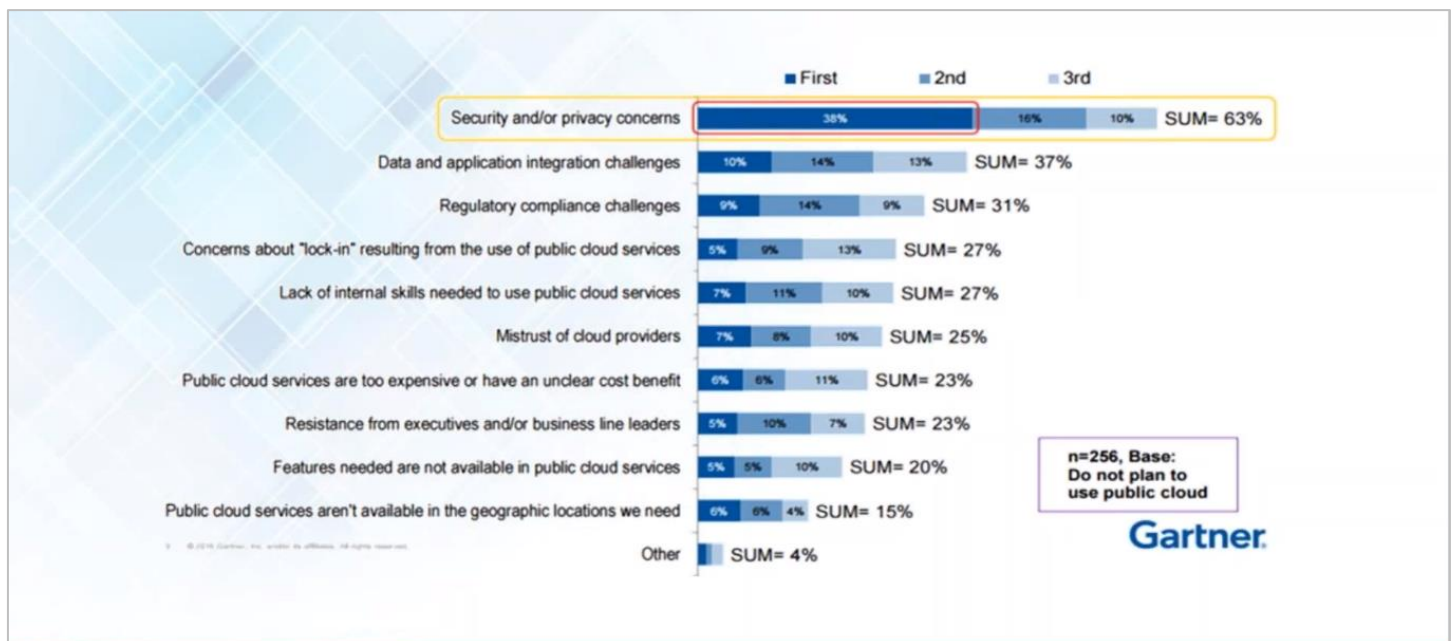


Figure 3.1

IV. REFERENCES

- [1] Aisha. O. Albadrany et al., International Journal of Networks and Systems, 7(6), October - November 2018, 8 – 12.
- [2] aws.amazon.com, 'The Beginner's Guide to Cloud Security', 2019. [Online]. Available: <https://aws.amazon.com/security/introduction-to-cloud-security/>. [Accessed: 3- March- 2019].
- [3] cloudcodes.com, 'Biggest Cloud Security Breaches in 2018', 2018. [Online]. Available: <https://www.cloudcodes.com/blog/biggest-cloud-security-breaches-in-2018.html>. [Accessed: 2- March- 2019].
- [4] edureka.com, 'AWS Architect Certification Training', 2017. [Online]. Available: <https://www.edureka.co/cloudcomputing>. [Accessed: 1- March- 2019].
- [5] edureka.co, 'Cloud Security: A Guide for Cloud Users', 2018. [Online]. Available: <https://www.edureka.co/blog/cloud-security/> [Accessed: 1- March- 2019].
- [6] MODELSWARD 2018 - 6th International Conference on Model-Driven Engineering and Software Development.