4 Security Aspects of Cloud Computing

Buen BAJRAMI
University “Kadri Zeka” Gjilan, Kosovo

4.1 Abstract

Cloud Computing is a new growing technology. Its concept is different from the technologies that already exist. It is very flexible and offers online services depending on customer’s requirements. Facilitates management and reduces the need for IT department across the company, as all services will be maintained by the cloud service provider. You will pay as much as you will use a service, unlike web hosts. There is a great and very fast development. Therefore, this has created disadvantages for companies that attach great importance to the aspect of data security. There are many companies who want to try this technology, but lack of information prevents them. Security is one of the main issues that hinder the rise of clouds. The idea of handing over important data to another company is worrying. Consumers should be vigilant about the risks of misuse of data. Through this document we will offer a detailed analysis of the security features the cloud offers. What can we improve for security? And the dangers we can afford and how we can avoid them.

Keywords: Cloud computing, services, security aspects, threats

4.2 Cloud Computing Security Threats

Cloud computing does not change much from personal computers of clients in terms of threats from viruses or other forms that aim at their damage. Namely, almost any kind of threat that could affect a computer or other device of a client may also affect cloud computing. In addition, cloud computing is even more threatened, as thousands of virtual machines work concurrently in configuration. And any damage directly affects. We are going to research for most of them.

Shared technology
Infrastructure sharing is an existence for IaaS suppliers. Disappointingly, the segments on which this infrastructure is based were not intended for that. To guarantee that clients don’t intrude on each other’s “zone", strong compartmentalization and monitoring is needed.

Data breaches
The risk of a data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

Human error
According to Jay Heiser, research vice president at Gartner, “Through 2020, 95% of cloud security failures will be the customer’s fault.”

Figure 1. *Human errors*

Data loss with no backup
An accident or catastrophe can lead to the permanent loss of customer data unless there are measures in place to back up that data.

Advanced persistent threats
Many advanced persistent threat groups not only target cloud environments but use public cloud services to conduct their attacks.

Insider threats
Insider threats to cloud security are also underestimated. Most employees are trustworthy, but a rogue cloud service employee has a lot of access that an outside cyber attacker would have to work much harder to acquire.

4.3 Conclusion

Cloud computing is a new technology that is growing steadily. The main problem with the rapid growth of cloud computing is data security and privacy issues. Reducing the cost of storing and processing data is a compulsory requirement of any organization, while data and information analysis is always the most important task in all decision-making organizations. So no organization will transfer its data or cloud information until trust is established between cloud service providers and users. There are many data protection techniques to achieve the highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is needed in cloud computing to make it acceptable by cloud service users. This primary goal was to provide basic knowledge on cloud technology and also to study data security and privacy, focusing on the storage and use of cloud data for data protection in cloud computing environments to build trust among providers cloud services and users. We hope to heighten awareness about using cloud technology.

4.4 References

[F1] International Journal of Computer Applications (0975 –8887)

[F2] H Kim, H Lee, W Kim, YKim,2010. A Trust Evaluation Model for QoS Guarantee in Cloud Systems. In Proceedings of the International Journal of Grid and Distributed Computing.

[F3] T Mather, S Kumaraswamy, SLatif,2009. Cloud Security and Privacy: An Enterprise perspective of Risksand Compliance. O'Reilly Media, Inc.

[F4] F Lombardi, RPietro, 2011. Secure Virtualization for Cloud Computing.In ProceedingsoftheJournal of Network and Computer Applications. Academic Press Ltd. London, UK.

[F5] MLouw, V.N. Venkatakrishnan,2009. BluePrint: Robust Prevention of Cross-Site scriptingattacks for existing browsers. In Proceedings of the 30th IEEE Symposium on Security and Privacy.

[F6] Bowers, K. D., Juels, A., Oprea, A. Proofs of retrievability: theory and implementation Proceedings of the ACM Workshop on Cloud Computing Security (CCSW '09) November

[F7] Rakesh, D. H., Bhavsar, R. R., Thorve, A. S. Data security over cloud International Journal of Computer Applications

[F8] Delettre, C., Boudaoud, K., Riveill, M. Cloud computing, security and data concealment Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11) July 2011 Kerkyra, Greece

[F9] Rakesh, D. H., Bhavsar, R. R., Thorve, A. S. Data security over cloud International Journal of Computer Applications

[P1] https://journals.sagepub.com/doi/full/10.1155/2014/190903#_i18

[P2] https://azure.microsoft.com/en-us/overview/what-is-iaas/

[P3] https://www.techopedia.com/definition/10254/confidentiality

[P4] http://www.diva-portal.org/smash/get/diva2:950573/FULLTEXT01.pdf

[P5] https://www.synopsys.com/blogs/software-security/10-cloud-security-threats-2018/

[P6] https://www.tripwire.com/state-of-security/security-data-protection/cloud/top-cloud-security-threats/

[P7] https://www.getkisi.com/blog/7-tips-prevent-cloud-security-threats