Project Assignment

Section B – Interim Report

During this modern time and modern world new technologies is being implemented and utilized by either multiple organizations or multiple individuals. Everybody will try to have the latest technology to work with to keep up to date with the new devices, services and technologies. When mentioning new technologies and services cloud computing is one of the main technology that almost everybody heard of and when an individual hear about cloud computing or an environment that is made from the cloud the individual will get quite curious of what this fascinating technology stands for and what the benefits can be. Cloud computing is a technology which gives the opportunity to both organizations and individuals to work remotely, to have access to their instance and control them, to view the services, and furthermore to provide a better working environment to their respective employees. But is the migration from a physical and normal environment to a cloud environment beneficial or are there some risks that when consider these risks the client may have huge concerns for the migration? (Saeed et al, 2019) mentioned that remotely stored data is preserved by a provider which offers service raises concerns which are related to either the privacy and the security of the data. (Ahmed et al, 2015) said for the migration to be an easy decision a great need to assess the risks involved when migrating to a cloud infrastructure. (Swedha et al, 2018) Mentioned types of technologies such as HTTP basic authentication and One Time Password to assist the user securing the cloud environment. After a comparison between the technologies were made to see which technology is better. (Tafazoli et al, 2016) mentioned Cloud services implemented a difficult environment to develop, managing, monitoring and incident response for a huge organization. (Narula et al, 2015) mentioned that the main concern for a company to initiate the migration to a cloud environment is the security that can be found in the cloud. (Wuyou, 2016) mentioned that data security was always the reason which delays the development of a cloud storage. (Saranya et al, 2016) mentioned that an important factor in cloud computing is the authentication, because the authentication gives the user the safety the he needs to make sure that he is communicating with the right person. It is visible that the papers that was mentioned are referring to two things, security in cloud computing and the tools to have the clients secured. There are multiple companies and individuals that are very interested to initiate the migration from a normal and usual environment to a cloud environment because of the benefits such easy access to resources, full control of the environment, full control of the users, easy services to operate with such as IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service), choose different types of cloud which the company or individuals prefers, such as private cloud, public cloud or hybrid cloud. These are the small number of features and benefits that the cloud service providers such as AWS, GCP, Azure, or OpenStack provides to their respective clients. But since there are multiple benefits, in the cloud environment disadvantages can take place, such as downtime, theft of data, data may not be accessible and breach between the conversation of instances. These are some of the drawback that are holding back the clients that are concerned of migrating to a cloud environment, although the cloud environment can be a huge advantage, it is visible and clear that there are multiple disadvantages that the clients can face when migrating to a cloud environment. (Swedha et al, 2018) in this paper, tests were initiated and done using One Time Password and HTTP Basic Authentication, the methodology of this paper was utilization of this two security tools, the author also provide a step by step documentation of how the tools were used in detail. (Ahmed et al, 2015) the methodology of this paper was quite interesting, the author provided the risks of cloud computing and after the most important are the results, the results were quantitative and the author showed which risks are the most dangerous by numbers and ranges value. (Saeed et al, 2019) the author presented the methodology stage by mentioning technologies that Azure and AWS provides to their respective clients. Technologies that include Azure Active Directory (Azure AD), Single sign on (SSO), these technologies are provided by Microsoft Azure, the AWS also offers services such as client-side encryption and server-side encryption. (Narula et al, 2015) mentioned multiple technologies that AWS offers for security, such as HTTPS, SSL and HTTS, the methodology of this paper was done by launching multiple security technologies together to try and protects their infrastructure. (Wuyou, 2016) presented the methodology of the paper by initiating two features that OpenStack provides which are the Keystone and the Swift and tried to integrate the security tools to the implemented cloud network. (Saranya et al, 2016) presented his methodology by first mentioning multiple security tools to be used in a cloud after collected multiple different papers which has to do with cloud infrastructures and their security features and compared them with one another. (Tafazoli et al, 2016) performed tests to make an evaluation of their developed organizations SOC in the environment of OpenStack, they ran two attacks which included single-step and multi-step attacks from the instances of OpenStack to other different virtual machines. All of the papers where chosen because on one main thing, security on cloud infrastructures. In every cloud network, where instances or Virtual Machines are used by their respective users, needs to be utilized in a safe way, where the clients are feeling secured, their data will be always available and also no authorized can access their data without their knowledge, without permission and most importantly without any type of authorization. Almost all of the papers that I found and used for my dissertation; their objectives were to test their respective network with tools to see whether the tool is strong enough to protect the clients from attacks mentioned earlier. These papers can be considered as qualitative but one paper that was quantitative (Ahmed et al, 2015) which presented a table of attacks that the user is afraid of, the most concerning risks for the user and the least concerning risks for the users. All of the authors were implicating that companies or individuals are very concerned with the migration because a lot of risks can be found when utilizing a cloud environment. The findings were the same, all of the security features used were successful and all of them protected the cloud environment although all of them mentioned that after some time new technologies were needed to be updated and to protect the cloud environment from stronger and robust attacks. Their respective conclusions were comparing the tools, comparing different technologies but the main thing that was interested, was that the authors mentioned that new technologies were in need to keep up with modern attacks and protect the clients and make them feel safe to be comfortable and use the cloud infrastructures. The research methodologies for all the papers had the same view, features and tools to be able to protect the cloud service providers topologies that the CSP provides to their clients. The protection includes tools to be able to protect the clients from certain attacks that does damage to the cloud infrastructures, (Ahmed et al, 2015) this paper research methodology was to identify the worst risk a user can face when utilize the cloud infrastructure. . (Swedha et al, 2018) the research question of this paper is what web authentication methods can be utilized when using Amazon Web Service? (Ahmed et al, 2015) the reseach question for this paper is what are the risks when using cloud computing and how much is their severity towards the user? (Saeed et al, 2019) the research question for this paper is what are the security features and privacy that AWS and Azure offer to their respective clients when AWS use S3 and Azure use Blob Storage services? (Narula et al, 2015) the research question of this paper is what is the cloud computing security that AWS offers? (Wuyou, 2016) What type of security OpenStack provides when the client utilizes Swift? (Tafazoli et al, 2016) the research question of this paper is What are the security features when implementing a network on OpenStack? (Saranya et al, 2016) The research question of this paper what type of security authentication features OpenStack provides for the clients? The methodologies were not the same but very similar, only one paper is not the same as the other papers because it was qualitative and provided the risks that can be met when utilize cloud computing environment. The papers presented security features, security protocols and an environment to be in use to launch the methodology and utilize the security tools to test whether an attack is successful or not when the security tool is in operation. During the research and project, it was noticeable that the user may have concerns when utilizing the cloud infrastructures, because the user may not want to take the risk of losing their respective data, another thing was that the cloud service provider create multiple tools and services for their customers to feel safe when make use of the cloud infrastructures.

References

1. Ahmed, N. and Abraham, A. (2015). *Modeling Cloud Computing Risk Assessment Using Machine Learning*. [online] https://link.springer.com/. Available at: https://link.springer.com/chapter/10.1007/978-3-319-13572-4\_26 [Accessed 7 Nov. 2019].
2. Narula, S., Jain, A. and Prachi, M. (2015). *Cloud Computing Security: Amazon Web Service - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7079135 [Accessed 30 Nov. 2019].
3. Saranya, N. and Nivedha, S. (2016). *Implementing authentication in an Openstack environment-survey - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7479966 [Accessed 13 Nov. 2019].
4. Saeed, I., Baras, S. and Hajjidab, H. (2019). *Security and Privacy of AWS S3 and Azure Blob Storage Services - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/8821735 [Accessed 15 Nov. 2019].
5. Swedha., K. and Dubey, T. (2018). *Analysis of Web Authentication Methods Using Amazon Web Services - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/8494054 [Accessed 16 Nov. 2019].
6. Tafazzoli, T. and Gharaee Garakani, H. (2016). *Security operation center implementation on OpenStack - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7881927 [Accessed 14 Nov. 2019].
7. Wuyou, L. (2016). *Design and implementation of an encrypted cloud storage system based on OpenStack Swift - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/7883089 [Accessed 17 Nov. 2019].