Security at migration data into cloud computing.

Andrés Felipe Florián Quitián

August 10, 2020.

For migrating to the cloud, it is necessary to follow some rules for the security of the data. First of all, we need to know some benefits like reaching a large audience and allow the customer to get access to their information easily. Migrate data to cloud computing implies risk, it is required to know that the migration could suffer an attack and it's probability increase each time that suffers one. Nevertheless, a feasible option is to encrypt the data. One way of encryption is to manage asymmetric encryption it could guarantee confidentiality, which manages two keys one for encrypt and the other to decrypt, on the other hand, is possible to use symmetric encryption this one only use one key for encrypting and decrypting, likewise, to transport data is useful to use https, due to, messages are end-to-end encryption.

Moreover, is important to take into account which information will be in the cloud and the permissions that employees, customers, and the administrator of the system, all of these to preserve the integrity and also the structure of the data center which encouraged the cloud.

As a consequence, is relevant to apply multifactor authentication for securing the data, this makes it difficult for the possibility of an attack. One option is to implement a second authenticator like verify the identity with something that people have or are. For example, receive codes via message. On the other hand, access to the cloud needs to be restricted each person can only have access to the information they are allowed. However, the agent can have access to all of the data. For that reason, encryption and those things mentioned before, secure the data, for instance, the integrity and confidentiality of the cloud.

The cloud must have a mobile agent that is responsible for maintaining the security and resource of data. Furthermore, could move into the cloud and have access to the information stored there, due to, this not limit the bandwidth, which implies, assure of migration of data.

Overall, to preserve the integrity, confidentiality, security at migrating or accessing data, some implementations as cryptography, multifactor system, and an agent. Helps to prevent attacks and control the process, furthermore, preserving the least privilege strengthens the system of the cloud at the limit the access to the users. In conclusion, these works for securing the migration of the data center to cloud computing and preserves the structure that is managed in the data center.

References:

[1] Kushwah, Virendra; Saxena, Aradhana. *A Security approach for Data Migration in Cloud Computing,* May 5 2013.

[2] Singh, Aart; Malhotra, Manish. *Agent Based Framework for Scability Cloud Computing*. April 4, 2012.