### Secure Cloud Computing from risk

abstract :

Technology has evolved significantly recently, whether at the level of institutions or individuals, and in this development, many services have emerged, including cloud computing.

But because it is connected to a computer network, this means that it is vulnerable to security risks, and this exposes its users to violating their privacy.

Therefore, it is imperative to put in place the protection and security of cloud computing.

Introduction :

In the last few years, we have seen a dramatic growth in IT investments, and a new term has come on the surface which is cloud computing. The National Institute of Standards and Technology defines the cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”[1]. It has five essential characteristics: on-demand self-service, measured service, rapid elasticity, broad network access and resource pooling. It is aiming at giving capabilities to use powerful computing systems with reducing the cost and increasing the efficiency and performance [1].

However, with all of these promising facilities and benefits, there are still a number of technical barriers that may prevent cloud computing from becoming a truly ubiquitous service. Especially where the customer has strict or complex requirements over the security of an infrastructure [2].

II. SECURITY CHALLENGES IN CLOUD COMPUTING

A. Data security and privacy

In cloud computing, data must be protected, and three things must be assured of the integrity of the data, its confidentiality and availability.

It is possible to store data in another country that has different regulations that may partially or completely disclose the data may be passed on to a third party to use it for any other purposes such as advertisements, etc. This is a security problem that is not easy

Data should be secured in the cloud and privacy maintained . [ 9 ]

B. Security attacks and threats

We know that things connected to the Internet, surrounded of security threats, as well as cloud computing are surrounded by security threats and attacks by hackers. Examples of these attacks:

* Cloud malware injection attack
* Metadata spoofing attack
* Account and service hijacking

Conclusions:

Security updates are necessary because they reduce potential risks, and based on the research, I concluded that laxity or failure to update the system or applications leads to a security weakness

Yes, security updates are necessary, but does that mean we only need updates?

Mostly we need individuals to awareness fraud or hacking methods in order for the system to be adequately protected.

Keyword :

Cloud malware injection attack

It is on the top list of attacks. it aims at injecting a malwares service, application or virtual machine into the cloud system [12]

Metadata spoofing attack

A web service’s server provides the metadata documents, which store all information about the web service invocation such as message format, security requirements, network location, etc. to the service clients. So, this attack aims at reengineering a web service’s metadata descriptions in order modify the network endpoints and the references to security policies [13].

Account and service hijacking

This threat could happen when an attacker hacks into a web site that is hosted in a cloud service provider and then secretly installing their software and control the cloud provider infrastructure [14].

list of references :

[ 1 ] - P. Mell and T. Grance, “The NIST definition of cloud computing,” *NIST special publication*, 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. [Accessed: 15-Oct-2012].

[ 2 ] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, Apr. 2010.

[ 9 ] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in Cloud Computing,” in *2009 17th International Workshop on Quality of Service*, 2009, pp. 1–9.

[ 12 ] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” in *2009 IEEE International Conference on Cloud Computing*, 2009, pp. 109–116.

[ 13 ] M. Jensen, N. Gruschka, and R. Herkenhöner, “A survey of attacks on web services,” *Computer Science-Research …*, vol. 24, no. 4, 2009.

[ 14 ] D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1. 0,” *Cloud Security Alliance*, 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. [Accessed: 12-Apr-2013].