Khalid Al Alshaykh

10/12/14

COM 416

Dr. Maladi

Cloud Computing

Is it secure?

Cloud Computing depends on sharing computing resources without using local servers. Cloud is a phrase that resembles the sharing process. Basically Cloud Computing is an off-site storage servers usually owned by a deferent company.

Cloud computing uses a large number of servers using an infrastructure that has massive pools of systems that are linked together. When dividing these pools into virtual servers, this will make a “cloud”. The positive thing about that is the cloud can be scaled to any size, since it is not a physical server.

Cloud computing became the norm in mass data storage industries currently. Some say it is the better choice, and some completely disagree. There are so many examples of famous cloud services that are in the web today. Dropbox, SkyDrive, Google Drive and many more that offer limited gigabytes for free and to expand your cloud, it won’t be free anymore.

Cloud Computing was not very well known before, due to the lack of technology that helps this service meets the demands of the consumer. Nowadays the service of cloud computing has all the resources it needs for fulfilling the demand. Mentioning all the positive aspects of cloud computing will not make the “elephant in the room” run away, which is the question of security (is it secure enough?).

Cloud computing has some challenges still, same as any new service that comes to life. But the most raised question in the community of consumers is the security of it. According to CSA (Cloud Security Alliance) one of the biggest threats in cloud services is data loss; it is a threat that could happen for many reasons. It could happen through carelessness from the provider, or it could happen through a natural disaster. Whose fault is it when this happens?

Another major risk in the cloud service is hacking the service. The threat of a hacker getting the data of a consumer can result lots of problems. For example hackers can monitor the activities and transactions of the user. According to CSA report, a way to defend the threat is to protect credentials from theft.

"Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible," (CSA, 2013). Another challenge is denial of service attacks, at any time a consumer that relies on their information 24/7 could face denial of service for a DoS outages.

Privacy issues:

Privacy is a challenge in cloud computing business, considering the trust in the insiders that is. A current or a former employee or such, can access the data or a system for malicious reasons. It has been mentioned that an insider can access high level of critical system and data. According to CSA "Even if encryption is implement, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack".

Organizations consider the insider attack one of the biggest concerns to data exposer. What could be unclear is that the cloud provider's employees are considered insiders as much as the organization's employees. Disregarding the benefits of cloud services, having it will surely raise the risk for inside attack or even human error.

Solutions provided:

There are as much concerns regarding privacy in cloud computing as any other services that provide data storage or software. What makes cloud computing somewhat special is that the service providers can use third parties for their own cloud usage. For example, a Software as a Service (SaaS) provider could use a Platform as a Service (PaaS) provider for building their services on. Using a third parties is usually escalates any small problems to bigger ones. A company called The Linkup was shut down after

a big data loss, they used another company to host the data for them, and that company used another application and data provider.

Cryptographic solutions in cloud computing:

Encryption is the best useful way for data protection, especially when it's transmitted. Using cryptography key lies into the hand of the subscriber, but there are ways to preserve data confidentiality and access control using cipher text. Data that can be changed and does not hinder the process of a system can be encrypted. This method can prevent third parties to access any confidential data. Also there are ways to limit data access only to authorized users which they can decrypt the data, it's called attribute-based encryption.

Generally there is a problem that comes with data encryption, which is lack of time efficiency. Decryption takes time, and encryption restricts data use. Also it is very difficult to search for an already encrypted data when one needs a plain-text data. However there are solutions for these problems as cloud technology keeps growing and evolve. One example is Searchable encryption, which allows the user to use a key which will be encoded and the cloud uses it for the search query and fetches the document intended from the search query. Another example is Fully-homomorphic encryption (FHE) which is processing data can be implemented through the encryption. FHE was mentioned as a generic solution, according to Myrto Arapinis.

However Arapinis said “FHE does not solve the problem of confidentiality from the cloud provider”, he continued “FHE is currently woefully inefficient in practice, and can only be considered usable in very specialized circumstances.”

It is clear that these methods and tools of encryptions need more research to improve it and make it work more efficiently with cloud computing.

Conclusion:

Confidentiality, Integrity and Availability is an important factor in cloud computing. Protecting data before and after transition and surly during should be implemented. Even though the main problems and the main solutions that are covered in this paper are what can define cloud technology, more research is needed definitely.

The options that will be available in the future for cloud computing are limitless, especially for the companies that implement the technology now. Insuring that companies have competitive advantages using the latest development in this technology will help them with productivity, and more important for the administrative sector, it will help with profitability.

Surely in the future the cloud computing will eliminate most if not all of the threats and challenges that the technology is facing nowadays. There are some unavoidable negatives that could affect the future of cloud computing technology; the most important one is unemployment. Will the community accept this technology or will it be shunned for sending all the IT jobs overseas.

Works Cited

Arapinis, M. (2014). *Privacy-supporting cloud computing by.* Retrieved from www.cs.bham.ac.uk.

CSA, T. T. (2013). *top-threats.* Retrieved from cloudsecurityalliance.org: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Jansen, W. A. (2011). *Cloud Hooks: Security and Privacy Issues in Cloud Computing .* Retrieved from http://www.hicss.hawaii.edu/hicss_44/bp44/st1.pdf.

Samson, T. (2013, FEB 25). *9 top threats to cloud computing security.* Retrieved 11 19, 2013, from infoworld: http://www.infoworld.com/t/cloud-security/9-top-threats-cloud-computing-security-213428?page=0,1

Sen, J. (2013). *Security and Security andPrivacy Privacy Privacy Issues in Cloud .* Retrieved from http://arxiv.org/.