60-592 Network Security Pravina Bhatt
Paper Review 2 104701991

Reviewing paper- "Cloud Computing Security Threats and Responses"

Now a days many critiques related to firewalls has created many disputes in customer centric market and rumors were set up as "firewall is dead"- as if every workforce relies on cloud based data storing. Thus, through this summary of above specified research paper I took an initiative to disagree with such baseless claim of firewall's inexistence which is being overlapped by cloud based computing techniques. In this research paper, author has step by step detailed about the security threats related to cloud computing, how the drift towards storing every data on cloud may create inconsistency of data and finally sets a base of proof about adoption of most of IT company to again maintain crucial data records remotely for which firewall is the only base to fight against security threats.

In the introductory part we can come across the exploratory description about Cloud computing, which is in demand in current technologies because of its flexible, scalable and cheaper computing methodology. This area is developing on fast pace during past few years as per researchers claim, and even adapted by various IT industries for storing, accessing and centralizing their data. As every coin has its other side, here author also claimed about severe concerns of same users, who adopted cloud computing methodology and are encountered by critical security based issues, which is creating negative impact on those potential user and there elevating interest towards shifting towards traditional methods of storing data remotely. In the initial part we come across three main types of clods such as public, private and hybrid clouds which is categorised on the basis on user accessibility in the same or other network, resources utilized and authority provided to every potential users of the network.

Secondly the paper covers information security policies that will declare every constraints dealing with the data reliability on cloud, which includes issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. This extends to analysing the importance of high performance data computing on cloud for academic verses enterprise users on the basis of seven critical security issues constraints such as privileged user access, regulatory compliance, data location, data segregation, recovery, investigate support, long term viability. The following part of the paper covers one of the most crucial drawback of cloud based computing environment that is shared responsibility, to some extent it is considered to be among one of advantage of cloud which is really vital breach with respect to security on cloud. Here we will understand about three major security issues like data leakage lead by adaptation of multi-tenant environment on single-tenant environment, cloud security issues created due to intrusion of hackers and detailed enlisting of wide variety of attacks on cloud. As the cloud can give service to legal users it can also provide service to users that have malicious purposes, most recent attacks created by potential hackers present on the network includes Distributed denial of service attack and performance of cloud against this DDos attacks.

In this section author took an edge to provide solutions for all the security breaches that affects the performance of cloud computing and enforce to setup remotely based accesses for all valuable data set access. This is majorly categorised into two parts as given below:

1. Access control: Access control mechanisms are tools to ensure authorized user can access and to prevent unauthorized access to information systems. Under the roof of access control we can understand its contribution towards cloud services using various trending technologies like Saas model which focuses on role of cloud provider to validate the users in a network and PaaS model whose emphases is in role of customer for access control to the application this not clear but direct claim of promoting remote accessibility of handling crucial data.
2. Incident countermeasure and response: Another key solution of cloud security facilitates on finding vulnerability present in the network and set a counter responses for all of the suspects. This is furthermore divide into three sections as partitioning for distributing workload among multiple computing nodes, migration supporting flexibility and workload analysis and allocation promoting collaboration of proper workload over virtual machines.

On concluding all the above specified security threats for cloud is a key proof of existence of alternatives of cloud based computing techniques proving the statement of misconception of "Data can be safe in the cloud" to be evidently untruthful. These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines. Thus author claims that even though cloud computing is fast growing and interesting technology, but it is not viable for all kind of industries motivate cloud based computation which proves that not all the industries are shifting towards cloud computing.