Abstract

Cloud is now tremendously growing technology in market. It provides us services beyond of our imagination, not only in the field of virtualization but it also facilitates in models like client/server deployment models. It provides advantage of distributed computing, grid computing, utility computing, autonomic computing, as well as various services like web services and software services. Cloud Computing provide various facilities and services to its user like, easy to use architecture, less cost and provide a delivery platform for customer and corporate world. The cloud has adapted technologies like SOA (Service Oriented Architecture) and virtualization. Basically, it is outsourced from the third party e.g. Amazon, which now becomes world’s
largest online book store. If a technology provides us various facilities and services on demand in all cases using virtualization than there will be some sort of security issues. Although Cloud provide us security at all levels but still it have various security issues like lack of security and access control, insecure information can flow on the network that can be access by multiple virtual machines. Most of the customers are nervous while they are using cloud because they are concern about risks. So, our sensitive data is not secure in cloud. In this paper, our main concern is to review the sensitive data security on trusted third party because it is responsible for providing cloud virtual environment. We also discuss various risks, threats and vulnerabilities present in cloud and various solutions proposed for securing it.

References

- J. Brodkin, Loss of Customer Data Spurs Closure of Online Storage Service &apos;The Linkup,&apos; Network World, August 11, 2008.
information security.

- VeriSign. Directories and Public—Key Infrastructure. PKI.


**Index Terms**

Computer Science

Cloud Computing

**Keywords**

Cloud Security  Sensitive Data  Trusted Third Party  Cryptography  Encryption  Xml

Based Publications

Virtualization

Threats

Vulnerabilities.