Abstract

Cloud computing is becoming very popular computing standard for network application. It is the result of existing technologies and paradigms. It is a set of resources and services offered to customers through network or internet. It provides resources that are provided as on request services to end user. It mainly aims at reduced cost, less complexity, flexibility, scalability and efficiency. Cloud computing extends various techniques such as grid computing, distributed
computing and utility computing [1]. Cloud computing is used in both industrial and academic field. The data storage as a service (DAAS) in cloud provides the user a facility to store their data in remote servers which may be accessible by the user anywhere he is through the internet facility [3]. The data stored in cloud can also be accessed by other users. There is also a possibility where a hacker can pierce the cloud by stealing a genuine user’s data. He is also capable of infecting the cloud which in turn affects the entire user's who are sharing the infected cloud. Here comes the problem of providing security to the cloud. Likewise both customer and service provider face few security threats [2]. Data communication through any network is at risk now, there are many encryption techniques used to protect the data. This paper discusses about security issues faced by client and server and also have analyzed about threats involved in different service models such as infrastructure as a service (IAAS), software as a service (SAAS) and platform as a service (PAAS). We have also tried to provide few countermeasures for those security issues.

References

- Frederick R. Carlson, "Security Analysis of Cloud Computing";
- Garima Gupta, P. R. Laxmi and Shubhanjali Sharma, "A Survey on Cloud Security Issues and Techniques";

Index Terms
Keywords