Abstract

With the advent of Information Technology in day-to-day activities, the need for online services such as storage space, software, platforms etc. is increasing rapidly. This lead to the rise of a new concept, the Cloud Computing. The Internet users rely heavily on the Cloud Computing for various computing resources. The main motive of the Cloud Providers is to provide these services in a virtualized manner. One of the main concern of cloud computing is the security of the Cloud Storage. When it comes to security of the data stored in the Cloud Storage, it is entirely in the hands of the Cloud Providers. The Cloud Providers assures the consumer of the Cloud that the data stored on their servers is safe. The consumer plays no role in securing the data. The various cloud providers claim that they provide highly secure cloud storage. But there have been attacks on hot-shot cloud providing companies such as Google, Salesforce.com and Dropbox[1]. Many cloud providers employee third party companies which has led to consumer losing their trust with these companies. Thus, the encryption techniques and the various security measures employed by the cloud providers should be equally strong. The privacy and security of cloud computing depend primarily on whether the provider has implement adequate and robust security controls as desired by the customer or not. In this paper we analyze the different security issues related to the cloud and different cryptographic algorithms to secure the cloud.
References

- Hashemi, Sajjad. "DATA STORAGE SECURITY CHALLENGES IN CLOUD COMPUTING. "
- Cloud Security Alliance (2010).
- www. wikipedia. com
Index Terms

Computer Science

Security

Keywords

Cloud security storage cryptography security issues.