

Privacy and Security Management in Cloud Environment

The wide acceptance of cloud computing is raising numerous concerns about handling of data in the cloud. Storage on a cloud provides many advantages: 1) Omnipresent access 2) High reliability 3) Flexibility 4) Scalability 5) Cost efficiency. However, there are number of security and legal risks, which should be considered. Some of them are unlawful access, sensitive data disclosure, intellectual property rights protection, communication threats as well as loads in transferring data and data integrity. Cloud data security is the most disturbing issue of cloud technology adoption. If cloud venders want enterprise or public authorities to fully outsource their data management in cloud then they have to improve security to suitable levels in cloud. Cryptography in cloud helps in increasing adoption of cloud computing by security concerned companies. The beginning level of security is the cryptography, which can help secure cloud computing. There are already some cloud providers that have started providing secure storage services with offering different levels of protection. It is observed that one of the major drawbacks of secure storage is inability to outsource the processing of the data without decrypting it. There is a requirement of technology to effectively encrypt and access the encrypted data with high degree of security on the cloud. With such technology any company's cloud can share, update, process and query data without leaking any information to the cloud provider. With this, any organization or institute can store any information in the cloud and access individual records without worrying about revelation of individual information to the outsiders.

Main objectives of the research work are as follows.

- To analyse the diverse security threats in cloud environment and to study how this security threats can be mitigated;
- To design and develop private cloud environment with secure IaaS features;
- To design and develop techniques to encrypt and access data on cloud platform for better security;
- To develop a prototype application that will demonstrate storage of data on cloud in encrypted form, allow complex mathematical operations to be performed on the encrypted data without compromising the encryption;
- To implement and analyse the results of the novel techniques contributed in this research work.

In present environment there is an urgent need to secure data in cloud without disclosing it to even cloud provider. There are many cryptography methods are available in present era but the major drawback of that cryptography methods are that user can not do searching and processing on that Data. This research might help in removing this deficiency of cloud storage with increased efficiency and security.