Abstract

Cloud computing offers numerous benefits including scalability, availability and many services. But with its wide acceptance all over the globe, new risks and vulnerabilities have appeared too. Cloud computing supplies facility of storing and accessing understanding and programs over the web without bothering the storage space on procedure. Storing the data on cloud eliminates one's worries about space considerations, buying new storage equipment or managing their data, rather they are able to access their data any time from any place provided they have internet access. However, the rising security issues have resisted the companies from connecting with cloud computing fully. Hence security risks have appeared as the main disadvantage of cloud computing. This paper involves the efforts to research the security risk and then proposes a framework to address these risk on the authentication and storage level in cloud computing. While addressing the security issues the first and the foremost thing is to classify what data needs security and what data needn't bother with security and hence data gets classified into two classes sensitive and non-sensitive. To achieve data classification, a data classification approach based on the confidentiality of data is proposed in this paper.
Following that an efficient security mechanism must be deployed by means of encryption, authentication, and authorization or by some enhanced means of security techniques to ensure the privacy of data on cloud storage.

References

14. H. Banirostam and a Hedayat, “A Trust Based Approach for Increasing Security in

**Index Terms**

Computer Science  Distributed Systems

**Keywords**

Cloud Computing, Data confidentiality, Security, Data Hiding, Machine learning, Cloudsim, Datacenter, Resource, Data Privacy