Abstract

Cloud computing is the delivery of cloud services over the Internet. Cloud services becoming popular because people are able to access their email, social networking site from anywhere in the world, at any time, at minimal charge or no charge. Cloud storage allows users to store their data remotely and use the on-demand high quality cloud applications without load of local hardware and software management. It moves the application software, databases and the important data to the centralized huge data centers, where the management of the data and services may not be fully secure. When user store their data on the cloud, there may be a risk of losing the data, or sometimes data may be modified or updated. It may not be fully secure because the client does not have copies of all stored data. To protect outsourced data against
corruption enabling data integrity protection, fault tolerance and efficient recovery for cloud storage is required. This paper delivers a survey about, different data integrity techniques and their limitation. The data integrity techniques for privacy preservation are POR (Proof of Retrivrability), PDP (Provable Data Possession), HAIL (High Availability and Integrity Layer for Cloud Storage), erasure codes etc.

References

- Sravan Kumar R, Ashutosh Saxena, Data Integrity Proofs in Cloud Storage, 978-1-4244-ss8953-4/11/@ 2011 IEEE.
- Ayad F. Barsoum and M. Anwar Hasan, Provable Possession and Replication of Data over Cloud Servers

Index Terms

Computer Science

Distributed Systems
Keywords
Data Integrity  Proof Of Retrievability  Provable Data Possession  Replication Based System