

Cloud Data Security Using Map/Reduce Implementation of Secret Sharing Schemes

Authors : Sara Ibn El Ahrache, Tajje-eddine Rachidi, Hassan Badir, Abderrahmane Sbihi

Abstract : Recently, there has been increasing confidence for a favorable usage of big data drawn out from the huge amount of information deposited in a cloud computing system. Data kept on such systems can be retrieved through the network at the user's convenience. However, the data that users send include private information, and therefore, information leakage from these data is now a major social problem. The usage of secret sharing schemes for cloud computing have lately been approved to be relevant in which users deal out their data to several servers. Notably, in a (k,n) threshold scheme, data security is assured if and only if all through the whole life of the secret the opponent cannot compromise more than k of the n servers. In fact, a number of secret sharing algorithms have been suggested to deal with these security issues. In this paper, we present a Mapreduce implementation of Shamir's secret sharing scheme to increase its performance and to achieve optimal security for cloud data. Different tests were run and through it has been demonstrated the contributions of the proposed approach. These contributions are quite considerable in terms of both security and performance.

Keywords : cloud computing, data security, Mapreduce, Shamir's secret sharing

Conference Title : ICPDCS 2016 : International Conference on Parallel and Distributed Computing Systems

Conference Location : Paris, France

Conference Dates : December 29-30, 2016