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. However, a limitation of these methods is that first they do not consider long term data storage and second they assume that data tempering only occurs at retrieval time, after the distribution of the shares has been correctly done. In this paper these two problems are addressed by presenting a novel scheme to ensure a perpetual secure data storage and retrieval.
References


Index Terms

Computer Science, Distributed Systems

Keywords

cloud computing; data security; secret sharing; blinding; distributed digital signature; threshold cryptography.