Light Weight Encryption Technique for Group Communication in Cloud Computing Environment

Abstract

Cloud computing is a typical example of distributed computing and emerged as a new paradigm that moves computing and data away from desktop and portable PCs into large data centers. Cloud services have three broad categories based on the fundamental nature of the cloud-based solution they provide: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), or software-as-a-service (SaaS). In this work we have focused on the SaaS services provided by the Cloud service providers (CSP). The issue with SaaS is data security and confidentiality that makes the cloud user reluctant towards the cloud services. Data confidentiality can be achieved by encrypted outsourced content before outsourcing to cloud servers. But due to excessive computation of existing cryptographic algorithms and distributed nature of cloud computing, there is a need of a light weight cryptographic technique that has less computational overhead and high throughput. In this paper a light weight encryption technique is proposed which has less computational time and overall good performance. In order to prove it, the proposed algorithm is compared with the existing encryption techniques and results are analyzed. The key distribution of the shared key and secret key between the two group members is also handled efficiently using the same algorithm. Enormous overhead
due to the large key size has been effectively ruled out in this paper. Light weight nature of proposed algorithm is well suited for distributed nature of cloud servers for an efficient processing with greatly enhanced user's confidence in cloud computing.

References

- Kai Hwang, Deyi Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE INTERNET COMPUTING 2010, Pg 14-22
Index Terms

Computer Science Security

Keywords

Distributed computing Cloud computing Encryption Software as a service (SaaS)

Data security