Abstract

Security is often cited as one of the most contentious issues in Cloud computing. It is argued that as the Cloud is intended to handle large amounts of data, attackers can be sure of a high pay-off for their activities. In addition, to benefit from the Economies of scale, the applications and operating systems are homogenized to a few images restricting the variations of products used within the Cloud. Millions of users are surfing the Cloud for various purposes, therefore they need highly safe and persistent services. The future of cloud, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. We propose a simple data protection model where data is encrypted using AES and Authenticated by Diffie Hellman algorithm before it is launched in the cloud, thus ensuring data confidentiality and security.

References

Cloud Computing Security Improvement using Diffie Hellman and AES


Op-ed: Encryption, not restriction, is the key to safe cloud computing. Available Online: http://www.nextgov.com/cloud-computing/2012/10/oped-encryption-not-restriction-key-safe-cloudcomputing/58608/


Index Terms

Computer Science, Distributed Systems

Keywords

Cloud computing, AES, D-H Algorithm, Security.