Abstract

In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect on performance of computing and for them cloud providers have to find a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. This paper discusses to which degree this scepticism is justified, by presenting the Cipher Cloud. The Cipher Cloud is a framework that lets users keep their data confidentially on public cloud frameworks. To achieve this, the Cipher Cloud uses a two-step encryption process, in by which all the data sent from a client to a cloud server or vice versa is kept totally encrypted and confidential. The most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. As the most promising cloud computing approach, this paper suggests selective encryption techniques, which almost gives the data confidentiality just like private cloud models.
References

- Xing Zhou, Xiaofei Tang 2011, Research and Implementation of RSA Algorithm for Encryption and Decryption, Department of Computer Science and Technology Harbin, china.

Index Terms

Computer Science
Security

Keywords

Google App Engine   Eclipse IDE