Abstract

Cloud computing is an imminent revolution in information technology (IT) industry because of its performance, accessibility, low cost and many other luxury features. Security of data in the cloud is one of the major issues which acts as barrier in the implementation of cloud computing. In past years, a number of research works have targeted this problem. In this paper discuss some of the data classification techniques widely used in cloud computing. The objective of data classification is to find out the required level of security for data and to protect data by providing sufficient level of security according to the risk levels of data. In this paper also discuss a survey of existing solutions for security problem, discuss their advantages, and point out any disadvantages for future research. Specifically, focus on the use of encryption techniques, and provide a comparative study of the major encryption techniques.

References

1. S. K. Sood, 2012 A combined approaches to ensure data security in cloud computing,
8. Feng Zhao, Chao Li, Chun Feng Liu 2014, A cloud computing security solution based on fully homomorphic encryption, IEEE Advanced Communication Technology (ICACT), pp. 485 - 488
9. Xin Dongy, Jiadi Yuy, Yuan Luoy, Yingying, Guangtao Xuey and Minglu Li, 2013, Achieving Secure and Efficient data collaboration in Cloud computing, IEEE, pp1-6

Index Terms

Computer Science
Information Sciences

Keywords

Cloud Computing, Data Classification, Data confidentiality, Cryptography, Caesar Cipher, Vigenere Cipher, fully Homomorphic, and Hierarchical Identity Based Encryption (HIBE).