Design and Implementation of an Algorithm to Enhance Cloud Security

Abstract

Cloud computing concept has been envisioned as architecture of the next generation for Information Technology (IT) enterprise. The Cloud computing idea offers with dynamic scalable resources provisioned as examine on the Internet. It allows access to remote computing services and users only have to pay for what they want to use, when they want to use it. But the security of the information which is stored in the cloud is the major issue for a cloud user. Cloud computing has been flourishing in past years because of its ability to provide users with on-demand, flexible, reliable, and low-cost services. With more and more cloud applications being available, data security becomes an important issue to the cloud. In order to make sure security of the information at cloud data storage end, a design and implementation of an algorithm to enhance cloud security is proposed. With a concept, where the proposed algorithm (PA) combines features of two other existing algorithms named Ceaser cipher and Attribute based cryptography (ABC). In this research work, text information are encrypting using "Caesar Cipher" then produced cipher text again encrypted by using proposed algorithm (PA) with the help of private key of 128 bits. And in the last step of encryption process, based on ABC, attribute related to cipher text is stored along with cipher text.
generated after encryption which provide two-step authentication during decryption process. A
security approach is designed and developed for data security concept regarding higher
confidentiality and authenticity for the cloud data at cloud storage end with experiment analysis
to authenticate its efficiency. From the result analysis it is clearly seen that the proposed
technique has better Avalanche Effect and execution time than existing technique and hence
can be incorporated in the process of encryption/decryption of any plain text or on any key
value.

References

- Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf,
- P. Mell and T. Grance, "The nist definition of cloud computing"; special publication 800-145; US Department of Commerce, Gaithersburg, MD, 2011.
- Keiko Hashizume, David G Rosado, Eduardo Fernandez-Medina, Eduardo B Fernandez
- Shuaishuai Zhu; Xiaoyuan Yang; Xuguang Wu "Secure Cloud File System with
- Chao Yang ; Weiwei Lin ; Mingqi Liu &quot;A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security; IEEE International Conference on Emerging Intelligent Data and Web Technologies, 2013.
- Preeti Garg, Dr. Vineet Shanna, &quot;An Efficient and Secure Data Storage in Mobile Cloud Computing through RSA and Hash Function;&quot; IEEE, 2014.
- Neha Tirthani, Ganesan R &quot;Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography;&quot;.

Index Terms

Computer Science
Security

Keywords