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 Caesar 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,
  &quot; NIST Cloud Computing Reference Architecture&quot;; US Department of Commerce,
  Gaithersburg, MD, 2011.
- P. Mell and T. Grance, &quot;The nist definition of cloud computing&quot;;, special
  publication 800-145,&quot; US Department of Commerce, Gaithersburg, MD, 2011.
- Bhaskar Prashad Rimal, Eunmi choi, Ian Lumb, &quot;A Taxonomy and Survey of Cloud
- Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, &quot;Service-Oriented Cloud Computing
- Mohammad Sajid, Zahid Raza, &quot;Cloud Computing: Issues & Challenges&quot;;
  International Conference on Cloud, Big Data and Trust 2013.
- Ramgovind S, Eloff MM, Smith E, &quot;The Management of Security in Cloud
- Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez
  &quot;An analysis of security issues for cloud computing&quot;;, Journal of Internet Services
- Sherif El-etriby, Eman M. Mohamed, &quot;Modern Encryption Techniques for Cloud
- Hamdan M. Al-Sabri, Saleh M. Al-Saleem &quot;Building a Cloud Storage Encryption
- Mao-Pang Pang Lin, Trend Micro, Taiwan, Wei-Chih Hong, Chih-Hung Chen, Chen-Mou
  Cheng &quot;Design and Implementation of Multi-user Secure Indices for Encrypted Cloud
- Shivani Gambhir, Ajay Rawat, Rama Sushil, &quot;Cloud Auditing: Privacy Preserving
  using Fully Homomorphic Encryption in TPA&quot;;, International Journal of Computer
  Applications, Volume 80, Number 14, 2013.
- Cong Wang, S. -M. Chow, Qian Wang, Kui Ren , Wenjing Lou &quot;Privacy-Preserving
  Public Auditing for Secure Cloud Storage&quot;;, IEEE Transactions on Cloud Computing,
- Shuaishuai Zhu ; Xiaoyuan Yang ; Xuguang Wu &quot;Secure Cloud File System with


- Neha Tirthani, Ganesan R "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography".


Index Terms

Computer Science  Security

Keywords