IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

Secure File Storage on Cloud Using Hybrid Cryptography Algorithm

Rushikesh Sadalage[1], Harshvardhan Shinde[2], Niprita Shetty[3], Shruti Dubhale[4], Prof. Sujay Pawar[5]
Student, Information Technology[1, 2, 3, 4]
Assistant Professor, Information Technology[5]
Dr. D. Y. Patil Institute of Technology, Pune, Maharashtra, India

Abstract: Cloud is used in various fields like industry, military, college, etc. for various services and storage of huge amount of data. Data stored in this cloud can be accessed or retrieved on the users request without direct access to the server computer. But the major concern regarding storage of data online that is on the cloud is the Security. This Security concern can be solved using various ways, the most commonly used techniques are cryptography and steganography. But sometimes a single technique or algorithm alone cannot provide high-level security. So we have introduces a new security mechanism that uses a combination of multiple cryptographic algorithms of symmetric key and steganography. In this proposed system 3DES (Triple Data Encryption Standard), RC6 (Rivest Cipher 6) and AES (Advanced Encryption Standard) algorithms are used to provide security to data. All the algorithms use 128-bit keys. LSB steganography technique is used to securely store the key information. Key information will contain the information regarding the encrypted part of the file, the algorithm and the key for the algorithm. File during encryption is split into three parts. These individual parts of the file will be encrypted using different encryption algorithm simultaneously with the help of multi threading technique. The key information is inserted into an image using the LSB technique. Our methodology guarantees better security and protection of customer data by storing encrypted data on a single cloud server, using AES, DES and RC6 algorithm...

Keywords: Cloud Computing and Storage, AES Algorithm, RSA Algorithm, Blow fish Algorithm

REFERENCES

[1] ”Fatf-gafi.org - Financial Action Task Force (FATF)”, Fatf-gafi.org,2016. [Online]. Available: http://www.Fatf-gafi.org. [Accessed: 22-Dec- 2015].
[2] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).
[3] Rewagad, P., & Pawar, Y. (2013). Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.
[4] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.
[5] Sunita Sharma, Amit Chugh:’Suvey Paper on Cloud Storage Security’.
[6] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (Smart Cloud).