IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

Hybrid Cryptography: Secure File Storage on Cloud using AES, RC6 and Blowfish Algorithm

Trupti Mankar[1], Nirmala Sagar[2], Pooja Bhusari[3], Snehal Gulbhamwar[4], Prof. Dhananjay Dumbere[5]
Students, Department of Information Technology[1,2,3,4]
Professor, Department of Information Technology[5]
Rajiv Gandhi College of Research and Technology, Chandrapur, Maharashtra, India

Abstract: *In this era, cloud computing 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, RC6 (Rivest Cipher 6), AES (Advanced Encryption Standard) and Blowfish 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 multithreading 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, RC6 and Blowfish algorithm..*

Keywords: Cryptography, Encryption, Decryption, Cloud Storage, Cloud Security

REFERENCES

[1] A. K. Shahade, V.S. Mahalle, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm", IEEE, INPAC, pp 146-149, Oct .2014.
[2] Palash Uddin, Abu Marjan, "Developing Efficient Solution to Information Hiding through text steganography along with cryptography", IEEE, IFOST, pages 14-17, October 2014.
[3] R. T. Patil and P. S. Bhendwade , "Steganographic Secure Data Communication",IEEE, International Conference on Communication and Signal Processing, pages 953-956,April 2014.
[4] Klaus Hofmann and S. Hesham, "High Throughput Architecture for the Advanced Encryption Standard Algorithm" IEEE, International Symposium on Design and Diagnostics of Electronic Circuits & Systems, pages 167- 170, April 2014.
[5]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).
[6] 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.
[7] Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). RSA Encryption and Digital Signature. 2011 International Conference on Computational and Information Sciences.
[8] Sunita Sharma,AmitChugh:'Suvey Paper on Cloud Storage Security'.
[9] Rawal, B. S., & Vivek, S. S. (2017). Secure Cloud Storage and File Sharing. 2017 IEEE International Conference on Smart Cloud (SmartCloud).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, May 2023

[10] Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using a hybrid cryptography algorithm. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 1635–1638. https://doi.org/10.1109/wispnet.2016.7566416

[11]. Shaikh, S., & Vora, D. (2016). Secure cloud auditing over encrypted data. 2016 International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/cesys.2016.7889842

[12]. Gajendra, B. P., Singh, V. K., & Sujeet, M. (2016). Achieving cloud security using third party auditor, MD5, and identity-based encryption. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304–1309. https://doi.org/10.1109/ccaa.2016.7813920

[13]. Bhandari, A., Gupta, A., & Das, D. (2016). Secure algorithm for cloud computing and its applications. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 188–192. https://doi.org/10.1109/confluence.2016.7508111

[14]. Taha, A. A., Elminaam, D. S. A., &Hosny, K. M. (2018). AN IMPROVED SECURITY SCHEMA FOR MOBILE CLOUD COMPUTING USING HYBRID CRYPTOGRAPHIC ALGORITHMS. Far East Journal of Electronics and Communications, 18(4), 521–546. https://doi.org/10.17654/ec018040521

[15]. Kranthi Kumar K, Devi T,(2018). Secured Data Transmission in Cloud Using Hybrid Cryptography. International Journal of Pure and Applied Mathematics, 119(16), 3257-3262.

[16]. Shimbre, N., & Deshpande, P. (2015). Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. 2015 International Conference on Computing Communication Control and Automation. doi:10.1109/iccubea.2015.16

[17]. Ronak Karani ,TejasChoudhari , Anindita Bhajan , Madhu Nashipudimath 2020). Secure File Storage Using Hybrid Cryptography.2020 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, 6(9).

[18]. Shakeeba S. Khan, Prof.R.R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms”, 2015

[19]. Anjali Patil, Nimisha Patel, Dr. Hiren Patel “Secure data sharing using cryptography in cloudenvironment”, 2016

[20]. Fortine Mata, Michael Kimwele, George Okeyo, “Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish