The Design and Implementation of a Secure File Storage on the Cloud using Hybrid Cryptography

Gift Chisoni[1] and Dr. Glorindal Selvam[2]
Master of Computer Science, DMI-St. Eugene University, Zambia[1,2]
gchisoni@gmail.com[1] and glorygj@yahoo.com[2]

Abstract: *In recent years, cloud computing has become a popular way of storing and sharing data. However, security concerns have been raised about the safety of sensitive information stored on the cloud. Hybrid cryptography, which combines symmetric and asymmetric encryption, has been proposed as a solution to these concerns. This paper proposes a new hybrid cryptography approach for secure file storage on the cloud regardless of the type of deployment model i.e., either public cloud, private cloud, or hybrid cloud. The proposed approach uses a combination of the Advanced Encryption Standard (AES) algorithm, Triple Data Encryption Standard (DES) algorithm, and Rivest cipher 6 (RC6) algorithms are used to provide block-wise security to data. LSB steganography technique is introduced for key information security.*

Keywords: Hybrid Cryptography, Cloud Computing, Secure File Storage.

REFERENCES

[1]. Shrikanta Jogar1 & Darshan S Handral. (2022). "Secure File Storage on Cloud Using HybridCryptography", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).

[2]. Gajanan T, S. Jayde, H.Gaurkhede, R. Vaidya, A.Wankhade& V.Yelekar. (2021). "Secure File Storage on Cloud Using Hybrid Cryptography", International Research Journal of Engineering and Technology (IRJET). ISSN: 2395-0056.

[3]. M.Naveetha Krishnan&T.Tamilarasan. (2021). "Secure File Storage on Cloud UsingHybrid Cryptography", International Journal of Advanced Research in Computer Science Engineering and Information Technology (IJARCSEIT).

[4]. Uttam Kumar, Mr. Jay Prakash. (2020). "Secure File Storage On Cloud Using Hybrid Cryptography Algorithm", International Journal Of Creative Research Thoughts (IJCRT). ISSN:- 2320-2882 [Base Paper].

[5]. Aditya Poduval, Abhijeet Doke, Hitesh Nemade& Rohan Nikam. (2019). "Secure File Storage on Cloud using Hybrid Cryptography", International Journal of Computer Sciences and Engineering (IJCSE).E-ISSN: 2347-2693.

[6]. M. Malarvizhi, J. Angela JennifaSujana, T.Revathi. (2014). "Secure File Sharing Using Cryptographic Techniques In Cloud",International Conference On Green Computing Communication And Electrical Engineering (ICGCCEE).

[7]. Rawal, B. S., & Vivek, S. S. (2107). "Secure Cloud Storage and File Sharing". IEEE International Conference on Smart Cloud (SmartCloud).

[8]. A. Buhari, A. Mubarak, B. Bodinga, and Muazu D. Sifawa. (2012). "Design of a Secure Virtual File Storage System on Cloud using Hybrid Cryptography". Int. J. Advanced Networking and Applications

[9]. Maitri, P. V., & Verma. (2016). "Secure file storage in cloud computing using a hybrid cryptography algorithm". International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),

[10]. Ping, Z. L., Liang, S. Q., & Liang, L. X. (2011). "RSA Encryption and Digital Signature". (2011), International Conference on Computational and Information Sciences.

[11]. 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".International Conference on Communication Systems and Network Technologies.

[12]. Anjali DV, Dr. S.N Chandrashekara. (2016). "Design and Implementation of Secure Cloud Storage System using Hybrid Cryptography Algorithms with Role-based Access Control Model", IJETR

[13]. 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.

[14]. Aman Kumar, Dr.Sudesh Jakhar, Mr. Sunil Makka. (2012). "Comparative Analysis between DES and RSA Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2 Issue.

[15]. M. N Wahid, A. Ali, B. Esparham, M. Marwan. (2018)."Comparison of crypto. Algo: DES, 3DES, AES, RSA & blowfish for guessing attacks prevention" in 2018 Comp Sci Appl Techno.

[16]. Ashish Sharma, Dinesh Bhuriya, Upendra. (2017). Singh Survey of stock market prediction using machine learning approach "International conference of Electronics, Communication and Aerospace Technology (ICECA)".

[17]. Mr. Gajanan N. Tikhe, Mr. Jeetendra Ambulkar. (2011). "A Certificate-Based Scheme to Defend against Wormhole Attacks in Ant-based Adaptive Multicast Routing Protocol for MANET", in ICCCT, Delhi

[18]. Mr. Gajanan N. Tikhe, Mr. Yogadhar Pandey. (2012) "A Secure Scheme to Avoid Wormhole Attacks in Ant-based Adaptive Multicast Routing Protocol for MANET", IFRSA's International Journal Of Computing (IIJC) Volume 2, Issue 1, ISSN (Print):2231:2153, ISSN (Online):2230:9039

[19]. Dan Dobre, Paolo Viotti, Marko Vukolic. (2017). " Hybris: Robust Hybrid Cloud Storage", ACM Transactions on Storage, Vol . 13, Issue 3, October 2017

[20]. Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing.

[21]. Kumar, A., Lee, B. G., Lee, H., & Kumari. (2012)."Secure storage and access of data in cloud computing". International Conference on ICT Convergence (ICTC).

[22]. A. Nadeem. (2006). "A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, pp. 84-89.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-9067

462

ISSN
2581-9429
IJARSCT