IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

Hybrid Encryption Model using One-Time Pad and Route Cipher algorithm with Integrity Check (Using MD5 hashing)

Niyanth Guruprasad, Sushanth Ravishankar, Dr. R. Renuka Devi
Department of Computing Technologies
SRM Institute of Science and Technology, Chennai, India
niyanthgp@gmail.com, sushanthpvr@gmail.com, renukadr@srmist.edu.in

Abstract: *The world is moving forward in terms of internet connectivity. While this enhances connectivity and strengthens communication, it brings with it its shortcomings. The advent of internet went hand in hand with emergence of hackers. This made businesses vulnerable and prone to malicious attacks by various groups and organizations. The business, to safeguard the data of the clients and consumers had to fool proof their servers and data-centres, hence the need to enhance and tighten security and close various vulnerable points. Cryptography is a technique involving encryption of data and messages so that only the intended audience can decrypt and comprehend it. For enhanced security, a hybrid encryption technique along with integrity check (MD5 hashing) is used. The encryption technique of One Time Pad (OTP - symmetric) and Route cipher (trans- positional) are combined and used.*

Keywords: Hybrid Encryption, Symmetric and Asymmetric Cryptography Algorithm, Encryption and Decryption, Message- Digest5, One-Time Pad Cipher

REFERENCES

[1]. S. Vatshayan, R. A. Haidri and J. Kumar Verma, ”Design of Hybrid Cryptography System based on Vigene`re Cipher and Polybius Cipher,” 2020 International Conference on Computa- tional Performance Evaluation (ComPE), 2020, pp. 848-852, doi: 10.1109/ComPE49325.2020.9199997.

[2]. Chaudhari, Swapnil. (2018). A Research Paper on New Hybrid Cryp- tography Algorithm.

[3]. Y. Alkady, M. I. Habib and R. Y. Rizk, ”A new security protocol using hybrid cryptography algorithms,” 2013 9th International Com- puter Engineering Conference (ICENCO), 2013, pp. 109-115, doi: 10.1109/ICENCO.2013.6736485.

[4]. A. Chauhan and J. Gupta, ”A novel technique of cloud security based on hybrid encryption by Blowfish and MD5,” 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017, pp. 349-355, doi: 10.1109/ISPCC.2017.8269702.

[5]. V. K. Soman and V. Natarajan, ”An enhanced hybrid data security algorithm for cloud,” 2017 International Conference on Networks and Advances in Computational Technologies (NetACT), 2017, pp. 416-419, doi: 10.1109/NETACT.2017.8076807.

[6]. M. J. Dubai, T. R. Mahesh and P. A. Ghosh, ”Design of new security algorithm: Using hybrid Cryptography architecture,” 2011 3rd Interna- tional Conference on Electronics Computer Technology, 2011, pp. 99- 101, doi: 10.1109/ICECTECH.2011.5941965.

[7]. S. A. Ahmad and A. B. Garko, ”Hybrid Cryptography Algorithms in Cloud Computing: A Review,” 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), 2019, pp. 1-6, doi: 10.1109/ICECCO48375.2019.9043254.

[8]. Arroyo, Jan Carlo and Dumdumaya, Cristina and Delima, Allemar Jhone. (2020). Polybius Square in Cryptography: A Brief Review of Literature. International Journal of Advanced Trends in Computer Sci- ence and Engineering. 9. 3798-3808. 10.30534/ijatcse/2020/198932020.

[9]. X. Li, L. Yu and L. Wei, ”The application of hybrid encryption algorithm in software security,” 2013 3rd International Conference on Consumer Electronics, Communications and Networks, 2013, pp. 669-672, doi:

10.1109/CECNet.2013.6703419.

[10]. Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 616-622, doi: 10.1109/CDS52072.2021.00111.

[11]. G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 3688-3693, doi: 10.1109/ICEEOT.2016.7755398.

[12]. D. S. Solanki and S. Shiwani, "A model to secure e-commerce transac- tion using hybrid encryption," 2014 International Conference on Con- trol, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, pp. 642-645, doi: 10.1109/ICCICCT.2014.6993040.

[13]. Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Com- puting," 2018 International Conference On Advances in Communica- tion and Computing Technology (ICACCT), 2018, pp. 187-190, doi: 10.1109/ICACCT.2018.8529627.

[14]. Saravanan, P., Kumar, R.H., Arvind, T., Narayanan, B. (2019). Hybrid Cryptosystem Using Homomorphic Encryption and Elliptic Curve Cryp- tography Algorithm, i-manager's Journal on Computer Science, 7(1), 36-42. https://doi.org/10.26634/jcom.7.1.15667

[15]. Goyal, Kashish and Supriya Kinger. "Hybrid Approach Using Encryption Algorithms For Data Storage." (2013).