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

Secure Text Transfer Using Doubly Encrypted Chat Application Based on Cloud

Simi Jain[1], Vaishali Nirmalkar[2], Bhagyashri Rewatkar[3], Archana Nikose[4]
Students, Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science and Engineering[5]
Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
simijain2000@gmail.com[1], vaishalinirmalkar0@gmail.com[2], bhagyashri132001@gmail.com[3],
nikose.archu@rediffmail.com[4]

Abstract: *One of the most important ways to preserve information security is to use cryptographic techniques. It provides digital signature, authentication, secret sub-storage, system security, and other capabilities in addition to keeping the information confidential. As a result, the encryption and decryption solution can secure information secrecy, as well as information integrity and certainty, to avoid tampering, forgery, and counterfeiting. The security of encryption and decryption algorithms is determined by the algorithm's internal structure and mathematical rigour, as well as the key secrecy. The key in the encryption algorithm plays a crucial role; if the key is released, anybody may use the encryption system to encrypt and decrypt data, rendering the encryption process ineffective. As a result, the encryption and decryption solution can secure information secrecy, as well as information integrity and certainty, to avoid tampering, forgery, and counterfeiting. The security of encryption and decryption algorithms is determined by the algorithm's internal structure and mathematical rigour, as well as the key secrecy. The key in an encryption algorithm plays a critical role; if the key is released, anybody may use the encryption system to encrypt and decrypt data, rendering the encryption technique ineffective. As a result, throughout the encryption and decryption process, the type of data you pick to be a key, how you disseminate the private key, and how you preserve both data transmission keys are all critical considerations.*

Keywords: Cryptographic Techniques

REFERENCES

[1]. Honda, K., Hu, R., Neykova, R., Chen, T. C., Demangeon, R., Deniélou, P. M., Yoshida, N. (2014). Structuring communication with session types.In Concurrent Objects and Beyond, pp.105-127,Springer Berlin Heidelberg.
[2]. Iwamoto, M., Omino, T., Komano, Y., Ohta, K. A new model of Client-Server Communications under information theoretic security. In Information Theory Workshop (ITW), pp. 511-515, 2014.
[3]. Chouhan, K., Ravi, S. (2013). Public Key Encryption Techniques Provide Extreme Secure Chat Environment. International Journal of Scientific & Engineering Research, 4(6), pp. 510-516
[4]. Anjaneyulu, G.S.G.N., Reddy, U.M. (2012). Secured directed digital signature over non-commutative division semirings and Allocation of experimental registration number,International Journal of Computer Science, Vol. 9, Issue 5, No. 3, pp:376-386.
[5]. Desmet, L.,Johns, M. (2014). Real-time communications security on the web. IEEE Internet Computing, 18(6), pp.8-10.
[6]. Khanezaei, N., Hanapi, Z. M. A framework based on RSA and AES encryption algorithms for cloud computing services. In Systems, Process and Control (ICSPC), 2014 IEEE Conference on, pp. 58-62, 2014.
[7]. Vollala, S., Varadhan, V. V., Geetha, K., Ramasubramanian, N. (2017). Design of RSA processor for concurrent cryptographic transformations. Microelectronics Journal, 63, pp.112-122.
[8]. Rajesh, M., Sairam, R., Big data and health care system using mlearningJournal of Recent Technology and Engineering, Volume-7 Issue-6S3 April, 2019.

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

[9]. Chandramouli, R., Iorga, M., Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In Secure Cloud Computing , pp. 1-30, Springer New York

[10]. Goshwe, N. Y. (2013). Data encryption and decryption using RSA Algorithm in a Network Environment. International Journal of Computer Science and Network Security (IJCSNS), 13(7), pp.9-13.

[11]. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19), pp.33-38.

[12]. Rajanbabu, D. T., Raj, C. Implementing a reliable cryptography based security tool for communication networks.

[13]. In Science Engineering and Management Research (ICSEMR), 2014 International Conference on, pp. 1-4, 2014.

[14]. Lent, C. S. (2013). Learning to program with MATLAB: Building GUI tools. John Wiley & Sons.

[15]. Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Das, R. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm.In 33 Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual, pp. 332-337, 2017.

[16]. Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). Modified RSA encryption algorithm (MREA).In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pp. 426-429.