IJIRMET ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering and Technology
Vol. 8, Issue 6, June 2023

To Secure The Data On The Cloud Using RSA Algorithm With Triple DES Algorithm

[1] B.Lavanya,M.Phil.,[2] Mrs. V.Ramya Msc.,M.Phil.
[1]Government Arts College for Men, Nandanam, Chennai – 600 035.
[2] Assistant Professor,Government Arts College for Men, Nandanam, Chennai – 600 035.

Abstract— Cryptography is consider as the secure communication technique, that allows only the sender and verified recipient of a message to views its content. Nowadays, people stores their data in cloud but the security of the data is a major issue. In our proposed work we use hybrid cryptographic algorithm to sort out the issue. It helps to provide greater security on data which is stored on cloud. RSA and TRIPLE DES algorithm are used to provide superior security to store the data's. Our proposed algorithm is working efficiently and give more security on data with less time.

Keywords—Cloud; RSA Algorithm; DES Algorithm; KeyGeneration; Private key; Public key; Secret key;

Authentication; Encryption; Decryption.

1. INTRODUCTION

In the current era, different technologies are used all over the world. The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drivers. The data can be anything such as files, images, documents, audio, video and more. Small as well as large IT company, we need a Server Room that is the basic need of IT companies. In that server room, there should be a database server, mail server, networking, firewalls, routers, modem, switches, QPS (Query Per Second means how much queries or load will be handled by the server), configurable system, high net speed, and the maintenance engineers. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing comes into existence. There are lot of algorithms are available for data security like symmetric and asymmetric algorithm in cryptography. Bunch of these algorithms contains AES, BLOWFISH, RSA, and DES, triple DES etc. all algorithms are used for data integrity, confidentiality and availability of data which are major concern in cryptography field and for security purpose.
Triple DES (3DES) is a type of encryption algorithm that offers enhanced security through

its triple-layered encryption technique. Triple DES (3DES) is a modified version of the Data

Encryption Standard (DES) algorithm that was developed by IBM in the 1970s. DES was widely used in the 1980s and 1990s, but its 56-bit key size was deemed insufficient for modern security needs. As a result, in the late 1990s, the National Institute of Standards and Technology (NIST) started a project to find a new encryption standard that would be more secure than DES.

PROPOSED WORK

In this proposed system we can store data's on cloud security using RSA and TRIPLE DES algorithm. In this first level we apply RSA algorithm to convert. In this process the data will be our plaintext into unreadable cipher text encrypted by Rivest Shamir Adhelman(RSA) algorithm. At the second level of encryption, the cipher text came from the first stage is under process with TRIPLE DES algorithm.

ADVANTAGES:

1. It solves the problems of distributing the key for encryption
2. Public key encryption allows the use of digital signature which authorize the recipient of a message to verify that the

message is exactly from a particular sender

3. The use of digital sign in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.

TRIPLE DES and RSA combine to create a very secure algorithm. For the second layer of security, we use Data Encryption Standard Algorithm to encrypt the data generated in the first stage. Cloud data uploads become more secure after applying TRIPLE DES and RSA algorithms. Triple DES (3DES) is a type of encryption algorithm that offers enhanced security through its triple-layered encryption technique.

Block Cipher Encryption: 3DES is a block cipher encryption algorithm that operates on 64-bit blocks of plaintext at a time.
Symmetric Key Encryption: 3DES uses a symmetric key encryption system, meaning that the same key is used for both encryption and decryption.
Triple Layer Encryption: 3DES uses three different keys to encrypt the plaintext three times, hence the name Triple DES.
Variable Key Size: 3DES supports variable key sizes, ranging from 128 to 192 bits, offering enhanced security compared to DES.
Advantages of 3DES
Enhanced Security: The triple-layered encryption technique of 3DES provides enhanced security compared to DES.
Widely Used: 3DES is a widely used encryption algorithm, and is included in many encryption standards and protocols.
Compatible: 3DES is backward compatible with DES, which means that it can be used in legacy systems that still use DES.
Customizable Key Sizes: 3DES supports variable key sizes, which makes it more adaptable to different security need.
ENCRYPTION PROCESS
The encryption process of 3DES involves the following steps:
Key Generation: Three unique keys are generated using a key derivation algorithm.
Initial Permutation: The 64-bit plaintext is subjected to an initial permutation.
Three Rounds of Encryption: The plaintext is encrypted three times, each time using a different key, to create three layers of encryption.
Final Permutation: After the three rounds of encryption, a final permutation is applied to the output to produce the ciphertext

While uploading the data to cloud, plaintext first encrypt the data using RSA algorithm then its generate the Cipher text 1. Cipher text 1 provide the encryption using triple DES algorithm which generates the Cipher text 2. Cipher text 2 uploading the data in cloud storage.

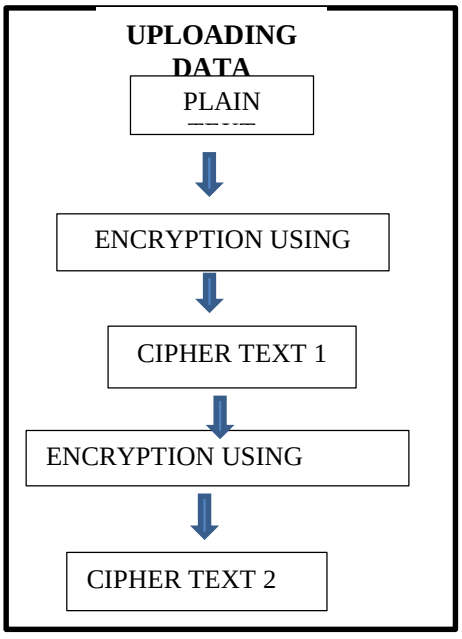


Fig. 1 (a) Uploading data on cloud

ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering, and Technology
Vol. 8, Issue 6, June 2023

Decryption Process

The decryption process of 3DES is simply the reverse of the encryption process, with the ciphertext being fed into the algorithm and the steps being performed in reverse order, using the three keys in reverse order.

Advantages of 3DES

- Enhanced Security: The triple-layered encryption technique of 3DES provides enhanced security compared to DES.
- Widely Used: 3DES is a widely used encryption algorithm, and is included in many encryption standards and protocols.
- Compatible: 3DES is backward compatible with DES, which means that it can be used in legacy systems that still use DES.
- Customizable Key Sizes: 3DES supports variable key sizes, which makes it more adaptable to different security needs.

Applications of 3DES
3DES is widely used in many applications, such as:
Financial Transactions: 3DES is used to secure financial transactions, such as online banking, credit card processing, and electronic fund transfers.
VPNs: 3DES is used to secure virtual private networks (VPNs) to provide secure communication between remote locations.
Healthcare Systems: 3DES is used to secure patient information in healthcare systems, such as electronic health records and medical imaging systems.
Government Communications: 3DES is used to secure government communications, such as military communications and secure data transfers.
While downloading the data from cloud first cipher text 2 is decrypted using Triple DES algorithm which provide Cipher text 1. Cipher text 1 is generate to decrypt using RSA algorithm which generate the plain text

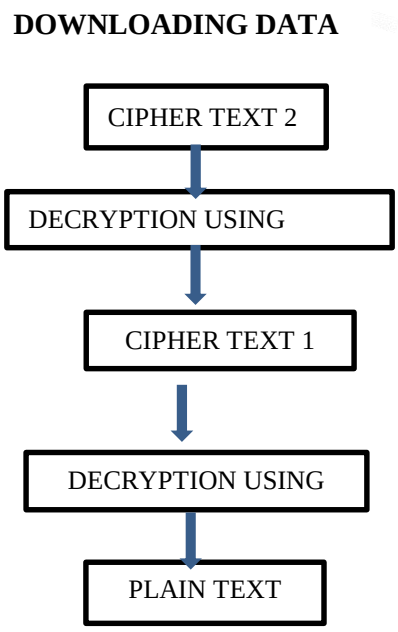


Fig. 1 (b) Downloading data from cloud
Triple DES algorithm

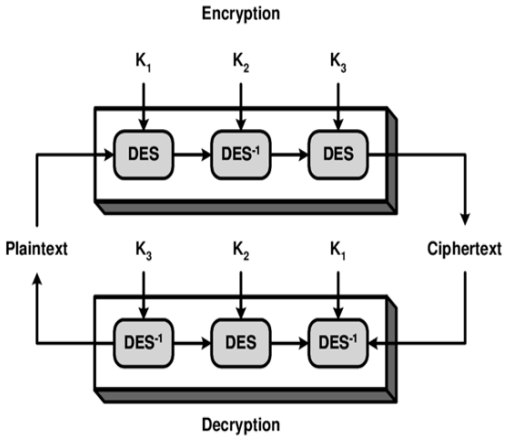


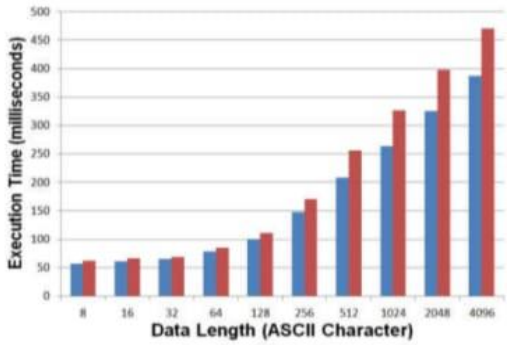
Fig.2 Diagram of Triple DES Algorithm

The Encryption scheme can be denoted as:

C(x) = EK3(DK2(EK1(P(x))))
Encrypt plaintext using the key K1; decrypt using key K2 and encrypt the resultant using K3.
And the Decryption scheme can be denoted as:
P(x) = DK3(EK2(DK1(C(x))))
Decrypt the plaintext using the key K1; encrypt using key K2 and decrypt the resultant using K3.
Where:
P(x) is the plaintext
C(x) is the ciphertext
EK is the encryption using a key K
DK is the decryption using a key K

RESULT AND ANALYSIS

In this work, a new security system is proposed using hybridization of RSA and Triple DES algorithms for cloud storage. The proposed approach is implemented in JAVA programming language on a sample plain text. Figure is showing the snapshot of implementation of the proposed approach.



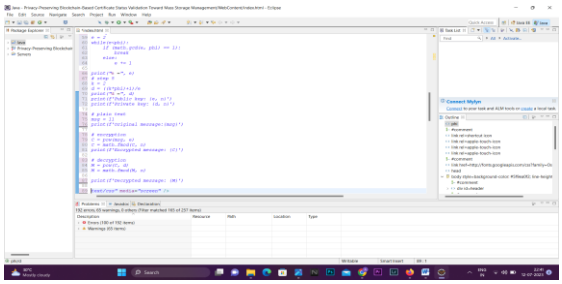


Fig. 3 Snapshot showing working of proposed security architecture for cloud storage

CONCLUSION

RSA and Triple DES algorithms are used in this paper to propose a hybrid technique for cloud-based data storage. We implement and simulate the proposed technique on a sample plain text string. The proposed technique is more secure than these algorithms, according to the results.

REFERENCES

[1] V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa&Aes) encryption algorithm,"2014 International Conference on Power, Automation and Communication (INPAC), Amravati, 2014, pp. 146-149.doi: 10.1109/INPAC.2014.6981152

[2] A. A. Kumar, Santhosha and A. Jagan, "Two layer security for data storage in cloud," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Noida, 2015, pp. 471-474.doi: 10.1109/ABLAZE.2015.7155041

[3] K. Saini, V. Agarwal, A. Varshney and A. Gupta, "E2EE For Data Security For Hybrid Cloud Services: A Novel Approach," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida (UP), India, 2018, pp. 340-347. doi: 10.1109/ICACCCN.2018.8748782

[4] N. L. Kodumru and M. Supriya, "Secure Data Storage in Cloud Using Cryptographic Algorithms," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India,2018,pp.1-6.doi: 10.1109/ICCUBEA.2018.8697550

[5] N. Jayapandian, A. M. J. M. Z. Rahman, S. Radhikadevi and M.Koushikaa, "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-4.doi: 10.1109/STARTUP.2016.7583904

6] P. Yellamma, C. Narasimham and V. Sreenivas, "Data security in cloud using RSA," 2013 Fourth International Conference on Computing, Communications and Networking Technologies
(ICCCNT), Tiruchengode, 2013, pp. 1-6.doi: 10.1109/ICCCNT.2013.6726471

[7] V. K. Pant, J. Prakash and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography," 2015 International Conference on Green Computing and Internet of Things
(ICGCIoT), Noida, 2015, pp. 490-494.doi: 10.1109/ICGCIoT.2015.7380514

[8] D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and
security (ids), Beijing, 2017, pp. 145-149.doi: 10.1109/BigDataSecurity.2017.12

[9] A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON),
Greater Noida, Uttar Pradesh, India, 2018, pp. 633-636.doi: 10.1109/GUCON.2018.8675033

[10] WenpingGuo, Zhenlong Li, Ying Chen and Xiaoming Zhao, "Security design for Instant Messaging system based on RSA and triple DES," 2009 International Conference on Image Analysis and
Signal Processing, Taizhou, 2009, pp. 415-418.doi: 10.1109/IASP.2009.505465

[11] G. Jain and V. Sejwar, "Improving the security by using various cryptographic techniques in cloud computing," 2017 International