 ISSN: 2321-8169
85 – 87

A Study of Data Transmission Algorithm for Secure Data Storage by using Cloud Computing

Ashish A. Patokar
Research Scholar
Dept. of Computer Science & IT,
Shri Shivaji College, Akola
ashishpatokar@gmail.com

Dr. V. M. Patil
Head & Associate Professor
Dept. of Computer Science & IT,
Shri Shivaji College, Akola
vinmpatil21@yahoo.co.in

Abstract— A secured data transmission by using cloud computing is a hot topic in a process of data transmission. In the fast process of data transmission the digital data exchange through cloud computing play an important role in case of data storage and transmission. Cloud computing solve many problems of use of peripheral devices handling, a peak load of data transmission, installing software, software uploads. In that features develop a various encryption algorithms so that the information can exchange securely through the authenticated person for that purpose develops a various algorithms include RSA, DES, 3DES and AES. In this paper study the data transmission algorithms with fastest transfer and secured data storage by the survey of various encryption algorithms.

Keywords- *AES, DES, RSA and 3DES, Cloud computing*

*****

I. INTRODUCTION

In the present Scenario number of business communities trading and banking transaction are used the public networks & demand for end-to- end to secured connections as well as should be confidential, ensured data authentication, accountability, confidentiality, integrity and measured show of the availability of the networks [1]. The resources include hardware, software firmware, information/ data and communications in these transactions the security is the main concern. Security is a mechanism in which information and related services are protected from un-authorized access, up gradations and hacking. In such transactions cryptography is the main concern about the security. The main aspects of the encryption are to guaranty the security of the sensitive data or information. The encryption, decryption algorithms performances and transmission on plaintext. The various encryption algorithms are available for the purpose information security. These encryption algorithms are divided into two parts mainly symmetric and asymmetric key. In the symmetric key encryption and decryption for performing by the same key and in asymmetric key encryption and decryption performing by the different key. From that one is public key and other private key. In short we can say that public key encryption and all these key is a form of cryptosystem [2].

Fig 1 Encryption-Decryption Flow

II. PROBLEM STATEMENT

In Cryptographic algorithm i.e. symmetric and asymmetric plays a vital role but the data access on Public, private, hybrid and community cloud. In this case security of the data is main goal. Suppose sender can send data to receiver in these processes of sending a data some data may be loss during sending or the attackers or hackers attacks on that data. The main problem is to give the permission of authorized users to access the secure data and not to the unauthorized users and these data kept away from the third party. For the point of security purpose cryptographic techniques such as symmetric and asymmetric keys are used and the data may be transmitted in the encrypted and decrypted form.

III. SECURITY ALGORITHMS

A. AES

AES stands for Advanced Encryption Standard and is a symmetric encryption algorithm. AES developed by two Belgian cryptographers Joan Doeman and Vincent Rljmen. AES is used to protect sensitive information implemented in hardware and software. It is suitable, suppose want to encrypt a private text into decrypt able format [3], [4]. The best example is, when demand to send sensitive information in email. The decryption of this information is possible if know the correct password. AES is six time faster than triple DES. AES performs all its computations on bytes than bits. The key length of AES is 128 bits.

 ISSN: 2321-8169
85 – 87

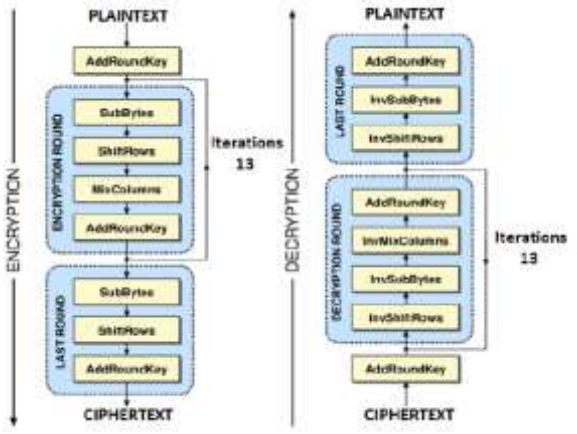

Figure 2. Architecture of AES Algorithm

B. DES

DES means data encryption standard is a symmetric key algorithm. DES uses the same key for encrypt and decrypt the message and the same private key is well-known by the one and other i.e. sender and receiver. DES takes 64-bits of plain text as an input and produces 64-bits of cipher text. The key length of DES is 56-bits and can be switch any time [5], [6]. DES is insecure for many applications due to 56-bit key size is too small. DES uses standard arithmetic and logical operations on number of 64-bits and implemented in late 1970s on hardware technology.

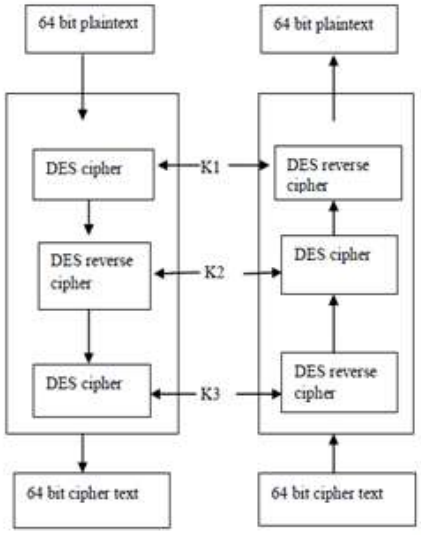

Figure 3. Architecture of DES Algorithm

C. RSA

RSA is invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. RSA is asymmetric or public key cryptographic algorithm. RSA is able to pillar encryption and digital signatures. RSA used the variable size key and encryption block [7], [8]. The main benefit of these algorithm is to upgrade the security. RSA defict in encryption speed. Big service providers such as Google mail, Yahoo mail etc. are used these algorithms for security purpose due to its outstanding performance [9]. D. 3DES 3DES or triple DES is a symmetric-key block cipher standard and is similar to DES. 3DES is slower as compared to other process. The key size of 3DES is 192 bits with block size is 64 bit. 3DES performs 3 times iterations of DES [10], [11].

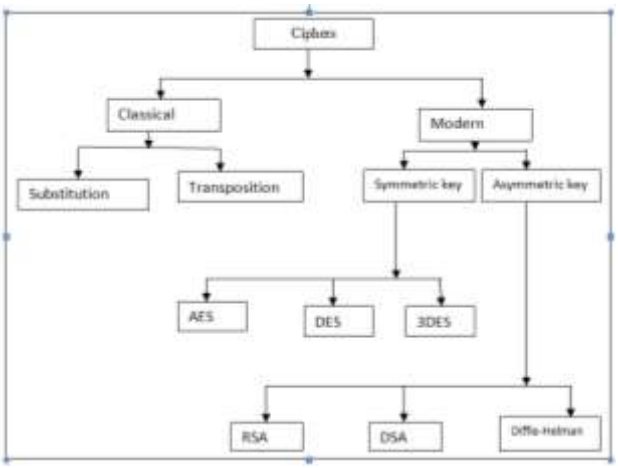

Figure 4. Classification of Encryption Mechanism

IV. COMPARISION AES, DES, RSA & 3DES

The following table compared the different cryptographic algorithms on the basis of performances given by the algorithms. By comparing their speed, security and Cipher form etc.

Factors	AES	DES	3DES	RSA
	Joan Doeman and Vincent Rljmen	IBM	IBMIN	Ron Rivest, Adi Shamirand Leonard Adleman
Years	2001	1975	1978	1978
Speed	fast	Slow	Veryslow	Slowest
Cipherform	Symmetric	Symmetric	Symmetric	Asymmetric
Security	Excellent	Notsecure	Fairsecurity	Lesssecure
Key Size(bit)	256	56	128	1024
Encryptionratio	High	High	Moderate	High
Compatibility of Cloud	Yes	Yes(Generallynotused)	Yes	Yes
UseofAlgorithmincloud	Google Drive, Dropbox	Notusedin Cloud	NotusedinCloud	AmazonwebServices

V. CONCLUSION

In this paper detailed study of encryption algorithm such as AES, DES, 3DES and RSA. In order to provide the security to the different networks and data we use the various encryption algorithms. Here we can conclude the survey of the existing work on encryption techniques and summarize all the techniques for their different application. The comparison for the most efficient algorithm in terms of speed, throughput and efficient way to solve the problem of

security. The comparison of various parameters used in the encryption algorithm with list memory utilization and reduction in exhibition time.

VI. FUTURE ENHANCEMENT

Cloud computing accessible many new trends, like using software that are not current on your computer, achieving data from anywhere. One of the huge benefit of cloud computing is virtualization, although can use cloud computing accurately it grant reliable security. Cloud computing provides enough storage area to its customer, and provide security to data. There are various security algorithms, still security of these algorithms can be split any person. So it is very significant to make security of cloud more vigorous.

REFERENCES

[1] Keivan As'habi, Arman Vafabakhsh and Saeed Borji, "Data transmission security in cloud computing",ISSN:2231-6345(online), Vol. 6(SI), 2016, pp 37-45.

[2] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887), Volume 67– No.19, April 2013, pp 33-38.

[3] K. R.Monisha, "Secure cloud computing using AES and RSA algorithms", proceeding of 20 th IRF International Conference, ISBN: 978-93- 84209-01- 8,1 st March 2015, pp 12-17.

[4] Rachna Arora,Anshu Parashar, "Secure user data in cloud computing using Encrypption Algorithms", International Journal of Engineering research and applications(IJERA), ISSN:2248-96222, Vol. 3, Issue 4, July-Aug 2013, pp 1922-1926.

[5] M.Indhumathi,B.Salai Nalvetham, R.Venkatesh, "Multilevel Security on Cloud Computing With Cryptography Algorithm", International Journal of Modern Trends in Engineering and Research (IJMTER)Volume 03, Issue 02, ISSN (Online):2349–9745; ISSN (Print):2393-8161@IJMTER ,February – 2016, pp 565-573.

[6] Ms. Theres Bemila, Karan kundar, lokesh jain, Shashikant Sharma, Nayan Makasare, " Comparative study of various Security Algorithms applicable in Multi-Cloud Environmebt", International journal of Advanced Research in computer and communication engineering, vol. 5, issue 3, March 2016, pp 460-463.

[7] Uma Naik, V. C. Kotak, "Security Issues with Implementation of RSA and Proposed Dual Security Algorithm for Cloud Computing", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e- ISSN: 2278-2834, p-ISSN: 2278-8735.Volume 9, Issue 1, Ver. V (Feb. 2014), PP 43-47

[8] Divya saraswat, Dr. Pooja Tripathi, "Cloud Security and Algorithms: A Review", International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463, Vol. 3 Issue 10, Oct.- 2014, pp 113-117.

[9] Navrang Pal kaur, "Comparison between RSA and Triple DES in Cloud Environment", International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 1 Issue: 9, pp 740-742.

[10] Vijendra Rajendra Augustine, prof Prabhaker L. Ramteke, " Data storage security in cloud environment with Encryption and Cryptographic Techniques", International journal of Application or Innovation in engineering and management(IJAIEM), volume 3, Issue 3, March 2014, pp 209-213.

[11] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 6, Issue 3, March 2016, pp 659-665.

[12] Poonam M.Pardeshi, Deepali R. Borade, " Improving Data Integrity for data storage security in cloud computing, IJCSNS International journal of computer science and network security, Vol. 15 No. 7, july 2015, pp 61-67.

[13] Y. N. Patil, Mangesh D. Namewar, " Data security in cloud Environment using Cryptography Algorithm", American International journal of Research in science, Technology, Engineering and Mathematics, ISS(Print): 2328-3491, ISSN(online): 2328-3580, ISSN(CD-ROM): 2328-3629, 2014, pp215-218.

[14] Selvamani K and Velumadhava Rao R, "RSA and AES Based Secure Data Sharing in Cloud Based Environment", Int'l Journal of Computing, Communications & Instrumentation Engg. (IJCCIE) Vol. 4, Issue 1 (2017) ISSN 2349-1469 EISSN 2349-1477, pp 111-114.

[15] Zaid KARTIT, Mohamed EL MARRAKI, "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage", Advance online publication: 17 November 2015.