Analysis of EnDeCloudReports for Encrypting and Decrypting Data in Cloud

Shweta Singh
Ph.D. Scholar (CS)
IIS University, India

Amita Sharma, PhD
Asst.Professor (CS)
IIS University, India

ABSTRACT

In the midst of the last decades, information security has become an important issue. Encryption and decryption of data have recently been universally researched and developed as there is a need for a secure encryption and decryption which is very difficult to break. Cryptography offers main functions to meet these demands. Today, researchers have proposed several encryption and decryption algorithms such as AES, DES, RSA, and others. But most of the proposed algorithms encountered some problems such as lack of robustness and significant amount of time taken in encryption/decryption of data residing on server in cloud to maintain the security in cloud. In this paper, the cloud security enhanced by EnDeCloudReports simulator tool is analyzed on various parameters and attacks which in turn enhance the data security in Cloud by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.

Keywords

Encryption, Decryption, EnDeCloudReports, Cryptography Analysis, Algorithms

1. INTRODUCTION

EnDeCloudReports is a powerful simulator tool used to simulate cloud environment to protect the hardware resource utilization information in cloud. Various industrial control systems can also be secured from Malware attacks by implementing the security concept of EnDeCloudReports respectively. In the previous paper "A Simulation Tool for Security of Hardware Resource Utilization Information in Cloud Environment with EnDeCloudReports Tool" [1], the proposed algorithm implemented through simulator tool EnDeCloudReports for enhancing hardware resource information security in cloud environment was defined in detail. Thus, preventing system shutdown and datacenter damage/crash through malware injection by implementation of EnDecloudReports. In this paper, analysis of the proposed algorithm on various parameters is discussed with respect to existing cryptography algorithms.

In cryptography plaintext is basically encrypted in some illegible format. This practice is called encryption. The only person having knowledge about how to decipher the cipher text can get the original information. This process is called decryption. On the basis of the type of keys used, cryptographic algorithms are categorized as asymmetric key algorithms, in which encryption and decryption is done by two different keys and symmetric key algorithms, where the same key is used for encryption and decryption [8]. On the base of the input data, cipher algorithms are categorized as block ciphers, where the size of the block is of fixed length for encryption and stream ciphers where a continuous stream of data is passed for encryption and decryption [9].

A data file format symbolizes the standard for encrypting the information to be saved in system as a file. The file formats like textual, image, audio and video data file formats are encoded through cryptographic algorithms. Textual data formats are ANSII, UNICODE (16 & 32 bit little and big Endian and UTF-8). ANSII is encoding program for 128 characters primarily made for English alphabets. It includes alphabets a-z and AZ, numbers 0-9 and some special characters. In Unicode standard unique numbers are given for each character independent of platform. Data size is space occupied by a file on a disk. Audio, video files take more space on disk as compared to textual files as they hold multimedia information. Key size in cryptography algorithms represents the size of key in bits. For example AES is having key sizes 128, 192 and 256 bits. The main objective of this paper is to analyze and compare the time taken for encryption by various cryptographic algorithms in comparison to proposed algorithm used in EnDeCloudReports tool on the basis of various parameters like data type, data size, data density and key size.

2. PROPOSED ALGORITHM FOR ENDECLOUDREPORTS

The proposed algorithm used in EnDeCloudReports is an attempt to secure raw data files holding hardware resource utilization information of any cloud in an organization. The information in files is responsible for any malware attack on information leak and is secured through implementation of the proposed encryption algorithm.

2.1.Encryption

In the encryption process the plain text is first converted into ASCII value. The data in ASCII value is then passed through 10 rounds for first 10 words and then so on starting from round 0 to 9 where round id is substituted before and after every word. Last character is substituted as first character and first character as last character for every word in the file along with the respective round id for that word (round id 0 to 10). The converted text file is divided in to a number of packets(eg.100 packets) of fixed size where size and number of packets vary from organization to organization. Each packet passes through a method having method id where bits are changed according to a pattern as discussed in the research paper, "A Simulation Tool for Security of Hardware Resource Utilization Information in Cloud Environment with EnDeCloudReports Tool" [1] and shown in figure 1.

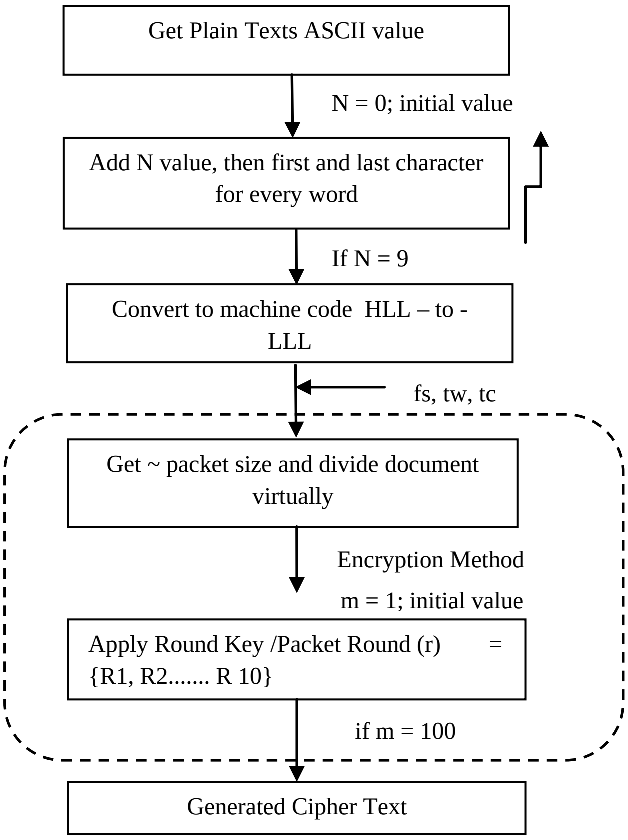
Get Plain Texts ASCII value
N = 0; initial value
Add N value, then first and last character for every word
If N = 9
Convert to machine code HLL – to - LLL
fs, tw, tc
Get ~ packet size and divide document virtually
Encryption Method
m = 1; initial value
Apply Round Key /Packet Round (r) = {R1, R2....... R 10}
if m = 100
Generated Cipher Text

Fig 1: Encryption of Plaintext

2.2. Decryption

In decryption the cipher text is decoded to obtain the original plaintext. The encryption process is just reversed to decrypt the cipher text. The decryption process starts from the state of arranging packets in form of queue where the encryption process ended. The proposed decryption algorithm consists of the following processes as shown in figure 2 .

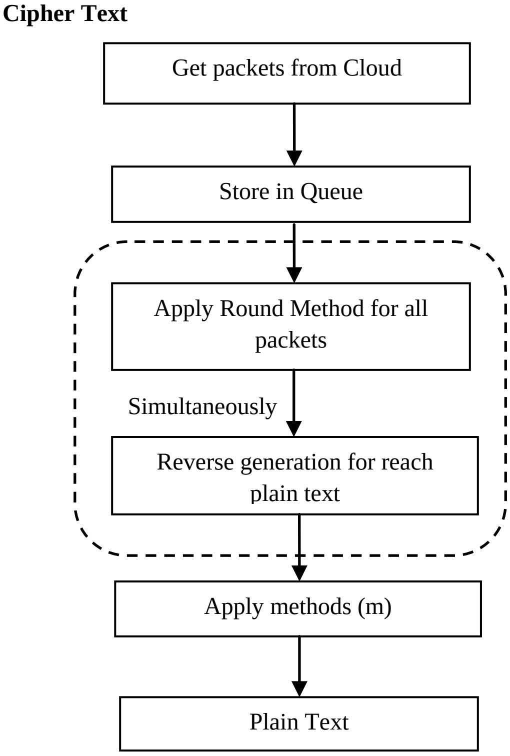

Fig 2: Decryption of Plaintext

3. PERFORMANCE ANALYSIS FOR ENCRYPTION AND DECRYPTION

In order to test the performance analysis for any encryption and decryption algorithms, the speed plays a important role [7, 9-10]. In this paper, the proposed algorithm for security of simulator tool EnDeCloudReports is compared with Rijndael algorithm in term of the speed in both encryption and decryption process because the National Institute of Standards and Technology (NIST) announced officially that Rijndael algorithm become the Advanced Encryption Standard (AES). Both algorithms are implemented in the same cloud environment and same conditions using *Java* language.

3.1.Speed Analysis for Encryption and Decryption

The speed of the proposed algorithm can be identified by calculating the time consumed for encryption and decryption of text file. This parameter is calculated for both the algorithms: AES results as shown in table 1, and 2[2][11] are calculated from C Language algorithm code. The proposed algorithm for enhancing the security of EnDeCloudReports is written in JAVA Language and results drawn are in milliseconds notation.

Table 1. Comparison of algorithms for 1024 bits plain text

	Proposed Algorithm(Java Lang)	**Standard AES (ms)(C Lang)**
Encryption Time	220	0.5500000
Decryption Time	218	0.5402866

Table 2. Comparison of Algorithms for 1 MB file

	Proposed Algorithm	**AES [11]**	**DES**	**RSA**	**BLOW FISH [11]**	**ANT + AES**
Key size (bits)	128	512	56	1024	512	128
Attacks	Brute Force	Brute Force	Meet in the middle attack	Wiener's attack	Brute Force	Denial of Service
Encryption time	235	230	16.9	30	200	35
Decryption time	230	250	14.38	102.9	350	94

3.2. Analysis of proposed algorithm with other evolutionary cryptography algorithms

The proposed algorithm is also compared with other evolutionary algorithms viz. neural cryptography, Genetic Algorithm and ant-crypto Algorithm on various parameters in table 3.

Table 3. Comparison of new evolutionary cryptography algorithms

	Proposed Algorithm	**Neural Network Algorithm**	**Genetic Algorithm**	**Ant-crypto Algorithm**
Attacks	DDoS	Brute Force	Denial of Service	Fault Injection
Block size	128	192	128	15
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Possible keys	2128	2192	2128	215
Key size	128	192	128	15

3.3. Comparison Analysis of simulator tools for Cloud

The various simulator tools available for simulating cloud environment viz iCanCloud, CloudSim/GenSim, Matlab are compared on certain parameters with the EnDeCloudReports simulator tool in table 4 as discussed [3].

Table 4. Comparison of Simulators for Cloud

	EnDeCloudReports	**iCanCloud**	**CloudSim/GenSim**	**Matlab**
Programming language	Java	C++ / java	Java	Simulink
networking	Full	Full	Limited	Limited
Simulator type	Packet based	Packet based	Event based	Event based

4. OBSERVATIONS AND DISCUSSIONS

This section briefly discusses the different observations drawn from the result and analysis tables. The table 1 shows the encryption time and decryption time taken by the proposed algorithm when implemented in JAVA eclipse environment. The results are drawn for encryption/decryption of text file of 1KB in size and compared with the standard AES algorithm encryption/decryption time. The proposed algorithm when compared with the standard AES algorithm on certain parameters viz encryption/decryption time, proved to be better with respect to time consumed.

The table 2 illustrates comparison of different cryptography algorithms for file size 1 MB. It was analyzed that the proposed algorithm protects the file against Brute Force attack. On comparison with other algorithms (AES and Blowfish) the proposed algorithm was found better as it protects file from Brute Force attack. It was also observed that proposed algorithm consumes same encryption time but takes less time in decryption. Thus, it was concluded that the proposed algorithm is better than AES and Blowfish algorithms. Other algorithms like DES, RSA and ANT+AES protect from different security attacks and take comparatively less time in encryption and decryption. But from literature survey following inferences can be stated [11-15]:

DES is less secured than AES. We have proposed an improved version for AES thus the proposed algorithm is much better.RSA is very computationally expensive in comparison with AES. It involves mathematics with very large numbers, whilst AES can be implemented with relatively simple bit operation .Thus proposed algorithm is cost effective and easy to implement.

*ANT+AES uses optimization techniques named ant colony optimization. It takes less time in encryption and decryption process but as the nature of ant it is quite difficult to analyze theoretically. If we discuss about convergence time in ANT, it is uncertain. Apart from this observation, implementation of such optimized algorithms is very complex. Thus proposed algorithm is simple to implement and takes reasonable execution time.

Thus, concluded from table 4 that EnDeCloudReports simulator tool is fully secure, efficient, flexible, easy to use from the networking requirement point of view when compared to other cloud simulator tools like iCanCloud, CloudSim/GenSim and Matlab[3]. The proposed algorithm is efficient enough to secure CloudReports simulator tool through encryption of rawdata.crd text file comprising hardware resource utilization information of the respective cloud environment.

5. CONCLUSION

This research paper introduces a new approach for complex encryption and decryption of industrial hardware utilization information kept on server in text form to overcome any malware attack. Though many researchers have worked on cryptography, but most of the existing cryptography algorithms face a number of weaknesses either because of low security level or increase in the delay time caused by the design of the algorithm itself. The proposed algorithm for enhancing the security of CloudReports have been analyzed on various parameters and tested against different known attacks and verified to be secure against them. Therefore, it can be considered as a good and secure algorithm to encrypt the hardware utilization information kept on server in text form which is responsible for any malware attack, thus enhancing the security of cloud environment and any industrial control system.

Cloud computing has become one of the rapidly developing branch in IT industry. Simulation based accession become famous in industry and academia to assess cloud computing systems, application and hardware machine behaviors, and their security. Various simulators have been particularly developed for performance analysis of cloud computing environments including CloudSim, GreenCloud, NetworkCloudSim, CloudAnalyst, EMUSIM and MDCSim [3] but the number of simulation environments for cloud computing data centers available for public use is limited. The EnDeCloudReports simulator based on cloudsim is probably the most refined and user friendly graphical user interface among the simulators overviewed. The EnDeCloudReports simulator is relatively a secure simulator enhancing the security of hardware utilization information kept on server thus preventing any malware attack in the cloud environment of any organization.

6. REFERENCES

[1] Shweta Singh, Amita Sharma, “A Simulation Tool for Security of Hardware Resource Utilization Information in Cloud Environment with EnDeCloudReports Tool”, International Journal of Computer Applications,vol.127-No.17,pp.12-19, October 2015.

[2] Obaida Mohammad Awad Al-Hazaimeh, “A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, pp. 95-103, March 2013.

[3] Dr. Rahul Malhotra* & Prince Jain, “Study and Comparison of CloudSim Simulators in the Cloud Computing” , The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 4,pp. 111-115, September-October 2013.

[4] Ragheb Toemeh and Subbanagounder Arumugam, “Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers” , The International Arab Journal of Information Technology, Vol. 5, No. 1,pp. 87-91, January 2008

[5] Ilker DALKIRAN, Kenan DANIS¸MAN, “Artificial neural network based chaotic generator for cryptology”, Turk J Elec Eng & Comp Sci, Vol.18, No.2,pp. 225-240, 2010.

[6] H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms". *International Journal of Computer Science Issues (IJCSI)*, Vol. 8, issue 4. 2011.

[7] S. Xenitellis, *The Open–Source PKI Book: A Guide to PKIs and Open-Source Implementations*, Open CA Team, 2000.

[8] W. Emm, “Impact of Multiencryption in Data Security”, *International Journal of Computer Theory and Engineering*, vol. 1, pp. 571-567 , 2009.

[9] B.D.C.N.Prasad, P E S N Krishna Prasad, “A Performance Study on AES algorithms”, International Journal of Computer Science and Information Security, Vol. 8, Issue. 6,September 2010,pp 128-132.

[10] M. Anand Kumar and S.Kartikeyan, “A New 512 Bit Cipher For Secure Communication” ,I.J. Computer Network and Information Security, Vol. No.11 ,pp. 55-61, October 2012.

[11] Omer K. Jasim, Safia Abbas, “Efficiency of Modern Encryption Algorithms in Cloud Computing”, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol.2, Issue 6, pp. 270-274, November-December 2013.

[12] Randeep Kaur, Supriya Kinger, “Analysis of Security Algorithms in Cloud Computing”, International Journal of Application or Innovation in Engineering &

Management (IJAIEM), Vol 3, Issue 3, pp. 171 – 177, March 2014.

[13] Dr. Prerna Mahajan & Abhishek Sachdeva, " A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol 13, Issue 15, Version 1.0, pp. 15 -22, Year 2013.

[14] Salabat Khan, Armughan Ali and Mehr Yahya Durrani, "Ant-Crypto, a Cryptographer for DES", International journal of Computer Science Issues, Vol 10, Issue 1, No 1, January 2013.

[15] Santosh Deshpande, "Symmetric Key Management : A new approach", International Journal of Enginnering and Computer Science (IJECS), Vol 1, Issue 3, pp.125-136, Dec 2012.