Data Security in Cloud System

Aishwarya Rajendran.
Department of Computer, Indira College of Engineering and Management, Pune, India.
aishwarya.rajendran2012@gmail.com

Renuka Ramesh Teli
Department of Computer, Indira College of Engineering and Management, Pune, India.
renukateli60@gmail.com

Potdar Parag Kishor
Department of Computer, Indira College of Engineering and Management, Pune, India.
paragpotdar55@gmail.com

***Abstract*--**Cloud stores the major data around the universe and is one of the most developing technologies today. To protect the data stored on such cloud is one major challenge faced now days. To overcome these data security challenges, an efficient data encryption to encrypt sensitive data before sending to the cloud server has been proposed. This addresses the block level data encryption using symmetric key with rotation. Besides, data users can re-construct the requested data from cloud server using shared secret key. The analysis of the privacy protection of outsourced data using experiment is carried out on the repository for all kinds of files with variable size. The security and performance analysis shows that the proposed method is highly efficient than existing methods performance.

Keywords-*Data Block, Security, Encryption, Decryption, Cloud Server.*

****

I. INTRODUCTION

The advancement of internet has drastically increased in the 21th century. Communication application, electronic mail or the World Wide Web are more popularly used but these are not completely secure for sending and receiving information. Information sent by these means may contain volatile or sensitive personal data which can be intercepted. Therefore encryption of data in the modern technology becomes necessary to ensure that data sent should be read and understood by people for whom the information is intended.

Data security is the major concern in the field of computer science and information technology. Particularly in the cloud computing as the data is stored all over the wold at different places. Data security and privacy protection are the two major concern of users in cloud technology. Though many techniques and topics are implemented on both academics and industries, data security and privacy protection are becoming more important for future cloud development.

Data security issues are relevant to both hardware and software in cloud architecture. Services of cloudcomputing are provided across entire computing spectrum. A number of data protection and data security techniques are proposed in the research field of cloud computing.

II. EXISTING ENCRYPTION ALGORITHM-

*A.*DES-The DES block cipher is a 16-round Feistel network with a block length of 64 bits and a key length of 56 bits. The same round function (*F*) is used in each of the 16 rounds. The key schedule of DES is used to derive a sequence of 48-bit sub-keys *k1, . . . , k16* from the 56-bit master key. Each sub-key (*ki)* is being a permuted subset of 48 bits of the master key.

1. *Plaintext encryption process*

The original 64-bit plain text is converted with the initial permutation (IP), encrypts in 16 rounds, followed by the inverse of the initial permutation (IP-1). In each round, the right-side 32 bits of the block are transformed with the function labeled (*f*) and a sub-key, then exclusive-OR (XOR) with the left side 32 bits. After each round, the two sides of the data block are swapped and the algorithm continues.

2. Key generation

For each DES round, a sub-key of 48 bits has to be generated. The input key is also 64 bit, but 8 bits are used for parity checking. After an initial key permutation (CP-1) the 16 sub-keys, one for each round, are derived from the 56-bit key selected for encryption. One sub-key is obtained after left shifting, and after a 56 to 48 bit permutation, (CP-2).

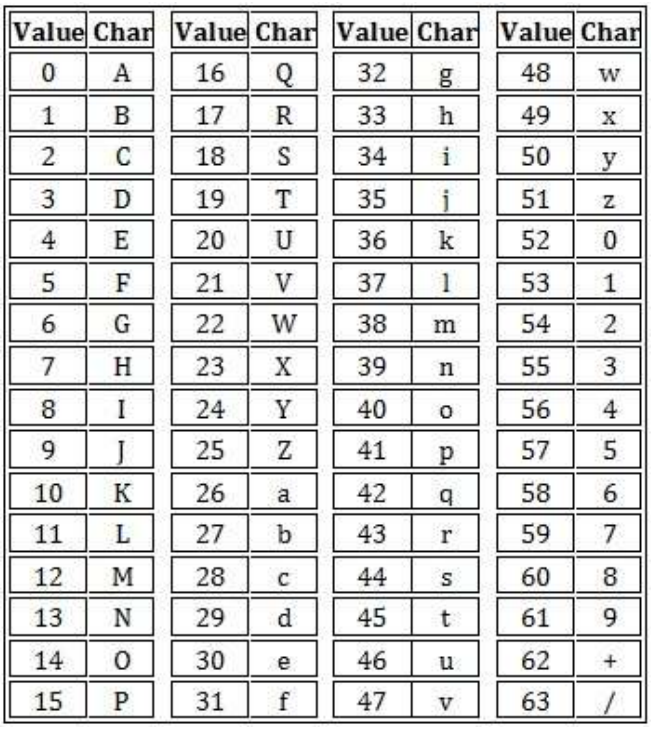
B. Base64 Algorithm- Base64 Encoding is mainly used when there is necessity to encode binary data as ASCII text that needs to be stored or transferred in environments that, perhaps for legacy reasons, are restricted to US-ASCII data. Base64 is commonly used for sending e-mail via MIME (Multipurpose Internet Mail Extensions) however the mainpurpose is not to send secure email but to achieve the effect of fail to understand the contents directly. Base 64

ISSN: 2321-8169
115 – 118

data representation is based on a 64-character alphabet. The alphabet is shown in Table 1.

Value	**Characters**
0…25	‘A’…‘Z’
26…51	‘a’…‘z’
52…61	‘0’…’9’
62	‘+’
63	‘/’
Padding	‘=’

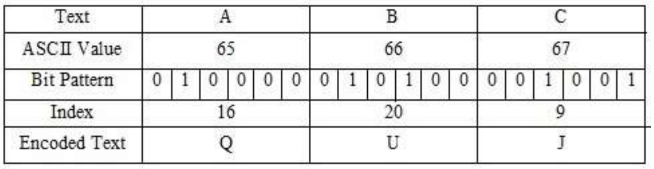
Table 1. Base64 Alphabet.



Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Table 2: Base64 Character Set.

In computer systems, a byte is a unit of data that is composed of eight bits. Base64 algorithm takes three bytes, each consisting of eight bits, and converts them into four bytes composed of six bits each. According to the value of each byte (after converting into four bytes), obtain the character from Table 1 based on the value. The padding character “=” is also used at the end of encoded text if the total number of bits (or number of characters in the plaintext) are not multiple of 3. If the total number of bits in text are 3n+1, the encoder puts one “=” at the end of encoded text, and if the total number of bits in text are 3n+2, it puts two “=” at the end of output.



Text	A						B						C					
ASCII Value	65						66						67					
Bit Pattern	0	1	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1
Index	16						20						9					
Encoded Text	Q						U						J					

Fig.1 Base64 Encoding.

Every encryption technique has its own strong and weak points. In order to apply a suitable technique we must know its strength and weakness. Therefore the analysis of the techniques are very necessary.

III. PROPOSED ENCRYPTION ALGORITHM

Step 1: The Digital file which is uploaded is converted into text format i.e. the binary numbers are converted into string format.

Step 2: The string format obtained by the Base64 encoding is implemented with DES algorithm. Here the DES double encrypts the file.

Step 3: The file obtained is again triple encrypted with the help of Base64 algorithm and is stored on the cloud system.

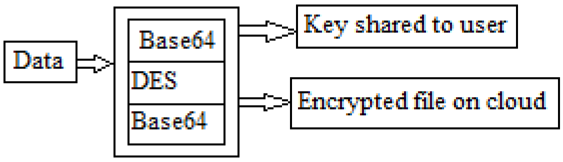


Fig 2. System Architecture.

Step 4: A secret key is generated in order to open the encrypted file that is stored on the cloud.

Step 5: The secret key is shared to the user via email. This key will be used to decrypt the encrypted file.

Step 6: The file selected will be decrypted in the original form using the key.

IV. SYSTEM MODEL

1. The binary format of the file is split into 4 bytes of blocks.
2. It is then combined to full 32 bit stream.
3. This stream is then converted to 6 bit values.
4. If padding is requires then zeroes are added to the binary stream.
5. These 6 bit binary values are converted into decimal values.
6. This values are then converted into Base64 characters.

V. OBJECTIVES

Data Security for outsourcing and accessing data from cloud servers, our proposed security model achieve the following objectives.

1. Lightweight and easy to use architecture for verification of authorised cloud user and access the cloud data.
2. Design binary level data encryption of the file.
3. Design an efficient data encryption before outsourcing to cloud and decryption at the user side.

VI. EXPERIMENTAL RESULTS

The experiments are carried out on a repository of text files, audio files and video files of different size. For testing purpose the binary format of the file is extracted which is then encoded by mapping values. The algorithm is implemented in JAVA. The NetBeans IDE and Windows OS forms the complete execution environment.

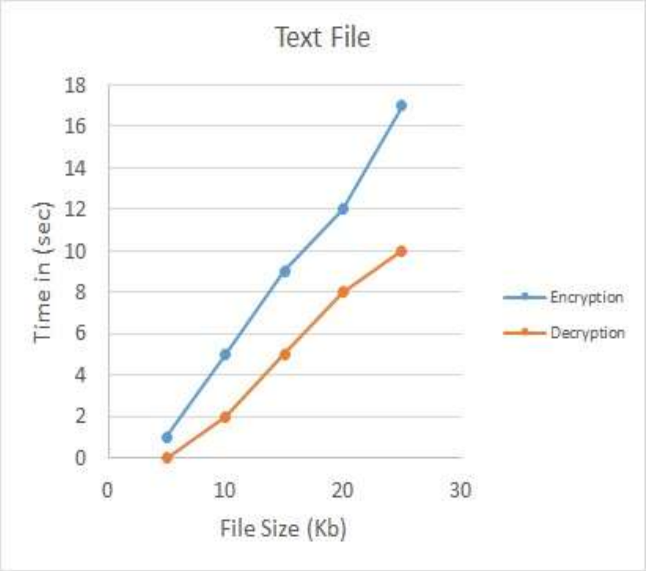


Fig 3: Data Encryption and Decryption time comparison for Text file.

From Fig 3. Time taken for encryption of the text file is less than compared to the other files as the size of the file is less. The decryption time required is comparatively less than its encryption.

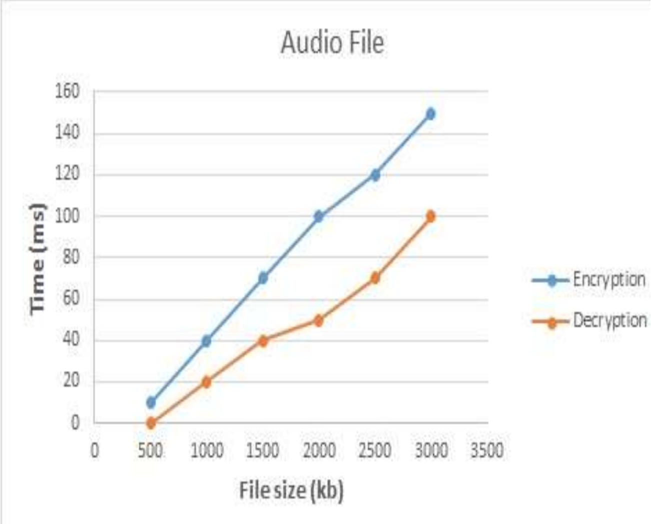


Fig 4: Data Encryption and Decryption time comparison for Audio file.

From Fig 4. Time taken for encryption of the Audio file is more than compared to the other files as the size of the file is in Mb's. The decryption time required is comparatively less than its encryption.

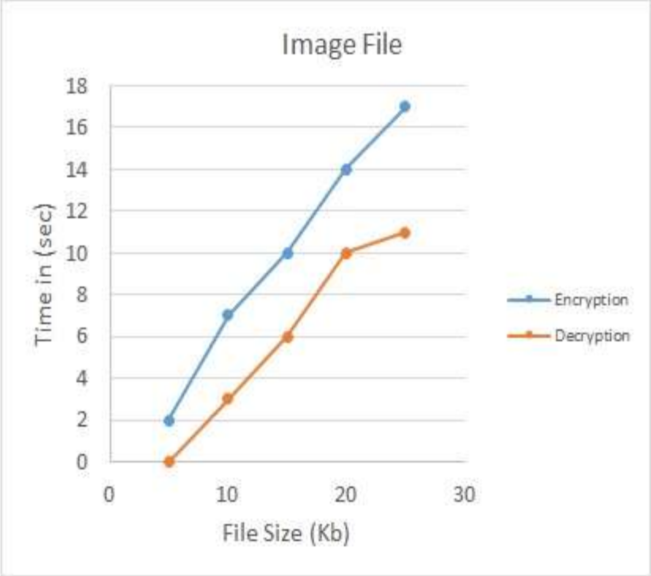


Fig 5: Data Encryption and Decryption time comparison for Text file.

From Fig 5. Time taken for encryption of the text file is less than compared to the other files as the size of the file is less. The decryption time required is comparatively less than its encryption.

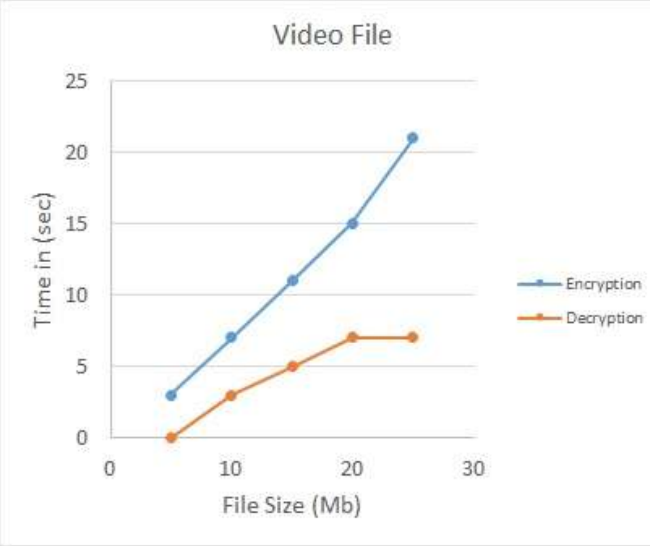


Fig 6: Data Encryption and Decryption time comparison for Audio file.

From Fig 6. Time taken for encryption of the Audio file is more than compared to the other files as the size of the file is in Mb's. The decryption time required is comparatively less than its encryption.

The overall time complexity of the process depends upon the size of the file. Smaller file size are processed early while the greater file size requires more time to encrypt and decrypt.

VII. CONCLUSION AND FUTURE SCOPE

Encryption is not a new technology.Previously encrypted data was stored on server which was located in a place where the company had direct control.Today many popular business applications hosted in cloud need to depend on contract language to protect their valuable data,selecting a cloud provider that will allow the customerto encrypt data before it is stored on cloud with software as a service(Saas) that will manage the encryption and decryption of the corporate data.In cloud computing,wehave proposed an efficient data encryption and decryption algorithm to protect the sensitive data in cloud environment. Also to reduce the burden,a trusted third party is invented for verification of authorised user to access the data on cloud. On the other hand,we also demonstrate for bit leveloperations on data for insertion,deletion and updation of data which we consider as an improvement for our future work.

REFERENCE

[1] Prakash G L, Dr. Manish Pratik, Dr. Inder Singh, Data Encryption and DecryptionAlgorithm using key Rotation for Data Security in Cloud System. University of Petroleum and Energy Studies, Dehradun.

[2] Jing-Jang Hwang, Taoyuan, Taiwan,Yi-Chang Hsu, ChienHsing Wu, ABusiness Model for Cloud Computing Based on a Separate Encryption and Decryption Service, in International Conference on Information Science and Applications(ICISA), pages 1-7,2011.

[3] Jing-Jang Hwang, Kun-Kai Chang, Securing the Cloud: Cloud ComputingSecurity Techniques and Tactics, Elsevier Inc., USA, 2011.

[4] Fatemi Moghaddam F,Karimi O,Alrashdan M T, A Comparative Studyof Applying Real-Time Encryption in Cloud Computing Environments, in IEEE 2nd International Conference on Cloud Networking, pages 185-189, 2013.

[5] Lan Zhou, Varadharajan V, Hitchens M, Integrating Trust with CryptographicRole-Based Access Control for Secure Cloud Data Storage Trust, in 12thIEEE International Conference on Security and Privacy in Computing and Communications(Trust Com), pages 560-569, 2013.

[6] Shaify Kansal, Minaksha Mittal, Performance Evaluation of various SymmetricEncryption Algorithm, Central University of Punjab, Batinda India.

[7] Naik Riddhi, Nikunj Gamit,An Efficient Algorithm for Dynamic Key Generationfor Image Encryption,Uka Tarsadia University,Bardoli,Surat,Gujrat.

[8] N.Jayapandian,Dr.A.M.J.Md.Zubair Rahman,S.Radhika Devi,M.Koushikaa,EnhancedCloud Security to Confirm Data Security on Asymmetric and Symmetric Key Encryption,Knowledge Institute of Technology,Salem,Tamil Nadu.

[9] http://aspe.hhs.gov/admnsimp/pIl0419I.html
104th United States Congress, Health Insurance Portability and Accountability Act of 1996.

[10] Tim Mather, Subra Kumaraswamy, and Shahed Latif, Cloud Securityand Privacy, Published by 0 Reilly Media, Inc., 2009.

[11] http://security.setecs.com, Security Architecture for Cloud ComputingEnvironments, White paper, 20 II .

[12] Junzuo Lai, Deng R H, Chaowen Guan, Jian Weng, Attribute-BasedEncryption With Verifiable Outsourced Decryption, in IEEE Transactions on Information Forensics and Security, vol. 8(8), pages 1343-1354, 2013.

[13] Qin Liu, Tan CC, Jie Wu, Guojun Wang, Reliable ReEncryption inUnreliable Clouds, in IEEE International Conference on Global Telecommunications(GLOBECOM), pages 1-5,20 II.

[14] Miwen, Rongxinglu, Kuanz hang, Jing Shenglei, Xiaohuiliang andXueminshen, PaRQ:A Privacy-Preserving Range Query Scheme Over EncryptedMetering Data for Smart Grid, in IEEE International Journal of Computer Networks,pages 178-191,2013.