ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Securing Cloud Data with Rijndael Encryption Algorithm

[1] Saurabh Hanwante, [2] Shivani Kitey, [3] Ankita Padole, [4]Roshni Khodke
[2] Assistant Professor
[1][2] Information Technology, Rashtrasant Tukdoji Maharaj Nagpur, University,Nagpur, Wardha,Maharashtra,India

Abstract **– As per recent time cloud data had gone through many new issues regarding securities as cloud is becoming one of the recent requirement in many sectors like Finance, Stock Market, Industrial Sectors and so on. As per demand of cloud services are increasing, issues regarding its security which is necessary. This paper focus on providing a encryption technique known as Rijndael algorithm. Also we have use a compression technique, which is also a key issue regarding cloud storage and management, this technique is generally known as Open-SSL. This system will provide a user interface for user by which he/she can upload the file to the cloud. This system will first provide compression and then will proceed to further encryption after which the file be securely stored in cloud. Then this file will only be access by authorized Personnel.**

Keywords- Cloud Security, Security Issues, Hybrid secure storage cloud, Rijndael, OpenSSL, Base64 and SHA-256 Algorithm.

I. INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow personal level and businesses to use software and hardware that are managed by third parties at locations not local. Examples of cloud services include online file storage, social networking sites, web e-mail, and business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is provided. Cloud computing provides a shared cards of resources, including data storage space, computer processing power, networks ,and specialized corporate and user applications .Security goals of data include three points namely: Availability secreacy, and Integrity. security of data in the cloud is accomplished by cryptography/Encryption [1].

Cloud computing is a "new" computer model that allows remote services through a network which uses various resources. It is basicallyhas to meant to provide the maximum capacity with the minimum resources. The end user has the minimum hardware requirement, but he uses the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. Cloud Computing provides IT services as on demand services, accessible from anywhere, anytime and by authorized user only [2].

There are two ways to attack data stored in the Cloud. One is outsider attack and the another one is the insider attack. The insider is an administrator who is one can have the possibility to hack the user‟s data in the cloud. The insider attack is a very difficult task to identify. So the users should be very careful during storing their data in cloud storage. Hence, there is a need to think of methods which impede use of the data even though the data is accessed by the other third party. He should not get the actual data which he wanted. So all the data must be encrypted before it is to be transmitted to cloud storage [3].

II. RELATED WORK

A. Rijndael Encryption Algorithm:

Rijndael as the standard symmetric key encryption algorithm which to be used to encrypt the sensitive information. Rijndael is one of the iterated block cipher. The encryption or decryption of a block of data is accomplished by the iteration of a specific transformation i.e. a round function. As a input to the Rijndael accepts one-dimensional 8-bit byte array that creates data blocks.

The plain text is a input and then mapped on to the state bytes. The cipher key which is also a one-dimensional 8-bit byte array that creates data block. With an iterated block cipher the different transformations operate sequencially on intermediate cipher results i.e.states[4].

```
Rijndael(State, CipherKey)

{


KeyExpansion(CipherKey,ExpandedKey);


AddRoundKey(State,ExpandedKey);


For( i=1; iFinalRound(State,ExpandedKey + Nb*Nr); }
```

And the round function is defined as:

```
Round(State, RoundKey)


{

ByteSub(State);


ShiftRow(State);


MixColumn(State);


AddRoundKey(State,RoundKey);

}
```

The User Details are encrypted by using the Rijndael Encryption. Symmetric key is used for the encryption. The Rijndael can be implemented easily and it is one of the most secure algorithms throughout the world. The Rijndael implementation has the 128,192 or 256 bit key lengths. The size of the data blocks to be encrypted with the Rijndael is always 128 bits respectively. The initial round of the Rijndael is AddRoundKey which is followed by four iterative round including the subBytes, shiftRows, mixColumns and the add round key. Rijndael with 128 bit key length has 10 rounds, 192-bit has 12 rounds and 256 bit which has 14 rounds. The AES algorithm is a symmetric block cipher that can be encrypt i.e. encipher and decrypt i.e. decipher information. The encryption converts data to an unintelligible form called the cipher text; decrypting the cipher text converts the data back into its original form which is called the plain text.

Each round consists of following steps which are as follows:-

1. Initial AddRoundKey
2. SubBytes () Transformation
3. Substitutional Box Created For Subbytes
4. MixColumns () Transformation
5. AddRoundKey () transformation

The Inverse process of the Encryption gives Decryption text[5].

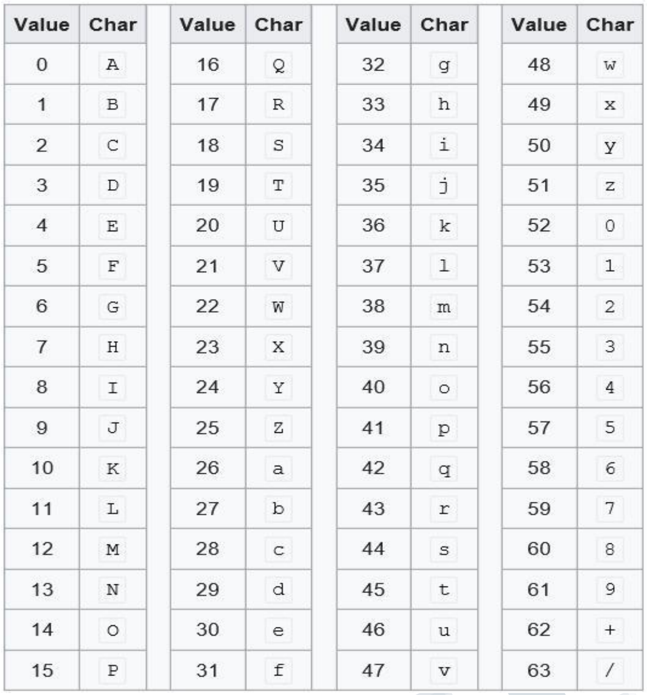
III. PROPOSED WORK

A. OpenSSL

OpenSSL is an open source tool for using the Secure Socket Layer and Transport Layer Security protocols for Web authentication. It offers cryptographic functions to support SSL/TLS protocols. In Secure Socket Layer security, websites use digital certificates to prove their legitimacy. OpenSSL is written in the C programming language and relies on different ciphers and algorithms to provide encryption. The product is under Apache license and Berkeley Software Distribution license. Many versions of OpenSSL have been developed since 1998, when the product was first established. The set of OpenSSL versions including 1.0.1 through 1.0.1f involves a dramatic security flaw discovered in 2014. The vulnerability relates to feature called TLS heartbeat extension, where a bug can release up to 64 kB memory. The vulnerability have been termed as 'Heart bleed bug‟ ,which has been estimated to affect at least half million secure web servers on Internet. A current version of OpenSSL is 1.0.1G and it has been modified to fix the Heart bleed bug[6].

B. Base64

Particular set of the 64 characters which is chosen to represent all the 64 place values for the base which always varies between the implementations. The general strategy is to choose the 64 characters that are both member of subset common to almost all the encoding and printable. This combination leaves data unlikely to be modified in transit through the information system which email that were traditionally not 8-bit clean. Example is MIME's Base64 implementation which uses A–Z, a–z, and 0–9 for the first 62 values and other variations share the property but differ between symbols chosen for the last two values .The example is UTF-7.



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	/

Fig 1 Base64 index table

When the number of bytes to encode is not divisible by odd number,(that is, if there are only one or two bytes of input for the last 24-bit block), add extra bytes with value 0 so it is three bytes, and perform the conversion to base-64. If there is only one significant input byte as „M‟, all 8 bits will be captured in the first two BASE-64 digits (2 times of 6 bits)[7].

C. SHA 256

The SHA-256 which is 256 bit is a part of SHA-2 set of cryptographic hash functions, designed and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS). A hash function is an algorithm that transforms data element which is also known as (hashes) an arbitrary set of data elements, such as a text file, into a single fixed length value (the hash). The computed hash value may then be used to verify the integrity of copies of the original data without providing any way to originate known as original data. Infact it is irreversive in nature, a hash value may be freely distributed, stored and used for comparative purpose. SHA stands for Secure Hash Algorithm. SHA-2 consists of a significant number of differences from its predecessor[8].

IV. CONCLUSION

Nowadays as cloud data is still vulnerable in the concept where issues of securities arrives , therefore this system will effectively overcome the need of securities issues with advance encryption techniques and advance cloud data compression techniques. After implementing all this algorithms to this cloud storage, the data stored on data will be more secured. Any file or data on cloud will be encrypted first and get compressed which will be unreadable or unrecognizable. Duable to noted date any unauthorized person cannot be able to access the data even if he hacked the data. This concept will reduce the security issues regarding cloud computing and its component.

REFERENCES

[1] Shakeeba S. Khan1, Prof.R.R. Tuteja2 ," Security in Cloud Computing using Cryptographic Algorithms " IJIRCCE(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January 2015.

[2] Zaid KARTIT, Mohamed EL MARRAKI,"Applying Encryption Algorithm to Enhance Data Security in Cloud Storage ",Engineering Letters, 23:4, EL_23_4_06(Advance online publication: 17 November 2015).

[3] L. Arockiam, S. Monikandan « Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm » International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[4] Prashant Rewagad, Yogita Pawar, "Use of Digital Signature and Rijndael encryption Algorithm to Enhanced Security of data in Cloud computing Services", Proceeding published in International Journal of Computer Applications (IJCA), 2012.

[5] G.Jai Arul Jose, C.Sajeev, “Implementation of Data Security in Cloud Computing”, International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011.

[6] [Online]Available:https://www.techopedia.com/definition/30174/openssl

[7] [Online]Available:https://en.wikipedia.org/wiki/Base64#cite_note-autogenerated2006-1

[8] [Online]Available:https://md5hashing.net/hash/sha256