ISSN 2286-4822
www.euacademic.org

EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 4/ July 2015

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

Data Security in Cloud Computing

SIKANDER SHAHZAD
MS (Computer Science)
Department of Computer Science and Information Technology
University of Balochistan, Quetta
Pakistan

Abstract:

Cloud computing is rapidly growing technology of computing which offers services to its users on demand over the internet. It involves data and computation outsourcing with infinite and elastic resource scalability on no upfront cost. Despite having numerous economical advantages, cloud computing is still subject to many issues. Security concern is one of the main issues which does not allow people to use cloud. This paper presents different solutions available to ensure security of data in cloud.

Key words: cloud computing, internet, data and computation outsourcing, security.

I. Introduction

Cloud computing is a new style of computing in which computer resources such as computes, storage, network, and applications can be obtained on lease over the internet. When the data are stored and programs are run from the hard drive, it is called local storage and computing. Everything needed is physically close to us and accessing data is fast and easy for the user on the local network. Whereas in cloud computing there is no need of having a dedicated hardware server in residence, data and programs are accessed over the internet.

II. Deployment Model

There are several different deployment models for implementing cloud technology as illustrated below:

A. Public Cloud

In public cloud, computer resources are obtainable for gen-eral use over the internet. Public cloud services may be offered on a pay-per-usage mode or other purchasing models.[4]

B. Private Cloud

In private cloud, computer resources are offered to a sin-gle organization that provides control and privacy to the organization.[4]

C. Hybrid Cloud

A hybrid cloud is a combination of public and private clouds. These are used by those organizations who want to use the cost benefit of public cloud but want their data to be protected.[4]

III. Service Model

There are three basic service models on which cloud com-puting is based on.

A. Infrastructure as a service (IaaS)

IaaS provides access to resources such as physical machines, virtual machines, virtual storage, network etc. Currently, Amazon Elastic Computue Cloud(EC2) is the most popular web service that provides complete control of computing resources.[8][6]

B. Platform as a service (PaaS)

PaaS provides environment and access for the development of applications. Google App engine, force.com, AppJet are some of the examples of PaaS.[8][6]

C. Software as a service (SaaS)

SaaS provides software applications to the user through browser for services. CRM, salesforce.com. Google App, window Azure, Oracle On demand are the good examples of Saas.[8][6]

IV. Issues in Cloud

Cloud computing offers the tenant to obtain infinite and elastic resource scalability, On demand provisioning of re-sources any time from anywhere, no commitment of buying hardware and no upfront cost just like utility bills, pay-as-you-use. Despite having so many economic advantages, a question arises here that if cloud computing is such a great thing, why everyone is then not doing it. The answer is because clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks.

A. Confidentiality

Cloud user fears that would sensitive data stored in cloud remain confidential and what is the guarantee that cloud service provider itself will not leak the confidentiality.

B. Integrity

Cloud user fears that how he will know that correct computations are being done on his data and what is the surety that cloud provider has saved his data without tampering. In this regard, cloud service providers should implement mechanisms to be able to tell what happened to his data and at what point.[16]

C. Availability

Tenant data is stored in large pieces on different servers in different locations or even in different clouds. In this regard, cloud user fears that what will happen if cloud provider is attacked and goes out of business.

D. Privacy Issues

As a lot of clients store their data in cloud and data mining algorithms can be run to get large amount of information on clients therefore, cloud user fears of violation of privacy and needs guarantee that access to his sensitive data will only be limited to him.

E. Additional Attacks

Now a user outside the organization can store and compute his data so the communication link between cloud service provider and a cloud user can be targeted even man in the middle (MITM)[2] can phish the cloud provider.

V. Data Security in Cloud

IDC (International Data Corporation) conducted a survey of 244 IT executives/CIOs and their line-of-business (LOB) colleagues about their companies use of, and views about, IT Cloud Services. In part 1, they looked at current and future adoption of IT cloud services and in part 2, looked at users perceptions of the key benefits and challenges of IT cloud services.[1]. According to the survey security issue related to IT cloud ranked topped. Figure 1 illustrates the benefits and issues related to cloud.

[1] http://blogs.idc.com/ie/?p=210#comments

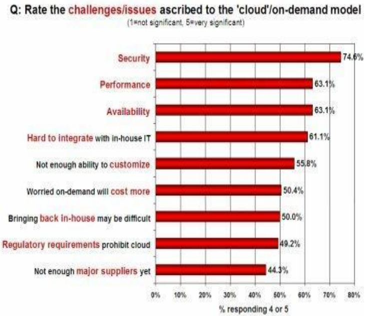


Fig. 1. Survey on benefits and challenges of IT Cloud Services

VI. Methods for Securing Data in Cloud

There are several methods available to secure data which can be classified in following categories:

A. Classical Encryption

There are several classical encryption algorithms such as (Caesar Cipher, Vigenere Cipher, and Play fair Cipher).

1) Caesar Cipher: It is the oldest and the simplest substitution cipher in which an alphabet is replaced with an alphabet that is 3 positions ahead[17]. For example CLOUD will be ciphered into FORYG.

Encryption in Caesar Cipher[2]

In Caesar cipher text can be encrypted as:

$$E_n(x) = (x + n) \bmod 26$$

Decryption in Caesar Cipher[3]

In Caesar cipher text can be decrypted as:

$$D_n(x) = (x - n) \bmod 26$$

2) Vigenere Cipher: It is the simple form of polyalphabetic substitution in which text is encrypted by using a series of different Caesar ciphers.[17]

[2] http://en.wikipedia.org/wiki/Caesar cipher

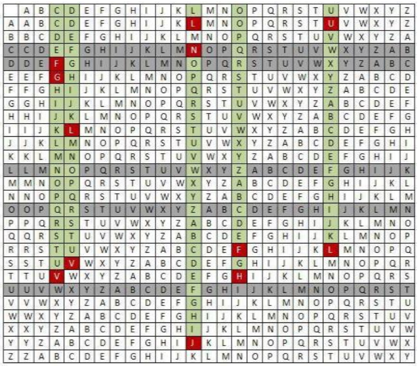
[3] http://en.wikipedia.org/wiki/Caesar cipher

Encryption in vigenere cipher

Message	data Security
keyword	cloud

After repeating keyword against the message

keyword	C L O U D C L O U D C L
Message	D A T A S E C U R I T Y



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 2. Vigener cipher table

After going through vigenere cipher table.

keyword	C L O U D C L O U D C L
Message	D A T A S E C U R I T Y
Ciphered	F L H U V G N F R L V J

3) Play Fair Cipher: The Play fair cipher uses a square matrix of 5 by 5 containing a key word that can be selected and placed in the matrix. The remaining alphabets are then placed one by one in the matrix of 5x5.[17] [13] [18]

- Choosing keyword in play fair cipher

  While choosing a keyword, there must be no repeating of letters. Here i have chosen "CLOUD" as there is no alphabet which is being repeated.

- Creating 5 x 5 matix

  1) Remove letter J.
  2) Insert the chosen keyword "CLOUD" in matrix.
  3) Insert remaining alphabets after keyword.

TABLE I
PLAY FAIR CIPHER 5 X 5 MATRIX

C	L	O	U	D
A	B	E	F	G
H	I	K	M	N
P	Q	R	S	T
V	W	X	Y	Z

- Message Generation

1) A message to send must be divided into pairs.

2) Insert letter X to separate the duplicate letters.

3) If there is single letter left while dividing message into pairs then insert X at the end to complete a pair.

4) Ignore all spaces.

Message	DATA SECURITY
Pair	DATA SECURITY

- **Encryption in play fair cipher**

1) Take each pair one by one and check their positions (same column, same row or forms rectangle).

2) If both letters in same column, move each letter down to one position, upon reaching end of table wrap around.

3) If both letters in same row, move each letter right to one position, upon reaching end of table wrap around.

4) If both letters form a rectangle, swap the letter with the letter end of the rectangle.

After applying above rules:

Original text	DATA SECURITY
Encrypted text	CGPG RFLDGKSZ

- **Decryption in play fair cipher**

The way in which encryption is done using play fair cipher, the reverse process is done to decrypt text.

The above classical encryption methods (caesar cipher, vi-genere cipher, and play fair cipher) operate on an alphabet of letters and are implemented by hand or with simple mechanical devices but these have fallen now and are not used now a days because in today's age of computers and technologies, they can be easily broken.

B. Symmetric Methods

In symmetric methods, the same cryptographic key is used for both encryption of plaintext and decryption of ciphertext such as (S-DES,DES,RC6 and AES)

1) S-DES (Simplified Data Encryption Standard): The S-DES algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of cipher text as output. The S-DES decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used to produce that cipher text as input and produces the original 8-bit block of plaintext.[17]

2) DES (Data Encryption Standard): DES algorithm increases the size of key from 10-bit of S-DES to 64 bits out of which 56 bits is used, however a 64 bits key is actually input. The least signicant bit of each byte is either used for parity or set arbitrarily. Plain-text message received to be encrypted is arranged into 64 bit blocks required for input. Multiple permutations and substitutions are integrated right through in order to increase the difculty of performing a cryptanalysis on the cipher. As in DES only one private key is used for encryption and decryption so if the key is lost to decrypt the data then the readable data would not be got readable at the receiving end. The 56-bit key size is the biggest fault of DES as the technology is improving lot more day by day so there is a possibility to break the encrypted code.[11], [17]

3) RC6 (Rivest Cipher 6): RC6 is a block cipher algorithm having a block size of 128 bits and supporting key sizes of 128, 192, and 256 bits. RC6 is like RC5 in structure, using data-dependent rotations, modular addition, and XOR operations. [15]

- **Encryption in RC6**[4]

```
$B = B + S[0]$
$D = D + S[1]$ for $i = 1$ to $r$ do
{
    $t = (B * (2B + 1)) <<< \lg w$
    $u = (D * (2D + 1)) <<< \lg w$
    $A = ((A \oplus t) <<< u) + S[2i]$
    $C = ((C \oplus u) <<< t) + S[2i + 1]$
    $(A, B, C, D) = (B, C, D, A)$
}

$A = A + S[2r + 2]$
$C = C + S[2r + 3]$
```

- **Decryption in RC6**[5]

```
$C = C - S[2r + 3]$
$A = A - S[2r + 2]$

for $i = r$ down to 1 do

{

    $(A, B, C, D) = (D, A, B, C)$
    $u = (D * (2D + 1)) <<< \lg w$
    $t = (B * (2B + 1)) <<< \lg w$
    $C = ((C - S[2i + 1]) >>> t) \oplus u$
    $A = ((A - S[2i]) >>> u) \oplus t$
}
$D = D - S[1]$
$B = B - S[0]$
```

4) AES (Advanced Encryption Standard): Rijendeal is one of the most secure algorithms that has 128,192 or 256 bit key lenghts. Rijendeal with 128 bit key length has 10 rounds, 192 bit has 12 rounds and 256 bit length has 14 rounds. [10][12]Each round consists of the following steps.

1) Initial AddRoundKey
2) AddRoundKey
3) SubBytes() Transformation
4) Substituional Box
5) Mix Columns() Transformation

[4] http://en.wikipedia.org/wiki/RC6#Encryption.2FDecryption

[5] http://en.wikipedia.org/wiki/RC6#Encryption.2FDecryption

6) AddRoundKey()Transformation

- **AES encryption process**

The encryption process of AES is shown in figure 3.

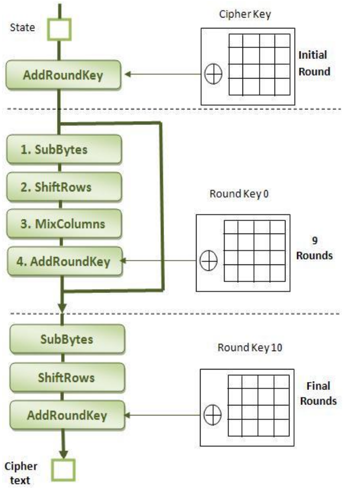


Fig. 3. AES Encryption Process

AES-encrypted data is secured in the sense that no known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all possible 256-bit keys.[2]

C. Asymmetric Method

In asymmetric methods, two separate keys (public and secret) are used for encryption of plaintext and decryption of ciphertext such as RSA algorithm.

1) RSA: RSA (Ron Rivest, Adi Shamir and Len Adleman) is wiely used public-key algorithm which involves a public key and a private key. The public key is known to everyone and is used for encrypting messages whereas private key is known only to the owner of data. Key generation, encryption and decryption are the three steps to RSA algorithm.[5][3]

1) Key Generation

There are following steps to generate key in RSA algorithm.

- Randomly choose two prime numbers n1 and n2 of similar bit length and multiply them with each other.

$$n = n1.n2$$

- Calculate the eulers totient function.

$$\varphi\ (n) = (n1\text{-}1).(n2\text{-}1)$$

- Choose an integer e that is greater than 1 and smaller than '(n). The choosen integer e will be a public key.

$$1 < e < \varphi(n)$$

So the public key is (e, n)

- calculate d from the following formula which will be the private key.

$$d = e^{-1} \bmod \varphi(n)$$

So the private key is (d, n)

2) Encryption

There are following steps to encrypt data in RSA algorithm.

- Public key (e, n) will be provided to the user by the cloud provider.
- Cloud user will map his data with an integer m using padding scheme.
- After mapping the data with integer, data will be encrypted using following formula.

$$C = m^e \pmod n$$

3) Decryption

There are following steps to decrypt data in RSA algorithm.

- Cloud user who wishes to access his data will be given encrypted data C after correct authentication by the cloud provider.
- Cloud user will map his data with an integer m using padding scheme.
- Cloud user decrypts his data using following for-mula.

$$m = C^d \pmod n$$

- After getting the value m, user will access his original data.

Once the data is encrypted using RSA algorithm, it is difficult to decrypt even if anyone gets data because the value of d is known only to user who owns the data.[9]

D. Layered Approach

There are three layers in order to obtain data security in cloud.

1) *User Authentication*: In order to perform operation (add, modify and delete) on data, there must be username and password to enter the cloud.

2) *System encrypt and privacy defence*: In this layer, user data is encrypted after a successful login using encryption algorithm.

3) *File quick regeneration layer*: In this layer user data can get maximum regenerations which is damaged through rapid regeneration algorithm.

Each layer performs its task and combines with other to ensure data security in cloud.[7]

E. Homomorphic Encryption

It is a type of encryption in which specific computations are passed on cipher data. In result, it generates an encrypted text. After decryption, matches the result of operations performed on the plain text.[1][19]

F. ABE (Attribute Based Encryption)

In ABE, attributes are associated with the message and based on these attributes, secret keys will be generated for users. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.[14],[20]

VII. Conclusion

Cloud computing is growing model of computing and still work has to be done on it regarding security challenges relating to clouds. In this paper, different methods for ensuring data security in cloud were presented out of which modern methods can be applied for encrypting data before storing in a cloud.

REFERENCES

[1] Huda Elmogazy and Omaima Bamasak. Towards healthcare data security in cloud computing. In Information Science and Technology (ICIST), 2013 International Conference on, pages 363–368. IEEE, 2013.

[2] C. Sajeev G. Jai Arul Jose. Implementation of data security in cloud computing. In International Journal of P2P Network Trends and Technology, August 2011.

[3] Birendra Goswani and Dr SN Singh. Enhancing security in cloud computing using public key cryptography with matrices. International Journal of Engineering Research and Applications, 2(4):339–344, 2012.

[4] Anita Deshmukh Prajakta Khandave K. S. Wagh, Swapnil Chaudhari. Data security in cloud computing. In International Journal of Current Engineering and Technology, INPRESSCO, June 2014.

[5] Simarjeet Kaur. Cryptography and encryption in cloud computing. VSRD International Journal of Computer Science & Information Technology, 2(3):242–249, 2012.

[6] Xueping Liu. Data security in cloud computing. In Proceedings of the 2012 International Conference on Cybernetics and Informatics, pages 801–806. Springer, 2014.

[7] Puneet Mittal Meenakshi Pawar, Sukhwinder Sharmar. A secure frame-work for data security in cloud computing. In International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), April 2014.

[8] Shivali Munjal and Ramandeep Singh. Data security in cloud computing. In International Journal of Scientific and Engineering Research, Volume 5, Issue 3, March 2014.

[9] Sudha Singaraju Parsi Kalpana. Data security in cloud computing using rsa algorithm. In International Journal of Research in Computer and Communication technology (IJRCCT), September 2012.

[10] Jing Peng. A new model of data protection on cloud storage. Journal of Networks, 9(3):666–671, 2014.

[11] Swati N Ranpise Meghana R Kanthale Prajakta R Rajapure, Deepali S Khandzode. Data security in cloud computing using separate encryp-tion/decryption cloud service. In International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), April 2014.

[12] P. Rewagad and Y. Pawar. Use of digital signature with diffie hellman key exchange and aes encryption algorithm to enhance data security in cloud computing. In Communication Systems and Network Technologies (CSNT), 2013 International Conference on, pages 437–439, April 2013.

[13] V Umakanta Sastry, N Ravi Shankar, and S Durga Bhavani. A modified playfair cipher involving interweaving and iteration. International journal of Computer theory and Engineering, 1(5):594–598, 2009.

[14] T V Sathyanarayana and L.Mary Immaculate Sheela. Data security in cloud computing. In Green Computing, Communication and Conser-vation of Energy (ICGCE), 2013 International Conference on, pages 822–827, Dec 2013.

[15] OM Soundararajan, Y Jenifer, S Dhivya, and TKP Rajagopal. Data security and privacy in cloud using rc6 and sha algorithms. volume 6, pages 202–205, 2014.

[16] M. Sugumaran, B.B. Murugan, and D. Kamalraj. An architecture for data security in cloud computing. In Computing and Communication Technologies (WCCCT), 2014 World Congress on, pages 252–255, Feb 2014.

[17] Sriram Ramanujam Vamsees Krishna YarlagAdda. Data security in cloud computing. In Journal of Computer and Mathematical Sciences, 2011.

[18] Stallings William and William Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[19] Feng Zhao, Chao Li, and Chun Feng Liu. A cloud computing security solution based on fully homomorphic encryption. In Advanced Commu-nication Technology (ICACT), 2014 16th International Conference on, pages 485–488, Feb

2014.

[20] Zhibin Zhou and Dijiang Huang. Efficient and secure data storage operations for mobile cloud computing. In Proceedings of the 8th International Conference on Network and Service Management, pages 37–45. International Federation for Information Processing, 2012.