International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 6 (2017), pp. 1419-1429
© Research India Publications
http://www.ripublication.com

Cloud Computing: Security Issues & Solution

Shweta Singh[1]
M. Tech Scholar, Department of CSE,
Jamia Hamdrad University, Delhi, India.

Tabrez Nafis[2]
Assistant Professor , Department of CSE,
Jamia Hamdrad University, Delhi, India.

Ankita Sethi[3]
Assistant Professor, Department of CSE,
IPEM group of institutions, India.

Abstract

It is the technology for providing the computing services such as servers, storage, database, networking etc over the internet on pay per use pattern. It is more popular in today's era as it helps in cost reduction associated with computing. Although it is one of the most prominent technology for such kind of services, the limitation of the technology is the "Data Security and Integrity" in the environment. The major reason for not opting the cloud environment is the threat in the user's mind about their data security and integrity. Therefore to ensure the security, we are proposing the algorithm for improving the security.

It is the hybrid approach of RSA (Rivest, Shamir, Adleman) and SHA 1 (Secure Hash Algorithm)

Keywords: Cloud computing, SHA1, RSA, Hashing, Encryption, Decryption, Data Security

I. INTRODUCTION

What is Cloud Computing?

It is the process of using remote servers hosted on the internet to store manage & process data instead of using local server or personal computer on pay per use pattern. The major reason for the usage of cloud in today era is the ease which provides to access those services.

That is the client needs to pay the amount of its usage. It is the type of internet based computing where the services are delivered to organization devices via internet. There are three components of cloud computing is client computers, distributed server and data center. Storage in the cloud refers to the storage of data online in the cloud where the company's data is stored & can be accessed from different distributed resources which forms a cloud**.** It **is** not necessary to install software locally on the computer therefore it provides platform independence. With the help of this concept the business applications become mobile and collaborative[10].

The three cloud layers are:

- Infrastructure cloud: Abstracts applications from servers and servers from storage
- Content cloud: Abstracts data from applications
- Information cloud: Abstracts access from clients to data

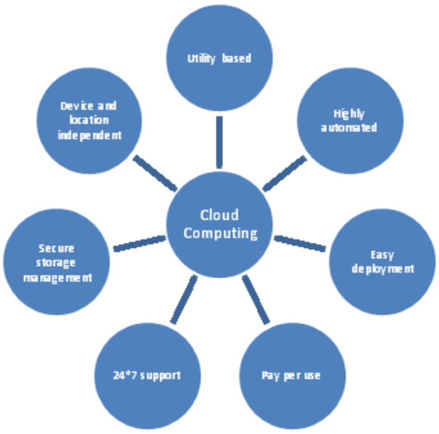

Figure 1: Cloud Computing

Figure 1 describes the characteristics of cloud computing. Cloud computing provides infrastructure, data and software as a service.

II. DATA SECURITY ISSUES IN THE CLOUD

People are using cloud for their business and they are using the cloud for data storage purpose, hence it is used as base for the companies[9] .But the major obstacle for the adoption of cloud as the storage medium is the threat in the user's mind with respect to the security of their valuable data in the cloud.

Some of the security issues[4] in the context of cloud computing are[14]-

1) Data Integrity
2) Privacy & confidentiality
3) Data availability
4) Data location & Relocation

1) **Data Integrity**: Data integrity is the basic component of information security. It refers to the assurance of consistency, correctness and trustworthiness of data.

   Integrity means that the data is free from tempering and alteration. Cloud service processing uses some efficient and effective mechanism to ensure the integrity in the cloud environment.

2) **Privacy & confidentiality**: Its refers to the property that the data is made unavailable unauthorized user. In simple words, it refers to the mechanism where the data is accessible to the user who is authorized to the access the sensitive data where others, including cloud computing processing should not take any information out of it. It also protects the data from accidental losses of data.

3) **Data availability:** It refers to a process in which data is made available wherever it is expected to be used by end user & the application. It ensures the occurrence and availability of the data in normal as well as in the disaster recovery operations.

   The availability of cloud technologies can be increased by making internet access available but the user is dependent on the resources available in the limited time frame.

4) **Data location & Relocation:** In the cloud computing the data is mobile which means data location is not known to the customers & user. Mostly it does not matter for the user. For example the photographs in the cloud can be anywhere in the world and it does not matter for the user .But in case of sensitive and confidential information user want to know the location of it.

   Sometimes user wants to specify a preferred location. To fulfill this purpose a contract is made between the Cloud computing processing and user regarding the space in the particular location or to reside on a known server.

   The contract should agree prior to the implementation of data but the issue is that the user is unaware of it.

   Another issue is the movement of data from one location to another. Initially data is stored in any location in the cloud but it is moved to other location because of various reasons.

III. RELATED WORK

In this section, we will summarize the work which has already done in the cloud computing data security.

Data security in cloud computing is very crucial as well as essential task as there is a threat to the security of confidential data. Since data is stored in cloud's space which is hosted by third party instead of storing the same in client computer. Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale [11] have discussed the importance of cloud security and steps to improve the cloud security. In [12] Ramgovind et al. suggested the ways to manage cloud security including : cloud governance, cloud transparency and cloud computing security impacts. In [13] the authors proposed an Effective Privacy Protection Scheme (EPPS) to provide the appropriate privacy protection for cloud services

.Sudhansu Ranjan Lekha et.al[4] has proposed the hybrid approach of RSA & MDI. In this algorithm the researchers have combined the two technologies for encryption, decryption & hashing. The work that has been already done in the area of data security in cloud is securing the data with the hybrid approach of RSA & MD5.

IV. PROPOSED WORK

We are combing RSA and SHA1 for the better security. RSA is for the encryption and decryption of the data and SHA1 is for generating hash value. It helps to provide security which only the authorized user can access it. Before storing the data into the cloud , it first encrypts the data. After receiving the request from the client , the CSP authenticates the user and finally decrypts the message and delivers it to the user. In this algorithm we are taking a string and we will generate the public key and private key and encrypt the string using the RSA algorithm and finally generating the hash value of the same message using SHA1. We have opted the manual mechanism as the tool requires highly skilled professionals and it is comparatively expensive.

RSA Algorithm

The RSA[2,3] algorithm is one of the popular and successful cryptographic algorithm. RSA stands for (RonRivest, Adi Shamir and Len Adleman. RSA is a the process of mapping the message into an integer. RSA includes of Public-Key and Private-Key. The data which is encrypted by Public -Key can be decrypted with the corresponding Private-Key only.

It is a three step process[8]:

1. Key Generation

2. Encryption

3. Decryption

Steps

Key Generation:

The first step in the RSA algorithm is key generation. It should be done before the encryption process between the CSP and the user.

Steps:

1. Select two random prime numbers x and y. It must be of similar bit length.

2. Compute $n = x * y$.

3. Calculate $m=(x-1)*(y-1)$.

4.Select a prime number 'e' such that e is co prime number of z and e and is not divisible by m.

5. Publish their public encryption key: KU={e,N}

6.. The private key is $e*j=1(\text{mod } m)$.

Encryption:

Encryption is the process of converting original message into scrambled (cipher)message.

Steps:

1. The function of CSP is to prove the public key to all the users who all are storing their data with cloud.

2. The message is now converted into the integer using an agreed reversible protocol called padding scheme.

3. The encryption of the data is done and hence the scrambled (cipher) text is generated C is C = me (mod n).

4. The CSP will then store the cipher text or encrypted text..

Decryption:

The conversion of the scrambled data into the original text is known as decryption.

Steps:

1.The request of the message(data) is generated to the CSP by the user .

2. After verification of the user’s authenticity, the cloud service provider sends the encrypted data i.e ’C’.

3. Then the encrypted data is then decrypted by the user by calculating m=Cd(mod n)

4. After the retrieval of m, using the reverse padding scheme the original data can be obtained.

SHA1: Secure Hash Algorithm

SHA1 is a cryptographic[5] algorithm for creating hash function. It generates a 160 bit message digest . A hash algorithm is the algorithm which converts the string of any length into a unique length string. The converted string (output) is comparatively smaller than the input data. . It is generally used to ensure data integrity, passwords authentication and message integrity.One way encryption is the result of a special mathematical function known as hash function.SHA-l processes input data in 512-bit blocks.

In this process the sender send signed, non secret message to the receiver. In this case the following steps are to be followed:

1. The original message is sent to the SHA1 algorithm in order to get a 160 bit hash value by the sender.
2. The hash value is then signed by the private key of RSA and finally both the original message and the signed hash is then send to the receiver.
3. The receiver calculates the SHA1 hash and applies the public key of sender to the signed hash to obtain the original hash after the retrieval of the message.

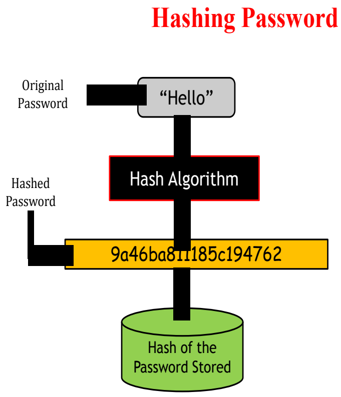

Fig 2: Hashing Password

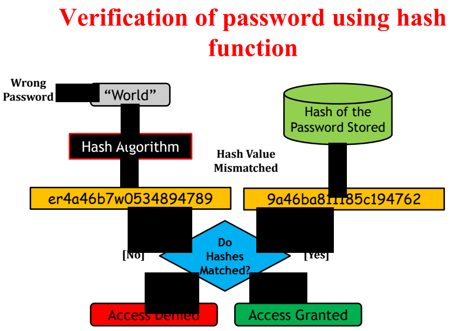

Fig 3: Verification of Password

V. IMPLEMENTATION OF PROPOSED WORK ON CLOUD

Now the step by step process of proposed work is as follows:-

1) R.S.A algorithm will generate the key on the cloud side which intern provide the public key of Cloud Service Provider (CSP) to all.
2) Then RSA will generate both the key (public& private) to the client only.The client can only send the public key to the authorized users only.
3) The public key is then sent to the cloud service provider (CSP) with the value of N by the client so that CSP can encrypt the data.
4) With the help of CSP's public key and N's value, the client will encrypt its public key and N's value using RSA algorithm. Post that it will generate the cipher text.
5) The hash value of this cipher text is then generated by using SHA1 by the client. Both the cipher text and hash value is then redirected to CSP.
6) After receiving the message from the client, the CSP will generate the hash value for the same cipher text using SHA1. The CSP then matched both the hash value in order to check the integrity. If the value matches then it is accepted otherwise it is rejected because of the indication of alteration in data.
7) If the data is accepted by the CSP, it uses its own private key and N to decrypt the cipher text for client's key and the value of N using RSA.
8) The user's data is then sent to CSP for storing it in cloud's database.
9) After receiving the data from the client, the CSP, with the help of RSA algorithm uses client public key to encrypt its data and then store the same data after encryption in cloud's database.
10) Whenever the client needs the data, it request CSP for that and to ensure the authenticity of the user, the client uses RSA algorithm to encrypt its request by its own private key and forward it to the CSP.
11) After the proper authentication& authorization of the client by the CSP then

decrypts the requests with the help of RSA algorithm using client public key. Since the message is encrypted by client private key who is only authorized to use it, and the same message can only be decrypted by the corresponding public key.

12) The CSP will send the data to the client in the encrypted form once it receives the request from the user for accessing the data.
13) The original data is retrieved by the client after decryption of the message using client private key.

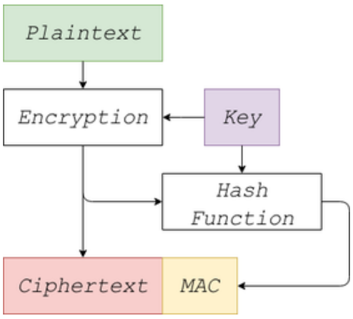

Fig 4 : Encryption Process

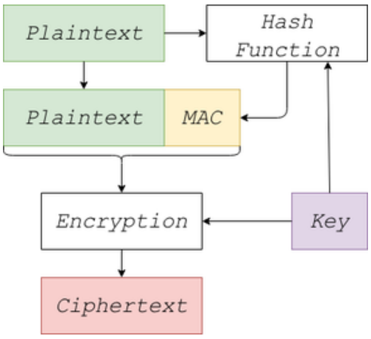

Fig 5: Key Generation Using Hashing

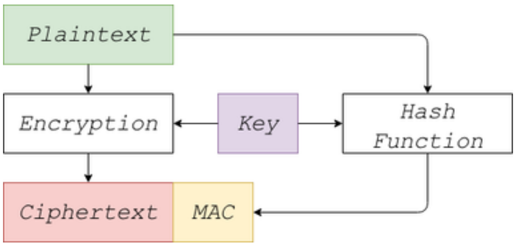

Fig 6 : Decryption Process

VI. EXPERIMENTAL OBSERVATIONS

For experiment purpose, we have some taken some sample data(a string) and implemented by using the proposed algorithm.

Step 1: Key Generation:

We have taken the sample string as " My name is Shweta Singh".

1) We have chosen two distinct prime numbers p=23 and q=53.
2) Compute n=p*q, thus n=23*53 =1219.
3) Compute Euler's totient function, Ø(n)=(p-1)*(q-1), thus Ø(n)=(23-1)*(53-1) = 22*52 = 1144.
4) Chose any integer e, such that 1 < e < 1144 that is gcd (e, 1144) =1. Here, we chose e=3.
5) Compute d , d = e-1(mod Ø(n)), thus d=3-1(mod 1144) = 763
6) Thus the Public-Key is (e, n) = (3, 1219) and the Private Key is (d, n) = (763, 1219). This Private-Key is kept secret and it is known only to the user.

Step 2: Encryption:

The Public-Key (3, 1219) is given by the Cloud service provider to the user who wishes to store the data.

1) Let the message to be send is "My name is Shweta Singh" which is converted to integer in the following manner:
2) A=0, B=1, a = 27, b=28, c=29 and so on . So the message "My name is Shweta Singh" is encoded to m= 77 121 32 110 97 109 101 32 105 115 32 83 104 119 101 116 97 32 83 105 110 103 104
3) Data is encrypted now by the Sender using the corresponding Public-Key which is shared by both the sender and the receiver.
4) C=memod n=C=77 121 32 110 97 109 101 32 105 115 32 83 104 119 101 116 97 32 83 105 110 103 104 (mod1219)= 625535179657807535.
5) This encrypted data i.e., cipher text is send to the recipient.

Step 3: Decryption:

1) The receiver decrypts the data by computing, m = Cd(mod n) = 77 121 32 110 97 109 101 32 105 115 32 83 104 119 101 116 97 32 83 105 110.

2) Once the m value is obtained, user will get back the original message using the same encoding technique.

Step 4: Generate hash value using SHA1:

1) Using SHA1 on the same string "My name is Shweta Singh", the hash value is then generated to convert the string into a unique length string.
2) The hash value of the string "My name is Shweta Singh", is

040937698BEDF9758AB2D33A4EA1BE25D4F65C12

VII. CONCLUSION

Security is the key element to the success of any cloud environment. Since many new attacks can be seen day by day and hence a very strong mechanism is needed to handle all these types of attacks. In this paper , the proposed algorithm which is the hybrid approach of RSA and SHA1 helps to provide new security solutions for these type of attacks. In our proposed work the major factor is data security and with this hybrid algorithm we are trying to meet the objective of data security.

REFERENCES

[1] Sudhansu Ranjan Lenka , Biswaranjan NayakEnhancing "Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm".

[2]. Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories , February, 2003.

[3] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, 1977.

[4] . William Stallings, "Network Security Essentials Applications and Standards", Third Edition, Pearson Education, 2007.

[5] Atul Kahate "Cryptography and Network Security".

[6] Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale "Improving Security of Cloud Environment in Dynamic Cloud Network" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1681-1684.

[7] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3), 242-249, 2012

[8] Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories , February, 2003.

[9] Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale “Improving Security of Cloud Environment in Dynamic Cloud Network” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1681-1684.

[10] Joachim Schaper, 2010, ―Cloud Services‖, 4th IEEE International Conference on DEST, Germany.

[11] Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale “Improving Security of Cloud Environment in Dynamic Cloud Network” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1681-1684.

[12] Ramgovind S, Eloff MM and Smith E. “The Management of Security in Cloud Computing” Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.

[13] I. Chuang, S. Li, K. Huang, and Y. Kuo, “An effective privacy protection scheme for cloud computing”, In Proceeding of the 13th International Conference on Advanced Communication Technology (ICACT), 2011

[14] Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73.

[15] Hadoop. (n.d.). Retrieved from http://hadoop. apache.org

[16] Hama. (n.d.). Retrieved from http://cwiki.apache. org/labs/cloudsglossary.html