Ensuring Data Security for Secure Cloud Hybrid Framework

Smriti[*], **Dr. Deepak Arora****
[*]Department of Computer Science Amity University, Lucknow, India.
[**]Professor, Department of Computer Science Amity University, Lucknow, India.

ABSTRACT

With increasing technology demand for the cloud application is also increasing. Due to this security demands are also increasing. A user can access a cloud services from anywhere and at any time or almost instantly. These features make cloud computing so flexible and prone to risk. Therefore there are possibilities of lacking confidentiality, integrity and authentication among the cloud users. So the key purpose of this research is to investigate cloud securities and build a framework using encryption algorithms to provide data confidentiality, integrity and authentication.

Keywords: Cloud Computing, Data Security, Symmetric Encryption, Public Key Encryption, SHA.

I. INTRODUCTION

Cloud computing have became very popular in today’s world. Since most of the work is done through clouds these days and data is stored in it. So information security has become one of the important issues in cloud computing, because most of the work is done through computerization and data is transferred over the network. Information security is a process of safeguarding information against intentional and malicious attacks to ensure its CIA triad [1] [2]. The CIA triad stands for three major tenets to information security: confidentiality, integrity and availability.

Confidentiality provides prevention from unauthorized usage of sensitive information. Integrity provides accuracy of information by preventing unauthorized modification of data and information.
Availability ensures that information is available whenever it is needed and it also includes prevention from denial of service attack.

Therefore CIA triad is achieved through encryption.

Encryption is the process of encoding a information in such a way that it become unreadable to unauthorized user. Encryption is done by applying encryption algorithms to the plaintext, turning it into cipher text. Encryption key is used by the encryption algorithm which specifies the method of encoding message. Any unauthorized user having a cipher text cannot see the original message. An authorized user can only be able to decode the cipher text to original text using decryption algorithm, which requires a decryption key. Generally secret key is generated by using a key-generation algorithm.

There are two basic types of encryption techniques: **Symmetric-key and public-key encryption [3]**. In symmetric-key encryption technique, encryption is done through same key. Thus communicating parties must share secret key before communication. In public-key encryption technique, the encryption is done through combination of public key and private key. Thus the encrypted message and key is published for everyone, but it can only be used by the receiving party.

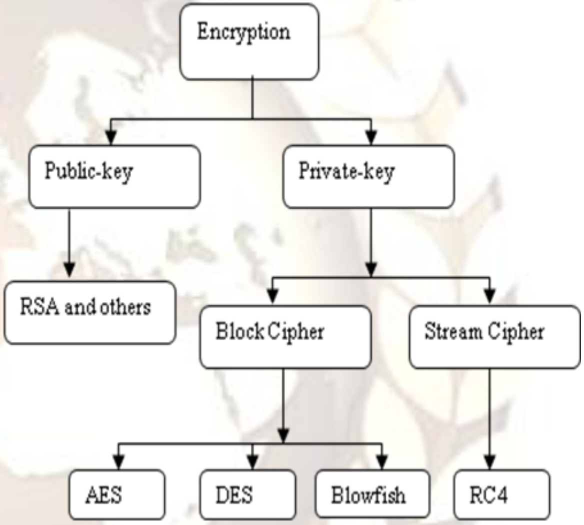


Figure1: Overview of encryption algorithms

Different combination of encryption algorithms can be used to provide information security. A framework had been proposed earlier using AES (block cipher), but when compared to stream cipher algorithms it is less energy efficient and slow[8]. So a new framework is proposed in this paper using RC4 (stream cipher) algorithm.

II. RELATED WORK

Sudha, [7] has proposed a simple security network in this paper. They have used cryptographic algorithms to provide data security in cloud computing. A symmetric and asymmetric algorithms are used to prepare a framework. Many security issues had been explored in cloud data storage, whenever a data vulnerability is perceived during the storage process a precision verification across the distributed servers are ensured by simultaneous identification of the misbehaving nodes through analysis in term of security malfunctioning, it is proved that their scheme is effective to handle certain failures, malicious data modification attack, and even server colluding attacks [5]. John Harauz et al. [6], escribed the Security Content automation protocol (SCAP) and benefits it can provide with latest cloud computing paradigm with reference to the latest report released by NIST, giving insight as to what SCAP is trying to do, It states that many tools for system security, such as patch management and vulnerability management software, use proprietary formats, nomenclatures, measurements, terminology, and content.

III. ENCRYPTION ALGORITHMS

RC4

RC4 is a stream cipher symmetric key encryption algorithm. It uses a variable key length 1 - 256 bytes to initialize a state table of 256 bytes. State table is initialized in the form of array. So the array is used for generating pseudo-random bytes and then pseudo-random stream. Thus the pseudo-random stream is XORed with the plain text to generate cipher text.

While initializing the state table there are two 256 bytes array are taken: S-Box and K- box. S-Box contains linear numbers such as $S_0=0, S_1=1, S_2=2, \ldots S_{255}=255$ and K-Box contained key to be used in repetition to fill the array. The key setup and key generation is performed for every new key to generate a unique key.

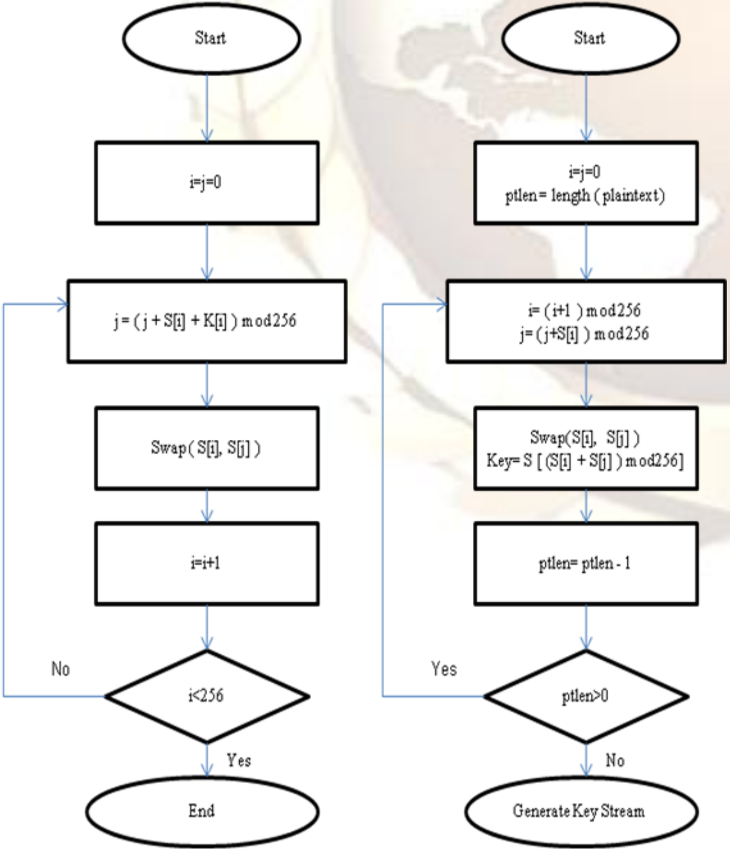


Figure 2: Block Diagram of RC4 Key generation Phases

In key set up phase S-Box is modified using pseudo random codes. It uses two counter i and j.

Key Setup phase:

```
j=0
for i from 0 to 255
j = ( j + S[i] + K[i] ) mode 256
 swap ( S[i] , S[j] )
end for
```

Pseudo Random Key Generation Phase:

```
i = 0
j = 0
ptlen = length( plaintext )
while ( ptlen>0 )
i = ( i+1) mod 256
j = ( j+ S[i] ) mod 256
swap ( S[i], S[j] )
key = S [ ( S[i] + S[j] ) mod 256 ]
output key
ptlen =  ptlen-1
end while
```

Once the pseudo random key is generated then plain text is XORed with it to generate cipher text.

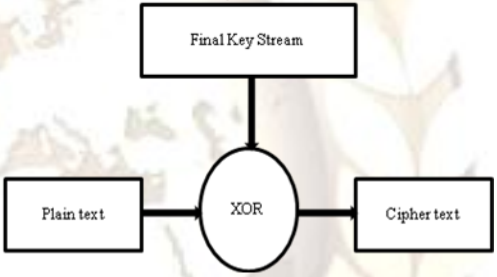


Figure 3: RC4 Working

SHA

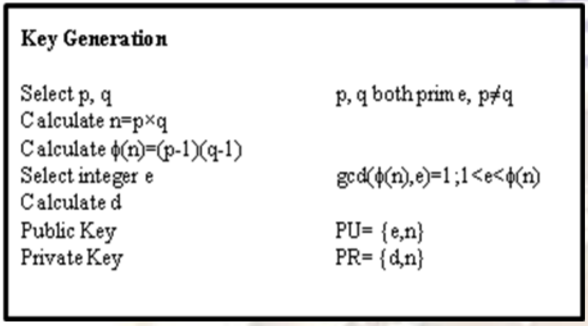
Secure Hash Algorithm uses compression function to convert a arbitrary size message to a fixed size message. Hash function can be applied to any size message and it produces a fixed size message. As compared to other hashing algorithms, it is more secure and easy to compute.

In our framework for the enhanced authentication the message digest or the hash value of the message is generated using secure hash algorithm which is of fixed size. Then the hash value produced is concatenated with the actual encrypted data and digital signature. Later whole concatenated strings are securely encrypted using RSA algorithm i.e. public key of the receiver and then send to the cloud to the requesting recipient. On the receiver side data integrity is checked by the hash value generated by deciphering message and sender authentication is verified.

RSA

RSA stands for Rivest, Shamir & Adleman of MIT, the one who introduced RSA. RSA is asymmetric public key encryption technique which is based on exponentiation in a finite field over integers

modulo a prime numbers. In order to encrypt a message M the sender should have a public key of the receiver, PU={e,n} is the public key which is used to compute the cipher message: $C=M^e$ (mod n) has to obtain public key of recipient, where $0 \leq M < n$. At the receiver end recipient uses their private key to decrypt the message, PR={d,n} is the private key which is used to compute the original message: $M = C^d$ (mod n), where $M < n$.
RSA uses Euler's Theorem: aø(n)mod n = 1 where gcd(a,n)=1 in RSA we have to initially calculate n=p.q such that ø(n)=(p-1)(q-1) one has to carefully chose e & d to be inverses mod ø(n) [7].



Key Generation

Select p, q	p, q both prime, p≠q
Calculate n=p×q	
Calculate ϕ(n)=(p-1)(q-1)	
Select integer e	gcd(ϕ(n),e)=1 ;1<e<ϕ(n)
Calculate d	
Public Key	PU= {e,n}
Private Key	PR= {d,n}

Figure 4: RSA key generation

IV. PROPOSED SECURITY FRAMEWORK

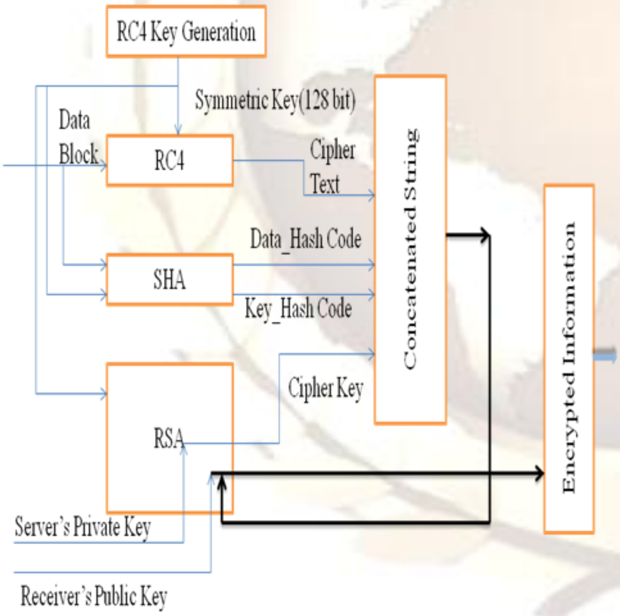


Figure 5: Proposed Hybrid Framework

In this scenario we have considered that interaction of cloud server and cloud client is the initial step. Only a registered cloud client can avail the services of the cloud. So the user has to be registered cloud client, if the user is registered user then only login and password is verified. If the user is new then he needs to register in the cloud server. So the user registers itself and the Certificate Authority generates a certificate for the cloud client. After user login authentication a random string is generated by the server for the client and digital signature is generated by sighing random string with client's private key.

The client can request for the data from the cloud data centers after the user is authenticated by the two step authentication. Then the proposed secure hybrid framework is executed to ensure the information security. The framework uses a symmetric key algorithm for efficiency, confidentiality and simplicity and along with it a public key algorithm for secure key exchange. So the hybrid is constructed with symmetric and asymmetric encryption algorithm for the enhanced framework.

Step 1: Upon successful authentication of the client by server, the data is encrypted using a symmetric (RC4) algorithm to generate cipher text.

Step 2: Data hash code and key hash code is generated using secure hash algorithm. A concatenated string is generated by combining data hash code, key hash code, symmetric key to generate cipher text and cipher text.

Step 3: Then the concatenated string is encrypted with the receiver's public key by using RSA algorithm.

Step 4: Apply the reverse process .i.e. the whole string is decrypted at receiver end by the recipient private key and the required symmetric key is obtained on decryption.

Step 5: Original message is decrypted using symmetric encryption algorithm (RC4) key, then the validation and verification of the sender is done.

Step 6: Secure Hash Algorithm (SHA) is used of generating hash value for checking integrity of the message sent.

Step 7: Digital Signature is only validated when the value of the message matches the hash code sent and then data integrity accepted.

Step 8: Once data is transfer in the secure form then the request is terminated.

Following were the steps to transfer secure data over clouds with the help of hybrid framework. Proposed algorithm for Hybrid Framework.

1. RC4 key set up
   a) Two arrays are initialized: S-Box and K-Box, S-Box contains linear number such as such as $S_0=0,S_1=1,S_2=2,\ldots S_{255}=255$ and K-Box contained key to be used in repetition to fill the array.

b) Select variable i, j as zero,
c) Calculate j=(j + S[i] + K[i]) mod 256,
d) Swap S[i] , S[j],
e) Increment i by 1 i.e. i=i+1,
f) If i<256 goto step c else end.

2. RC4 key generation
   a) S[i] is the modified S-Box during key set up phase.
   b) Select variable i, j as zero,
   c) Calculate length of plaintext such that
      ptlen= length (plaintext),
   d) Calculate i= (i+1) mod 256
      j= (j + S[i]) mod 256
   e) Swap S[i], S[j],
   f) Calculate Key as
      Key = S[(S[i] + S[j]) mod 256]
   g) Decrease plaintext length by 1 i.e.
      ptlen = ptlen -1
   h) If ptlen > 0 goto step d else end.

3. Encrypt datablock using RC4
   Plaintext Xored with Key to produce Cipher text
4. Data Hash code and Key Hash code are generated using Secure Hash Algorithm
5. RSA key generation
   a) Select variable p and q where p and q both are prime, p≠q,
   b) Calculate integer n= p × q ,
   c) Calculate function of
      Such that $\phi(n) = (p-1)(q-1)$,
   d) e_s a public key of server
      Select integer e_s such that
      gcd $(\phi(n), e)=1$; $1<e<\phi(n)$,
   e) Calculate d_s
      $d_s = e_s^{-1} \pmod{\phi(n)}$
   f) Server Public key ($e_{s,}$ n)
      Server Private key ($d_{s,}$ n)
   g) Similar steps are followed to generate receiver's public and private key
   h) Therefore Receiver Public key ($e_{r,}$ n)
      Receiver Private key ($d_{r,}$ n)

6. Encrypt key of RC4 using RSA(Server private key)
   Cipher key = (Key) power of d_s mod n
7. Concatenate String = cipher text + data hash code + key hash code + cipher key
8. Encrypt concatenated string using RSA(receiver's public key)
   Encrypted text = (concatenated string) power of e_r mod n.

V. CONCLUSION AND FUTURE SCOPE

In this paper a simple hybrid framework is proposed with the help of encryption algorithms. This hybrid framework produces a secure data which can be transferred over the clouds. The combination of RC4, SHA and RSA is used to enhance data security and to give more energy efficient and fast working environment. A practical implementation of the framework can be performed.

REFERENCES

[1] http://www.mhprofessional.com/downloads/produ cts/0072254238/0072254238_ch01.pdf

[2] Kinamik, "the CIA triad: have you thought about integrity", kinamik data integrity, 2007.

[3] Goldreich, Oded. Foundations of Cryptography: Volume 2, Basic Applications. Vol.2. Cambridge university press, 2004.

[4] Nidhi Singhal, J.P.S.Raina "Comparative Analysis of AES and RC4Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.

[5] M.Sudha and M.Monica "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications, Vol. 1, No. 1, March 2012.

[6] Cong Wang, Qian Wang and Kui Ren. "Ensuring Data Storage Security in Cloud computing", IEEE 978-1-4244-3876-1/2009.

[7] John Harauz, Lori M. Kaufman and Bruce Potter, "Data security in the world of cloud computing" IEEE CO Published by the IEEE Computer and Reliability Societies, 2009.

[8] Bellare, Mihir, "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000.

[9] Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012.

[10] Rashi Vohra, Brajesh Patel, "An Efficient Chaos - Based Optimization Algorithm Approach For Cryptography", International Journal of Communication Network Security ISSN: 2231–1882, Volume-1, Issue-4, 2012.

[11] Shashi Mehrotra Seth, Rajan Mishra "Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011.

[12] S. Subasree and N. K. Sakthivel, "Design Of A New Security Protocol Using Hybrid Cryptography Algorithms", IJRRAS 2 (2), February 2010.

[13] Allam Mousa, Ahmad Hamad, “Evaluation of the RC4 Algorithm for Data Encryption”, International Journal of Computer Science and Applications, Volume 12, Number.2, June2006.

[14] Guang Gong, Kishan Chand Gupta, Martin Hell and Yassir Nawaz, “Towards a General RC4-like Keystream Generator”, Information Security and Cryptology Lecture Notes in Computer Science Volume 3822, 2005.

[15] Mihir Bellare, Phillip Rogaway, “Optimal Asymmetric Encryption How to Encrypt with RSA”, Advances in Cryptology Eurocrypt 94 Proceedings, Lecture Notes in Computer Science Vol. 950, A. De Santis ed., Springer-Verlag, 1994.

[16] William Stallings, “Cryptography and Network security”, 5e -Pearson education publications.