Int. Journal of Engineering Research and Applications www.ijera.com
ISSN : 2248-9622, Vol. 4, Issue 9(Version 1), September 2014, pp.83-86

RESEARCH ARTICLE OPEN ACCESS

Security Issues related with cloud computing

Manju, Dr. P.C. Vashist
*(Department of Computer Science, MVN University, Palwal)
Guide:
(HOD of Computer Science and Engineering), MVN University, Palwal)

ABSTRACT
The term CLOUD means Common Location Independent Online Utility on Demand. It's an emerging technology in IT industries. Cloud technologies are improving day by day and now it become a need for all small and large scale industries. Companies like Google, Amazon, Microsoft etc. is providing virtualized environment for user by which it omits the need for physical storage and others. But as the advantage of cloud computing is increasing day by day the issues are also threatening the IT industries. These issues related with the security of the data. The basic idea of this review paper is to elaborate the security issues related with cloud computing and what methods are implemented to improve these security. Certain algorithms like RSA, DES, and Ceaser Cipher etc. implemented to improve the security issues. In this paper we have implemented Identity based mRSA algorithm in this paper for improving security of data.
Keywords – Cloud computing, RSA, Encryption, Security Issues

I. INTRODUCTION

In Modern Era, the whole work is now shifting towards the internet. When we hear Cloud Computing then the concept of "ON-DEMAD" access of data and "VIRTUALIZATION" comes into mind. Today the users should have no concern about the server, physical storage like RAM, Hard Disk, and CD etc. to store the data. Cloud is divided into two parts- The Front part and the back part. The Front end includes "The users and the customers". The user should have a device to access the data and they should also have the internet connection with the device and the second part includes the collection of various computers, data storage (like RAM, Hard disk etc.) And server. They are connected with each other through internet. All servers have their own independent operating system. Apart from back end and front end we also have an Administrator whose work is to check "Is everything going smoothly or not". It follows some set of rules which are called Protocols and use a special kind of software called Middle ware.

Identity base encryption method uses user's identity to create public keys and the private key is generated from this public key. After that private key is distributed between user and SEM server. In this way only authenticated user and SEM server have detail about the private keys. We assume here that SEM sever is not compromised.

Cloud computing has three service models which are:-
Public Cloud
Private Cloud
Hybrid Cloud

Public Cloud: It is a model where user access the data via mainstream web browser. It is based on pay-per-use model because the user got only that data for which he pays. Public clouds are accessible to anybody. In daily life we access certain applications like Google, Yahoo etc. are example of public cloud.

Private Cloud: Private cloud is company's own data center where the employers of companies can access the data and store this data. It is easier to regulate the data in private cloud because it is limited only with the organization. Security is better inn private cloud as compared to other model.

Hybrid Model: Hybrid cloud are both combination of public and private cloud as they combine features of both the clouds. It combines feature of virtualization environment as provided in private cloud and they also use of public model which use traditional computers but they should have hard disk, internet and other means to access the data. It provides more security to data because it combines features of both the clouds. It also give more access of data to the customer

Community cloud

As we know there are many organizations who have same interest and requirement of data. This need of sharing data can be shared between different organizations. This operation can be within the company or outside the company also. This also has one major advantage that companies with same interest can save lots of money by sharing. This model is very helpful for small IT companies and business. The cost can be shared by different organizations

II. LITERATURE SURVEY

[1] Identity-Based Encryption from the Dan Boneh, Mathew Franklin: Boneh & Franklin found this scheme 'BasicIdent' in 2001, in which central role is played by the mathematical primitive "Bilinear Pairing" for encryption. This scheme is with Random Oracle Model which involves a hash function. It provides Chosen Plaintext Security (IND-ID-CPA) [7].

Bilinear Diffie-Hellman Problem: The problem is defined as, given (G, q, ê, P, AP, bP, cP) where P $\in$ G and a, b, c are selected at random from $\mathbb{Z}_q^*$, compute ê (P, P) ^{abc}. It means that this problem is computationally intractable [9]. In Boneh-Franklin scheme.

[2] **P. Subhasri et al. in his Journal "Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing**" explains about the problem of data privacy, data stealing, etc. In her proposed work she give an encryption algorithm for designing complete security solution using Reverse Ceaser Cipher Algorithm. She proposed two level of data security solution using Reverse Ceaser Cipher algorithm with encryption using ASCII value of full 256 characters. The main idea of this paper is to explain about the security related with the both cloud providers and cloud consumers. This paper overcomes the problem of earliest ceaser cipher algorithm. Through this propose algorithm user can easily encrypt and decrypt the combination of alphabets, numbers, and special characters efficiently.

[3] **Xuhua Ding and Gene Tsudik** implemented **"simple identity based cryptography with mediated RSA**". In this paper RSA key is splatted between user and another server SEM. Here, we omit the need of public key certificates because the public key is derived from the user's entity such as email, name, phone number and other information. . When user want to send any information to another user then public key is derived from the user's identity and then private key is split between user and server. In this server should not be compromised, if this condition become true then this is the secure system. It changes the nature of obtaining public keys by constructing one to one mapping between identities and public keys.

III. FIGURES AND TABLES

Key areas	RSA	DES	AES
Invented By	Rivest, Shamir	IBM 75	Rijman, Joan
Length of key	256 bits	56	128,192 and 256
Total rounds	1	16	10,12 or 14
Size of block	Variance	64	128
Security	Good	Not-enough	Excellent
Execution Time	Slowest	Slow	More fast

IV. Proposed work

The proposed System, uses socket programming language, c programming, and open SSL layer. Identity Based Encryption with Mediated RSA (IBE-mRSA) is to provide the better security to the data in Software-as-a-Service of Cloud Computing. It is based on Public Key Encryption algorithm Mediated RSA and Basic Identity Based Cryptography scheme. Here the public key is generated from the user's identity such as email, phone no etc. Here SEM is the mediator which distribute keys between user and server. The half private key store in SEM server and half to user. Hence key escrow problem can be solved by this method.

5.1 Proposed Algorithm: IBE with Mediated RSA

1. Setup(ID_r)

Input: Identity of Receiver.

Method:

1. Take random s $\in \mathbb{Z}_q^*$, which is master key of prime order q.
2. Public Key P_{id} is defined as

$$P_{id} = s \bullet H(ID_r)$$

Output: Public Key P_{id}

1. Keygen(P_{id})

Input: Public Key P_{id}

Method:

1. Let k be the security parameter
2. Generate random k/2-bit primes, p′ and q′
   such that p = 2p′ + 1 and q = 2q′ + 1 are also prime.
3. n ← pq, e $\in_R \mathbb{Z}^*_{\emptyset(n)}$, such that
   $d \leftarrow e^{-1} \bmod \emptyset(n)$
4. For each user (x)
   a. $s \leftarrow k - |P_{id}| - 1$
   b. $e_x \leftarrow 0^s \,||\, P_{id} \,||\, 1$
   c. $d_x \leftarrow 1 / e_x \bmod \emptyset(n)$
   d. $d_{x,u} \leftarrow Z_n \oplus 1 - \{0\}$ *//private key for user*
   e. $d_{x,sem} \leftarrow (d - d_{x,u}) \bmod \emptyset(n)$ *//private key for SEM*

Output: Private Key for user and Security Mediator, security parameter, modulus n.

3. Encryption(k, P_{id}, n)

Input: Public Key P_{id}, Security Parameter k and Modulus n

Method:

1. Retrieve P_{id} from Setup procedure.
2. s ← k - | P_{id} | - 8
3. e ← 0^s || P_{id} || 1
4. Encrypt message m with (e, n) using standard RSA technique.

Output: Encrypted Message m′.

4. Decryption (m′)

Input: Encrypted Message

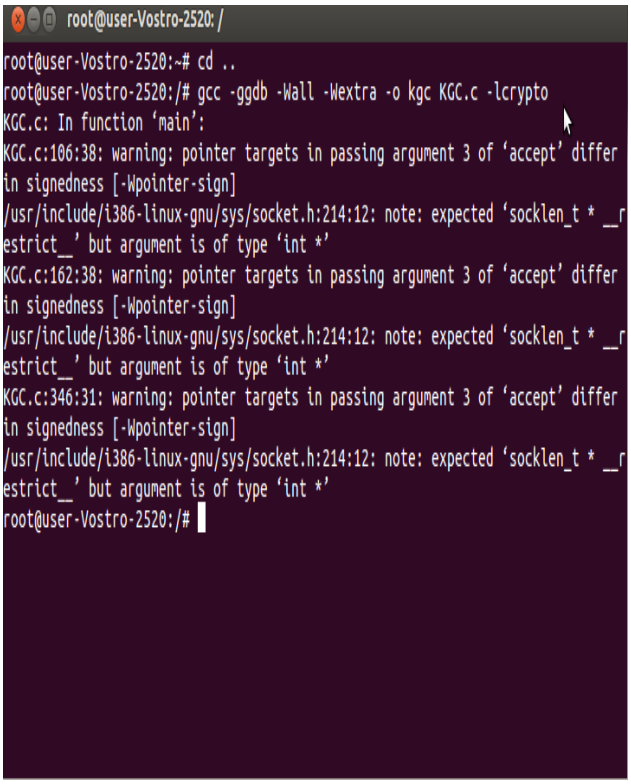
Method:

1. User m′ = encrypted message
2. User sends m′ to SEM
3. In parallel,
   SEM:
   1. If USER revoked return (ERROR)
   2. $PD_{sem} \leftarrow m'^{dsem} \bmod n$
   3. Send PD_{sem} to USER
   USER:
   4. $PD_u \leftarrow m'^{du} \bmod n$
4. USER: M ← ($PD_{sem} * PD_u$) mod n
5. USER: If succeed, return (m)

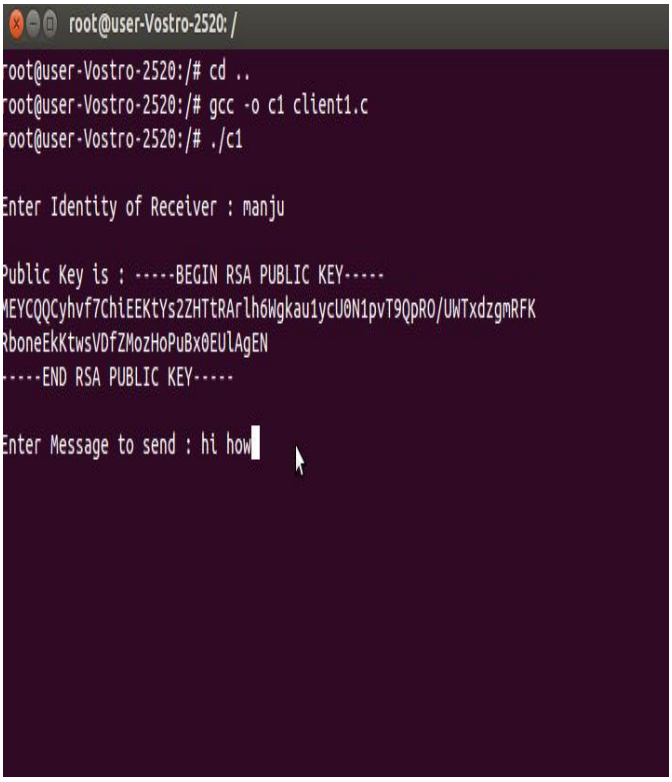
V Implementation

The Program is implemented on Ubuntu Software which is an open source software of Linux. It can also run into other software's of Linux. The important steps of this evaluation are explained as below:-

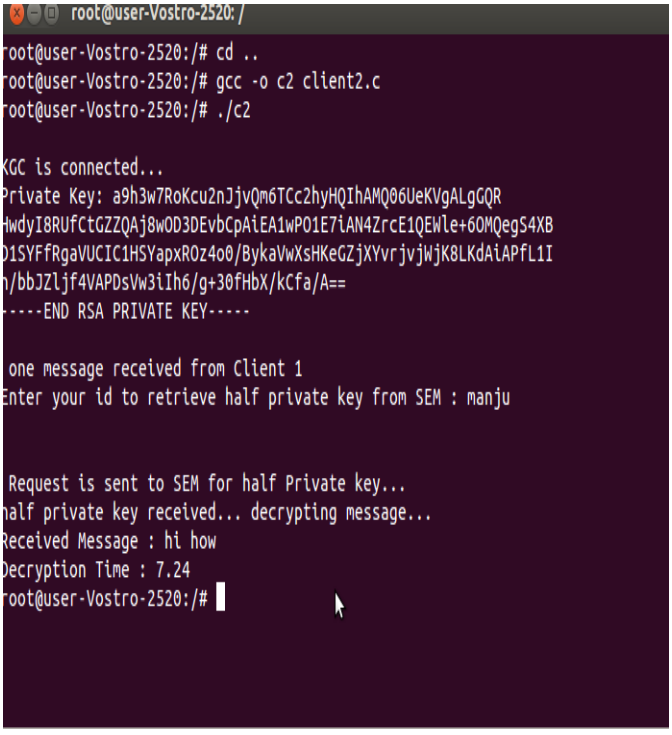
Step:1 Open 4 terminals and write their specific command on them and request for client process.



Step:2 Type message to send and distribution of public and private key runs on background



Step:3 Encryption time and decryption time generated for message



V. CONCLUSION

We know that the internet field is increasing day by day and the scope of cloud computing is also increasing in IT firms.

This system is work under random oracle model. Key Generation operation uses Hash function to generate key, which increase time to generate key. So it's needed to find out alternative technique which doesn't use hash function. So that key generation time will be reduced. And in encryption is also expensive because it doesn't use standard RSA technique to encrypt message and it requires public key mapping all the time.

REFERENCES

[1] P. Subhasri, Dr. A. Padmapriya, *Implementation of Reverse Ceaser Cipher Algorithm for cloud computing*, International Journal for advanced Research in Engineering and Technology, Vol-1, Issue VI, July-2013.

[2] Omer K. Jasim, Safai Abbas, El-sayed M. El-*Horbaty and Abdel-Badeeh M. Salem, Efficiency of Modern Encryption Algorithms in Cloud Computing*, International Journal of Energing Trends and Technology in Computer Science, Vol-2, Issue 6, Nov-Dec 2013.

[3] D. Boneh, X. Ding, and G. Tsudik. Identity based encryption using mediated rsa. In 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug. 2002. KIISC.

[4] D. Boneh, X. Ding, G. Tsudik, and C.M. Wong. A method for fast revocation of public key certificates and security capabilities. In 10th USENIX Security Symposium, Washington, D. C., Aug. 2001. USENIX.

[5] D. Boneh and M. Franklin. Identity-based encryption from the Weil Pairing. In Kilian [15], pages 213–229.

[6] J.-S. Coron and D. Naccache. *Security analysis of the gennaro-halevi-rabin signature scheme*. In Preneel [18], pages 91–101.

[7] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. *RSA-OAEP is secure under the rsa assumption*. In Kilian [15], pages 260–274

[8] P.Subhasri, *Multilevel Encryption for Ensuring Public Cloud*, International Journal of Advanced Research in Computer Science and Software Engineering, Vol-3, Issue-7, July 2013.

[9] Vijay. G.R., Dr. A. Rama Mohan reddy, *Security Issues analysis in Cloud Enviornment*, International Journal of Enginnering Research and Applications, Vol-3, Issue 1, PP. 854-857, Jan-Feb 2013.

[10] M. Bellare, A. Boldyreva, and S. Micali. *Public-key encryption in a multi-user setting: Security proofs and improvements*. In Preneel [18], pages 259–274.