Cloud Computing and its Challenges

Khushbu
M.tech Student,Department of CSE,
NGF College of Engineering & Technology,
Palwal Haryana, India,
9017302991
sharma.khushbu123@gmail.com

Meenakshi
M.tech Student,Department of CSE,
NGF College of Engineering & Technology,
Palwal Haryana, India,
8930218403
Meenakshi.attri54@gmail.com

Abstract:- The term CLOUD means, In today's world we cannot imagine our life without internet. The whole data is now shifting towards "cloud". The term cloud (Common Location Independent Online Utility on Demand) computing explains how a "cloud" holds millions of data with safety and it provides data to users whenever it necessary. So the term cloud computing also explains the concept of virtualization. But with increasing its usage the threats with cloud computing also increasing, these issues like privacy, data handling, data stealing, etc. In this paper we are explaining the concept of identity based mRSA algorithm where our SEM server is never compromised and security issues are increased at great level.

Keywords **–** Cloud computing, IB-mRSA, Encryption, SEM server, KGC

*****

I. INTRODUCTION

It is the most widely used techniques now a days in IT industries. Term cloud computing requires understanding of various other terms that are closely related with the computing. We can also say that cloud computing is a future in the next few years, maybe we can say that cloud computing can save the world, possibly people could have everything they demand on their desktops. It could be the next natural step of developing of on-demand services and products. Cloud computing explains computing in which IT-related capabilities are provided as a service this allow users to access technology from anywhere and hence user is able to get the information.The basic concept of cloud computing is that we should have internet connection and we should also have the desktops and other medium where we can see our data.

Cloud computing is a subscription based service where one can obtain networks storage space or computing resource. In the same way its resources are also trying their best to provide all the basic hardware and software need of customers We know we can access our email from anywhere from we want in the same way in cloud computing our data is stored on the cloud and we can access it whenever we have any need and one major advantage is that we can access in any source like in desktop, mobile phones or in tablets. Computing can be described as activity of using or developing computer hardware and software.

One of the main requirement of cloud computing is that we should have an internet connection in order to access the data. Internet connection can be wired internet or it can be wireless or a mobile broadband connection. This benefits us to access the data from where we want to access. This can also help to run any type of business smoothly.

The main problem of the cloud computing is related with the security. Here the algorithms like RSA and mRSA algorithms are implemented. Certain symmetric and asymmetric algorithms are implemented in order to secure the data. In RSA algorithm key size is 256 bytes which secure the data. Here the time of encryption and decryption is calculated after sending and receiving the data. Decryption time is more as compared to encryption of data because private key is spitted between SEM and client. This private key needs to be collected from both server and client. Today, most of the cloud computing server are using basic algorithms like AES, RSA and DES other symmetric and asymmetric algorithms. The main problem of these algorithms are that they are bit complex while using more bits. RSA and other algorithms take more time to encrypt and decrypt the data. Here we have used m-RSA algorithm, which is more secure and faster as compared to other algorithms. It also does not need any certificate for authentication. But these algorithms works not properly when we increase the size of bit. We have used 256 bits and 512 bits and comparison between other key sizes.

Cloud computing has three basic models and each model have its own feature. These models are:-

- Public Cloud
- Private Cloud
- Hybrid Cloud

Public Cloud: Public models are used by us everyday. These are accessed by internet and web browser. In our daily life we use various applications like Google,amazon,yahoo and other. These all are based on the concept of pay per user model. Security, Privacy and data stealing are the major problem associated with this type of cloud computing. The advantage of the public cloud computing is that we can use it whenever we want and its free of cost to use.

Private Cloud: Private cloud computing is more secure than public cloud because here data sharing is restricted only to some personal users and these can be accessed by authenticating users. So we can handle security, data privacy and other issues easily. Private cloud is restricted only to some limited and authorized companies and they are costlier than public cloud.

Hybrid Model: Hybrid cloud is a combination of both public and private cloud. It combines feature of virtualization environment as provided in private cloud and they also use of public model which use traditional computers concept but they also have internet, hard disk, and other means to access the data. Hybrid cloud is more convenient to use

II. LITERATURE SURVEY

Pranita P. Khairnar discussed about the problems of security methods. In his paper he try to minimize the risk factor of security. He introduces many methods to improve the security of data. He introduced the many security concerns like Lack of standards, Privacy and various attacks etc. For all these problems he introduced the solution . In his research paper he introduced the methods like encryption, authentications etc. Many cloud providers does not expose their infrastructure to customers hence it is difficult to secure their own environment by the customers. He included many services like authentication and encryption, access control ,encryption, use of filters and important data security model.

Chang-**Lung Tsai *et al.*** proposed a mechanism which try to find out some feasible solution for security mechanisms. Cloud computing was a new concept of providing dramatically scalable and virtualized resources, software and hardware on demand to consumers. Consumers could typically requests cloud services via a web browser or web service. Using cloud computing, consumers could safe cost of hardware deployment, system maintenance or software licenses.

Danish Jamil *et al* explained the uses of cloud computing environment but he also explained about some cloud security problems, which are Browser Security, XML Signature Element Wrapping, , Cloud Malware Injection Attack and Flooding Attacks, and also give the possible countermeasures. Cloud computing moved away from computers and the distinct enterprise application server to services provided by the cloud of computers. The emergence of cloud computing made a tremendous impact on the Information Technology (IT) industry over the past few years. Currently IT industry need Cloud computing services to provide best opportunities to real world. The objective of that was to explore the different issues of cloud computing and identify important research opportunities in this increasingly important area.

III. PROPOSED WORK

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

	Identity Based Encryption	**IB-Mediated RSA**
Compatible with Standard RSA	No	Yes
Certificate Authority Required (PKI)	No	Yes (it's Optional)
Deployment	Hard	Easy
Easy to Maintain	No	Yes
Key Generation (On Standard Machine)	7ms	1 ms
Encryption (On Standard Machine)	40 ms	7 ms
Decryption (On Standard Machine)	40 ms	35 ms
Key Revocation	Periodic	Per-operation
Key Escrow Problem	Yes	No
Private Key Generated by	Key Generator Centre	Certificate Authority
Private Key Divided?	No	Yes, between Security Mediator and User
Security Mediator Required	No	Yes

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 standard RSA technique.

Modulus n

Method:

1. **Retrieve P_{id} from Setup procedure.**
2. **$s \leftarrow k - |P_{id}| - 8$**
3. **$e \leftarrow 0^s \| P_{id} \| 1$**
4. **Encrypt message m with (e, n) using**

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: $M \leftarrow (PD_{sem} * PD_u) \bmod n$
5. USER: If succeed, return (m)

Implementation

The program is implemented on Ubuntu Software And it can also be used on other software also.

To implement this project we should follow following methods.

Step:1 Open terminal and execute commands on terminal kgc, sem, client1, client2.

Step:2 Run all commands in all 4 terminals.

Step:3 KGC generate private key and splits it between client and SEM server.

Step:4 Enter message to be send and after sending message encryption time is calculated.

Step:5 After receiving message the client2 takes its private key from SEM server and decrypt the message.

Step:6 In this way we calculate decryption time and encryption time.

V. CONCLUSION

We know that our daily life is now become dependent on internet so it must be necessary to increase the safety of cloud computing.

Our present system is working under random oracle model. We know here our key is separated between SEM server and other client. So here our encryption time is less but decryption time is more. So we should work on this area to decrease decryption time.

REFERENCES

[1] "Simple Identity-Based Cryptography with Mediated RSA", Xuhua Ding, Gene Tsudik (2003), CT-RSA LNCS 2612, Pages 192-209.

[2] "Identity-based Broadcast Encryption Scheme with Untrusted PKG", Shanqing Guo, Chunhua Zhang (2008), The 9th International Conference for Young Computer Scientists, Pages 1613-1618.

[3] "Identity-Based Mediated RSA", Dan Boneh, Xuhua Ding, Gene Tsudik, June 2003

[4] Chu C K, Tzeng W G. "Identity-based proxy re-encryption without random oracles" In Proc. ISC2007, Valparaiso, Chile, Oct. 9-12, 2007, pp.189-202.

ISSN: 2321-8169
3049 - 3052

[5] "An Improved Identity-Based Encryption Scheme without Bilinear Map",Minghui Zheng, Huihua Zhou, Guohua Cui (2009)", International Conference on Multimedia Information Networking and Security, Pages 374-377.

[6] 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.

[7] 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.

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

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

[10] A. Shamir. Identity-based cryptosystems and signature schemes. In G. Blakley and D. Chaum, editors, Advances in Cryptology – CRYPTO '84, number 196 in Lecture Notes in Computer Science, pages 47–53. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 198