International Journal of Advancement in Engineering Technology, Management & Applied Science
Volume 2, Issue 10 October 2015 ISSN No: 2349-3224

Title
Security Related Issues for Cloud Computing

Ashwini Singh

Abstract:

The term CLOUD implies Common Location Independent Online Utility on Demand. It's a rising innovation in IT commercial ventures. Cloud advances are enhancing step by step and now it turn into a requirement for all little and substantial scale commercial ventures. Organizations like Google, Amazon, Microsoft and so on is giving virtualized environment to client by which it discards the requirement for physical stockpiling and others. At the same time, as the upside of distributed computing is expanding step by step the issues are additionally debilitating the IT commercial enterprises. These issues related with the security of the information. The essential thought of this survey paper is to expand the security issues related with distributed computing and what strategies are actualized to enhance these security. Certain calculations like RSA, DES, and Ceaser Cipher and so on actualized to enhance the security issues. In this paper we have executed Identity based mRSA calculation in this paper for enhancing security of information.

Keywords: ***WSN, Security; Network; Routing; Privacy***

I. INTRODUCTION:

In Modern Era, the entire work is presently moving towards the web. When we hear Cloud Computing then the idea of "ON-DEMAD" access of information and "VIRTUALIZATION" comes into psyche. Today the clients ought to have no worry about the server, physical capacity like RAM, Hard Disk, and CD and so forth to store the information. Cloud is isolated into two sections The Front part and the back part. The Front end incorporates "The clients and the clients". The client ought to have a gadget to get to the information and they ought to additionally have the web association

with the gadget and the second part incorporates the accumulation of different PCs, information stockpiling (like RAM, Hard circle and so on.) And server. They are joined with one another through web. All servers have their own autonomous working framework. Aside from back end and front end we additionally have an Administrator whose work is to check "Is everything going easily or not". It takes after some arrangement of tenets which are called Protocols and utilize an extraordinary sort of programming called Middle product.

Personality base encryption system uses client's character to make open keys and the private key is produced from this open key. After that private key is disseminated in the middle of client and SEM server. Thusly just verified client and SEM server have insight about the private keys. We accept here that SEM separate is not traded off.

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 is 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 ∈ 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.

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.

VI. 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.