Achieving Cloud Security through Multiplicative Homomorphic Algorithm by Adding Zero

Annwesha B Majumder
Department of Information Technology
JIS College Of Engineering,Kalyani, WestBengal,India

Dipak Kumar Shaw
Department of Information Technology
JIS College Of Engineering,Kalyani, WestBengal,India

Md. Shabbir Ahmad
Department of Information Technology
JIS College Of Engineering,Kalyani, WestBengal,India

Abstract- Cloud computing is an emerging trend in today's computing domain, where security is a major concern. Less maintenance, continuous availability, Scalability, Elasticity etc are main advantages of cloud computing. Data are being accessed over the web , that a makes cloud at big risk of different attacks on the users' data. In this paper we propose a multiplicative homomorphic algorithm in the field of cloud computing. With the help of the homomorphic encryption user and store encrypted data instead of raw data, and multiplication operation can also be done with encrypted data and then result can be decrypted.

Keywords – Cloud Computing, Homomorphic Encryption

I. INTRODUCTION

Cloud computing is a revolutionary invention in the field of computing model. It has changed the paradigm of computing. Cloud is a poll of resources that actually provides user the services in various dimension in a pay per use model. Collection of devices interconnected to each other can form a cloud where they can run parallel and provides huge computing power.

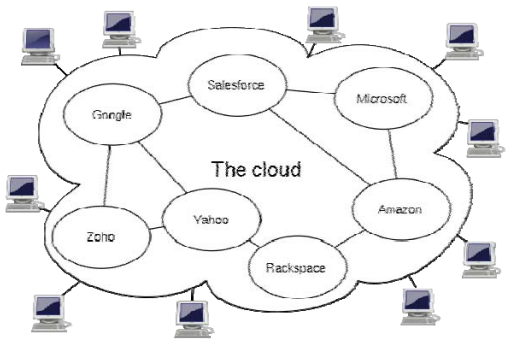

Figure 1. Cloud Computing model

NIST define cloud computing with five essential characteristics i.e. Broad network access, Rapid elasticity, Measured services, On demand self services and Resources pooling, three service models i.e. Software as a service,

Platform as a service and Infrastructure as a service and four deployment model i.e. public cloud, private cloud, community cloud and hybrid cloud.[1].

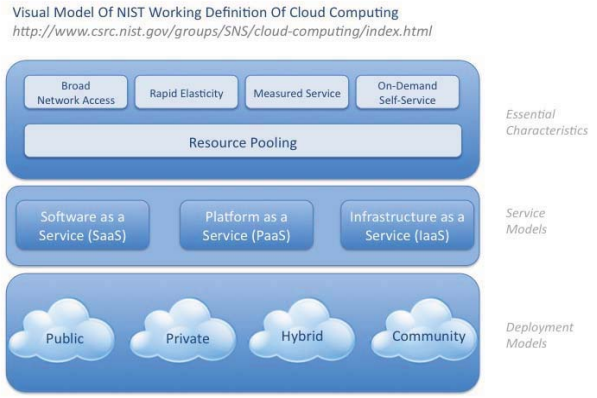

Figure 2. NIST Cloud Model

With the help of cloud computing the user are now need not be bother about the maintenance of resources software or hardware. This makes cloud so popular. At the same time security is a major concern in cloud as resources are being available over the web, so it is very vulnerable to security threats. Followings are the main cloud security threats:[2]

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Interfaces and APIs
3. Malicious Insiders
4. Shared Technology Issue
5. Data Loss or Leakage

Various encryption techniques are being proposed in this domain. 'Cell as Service' by using virtual machine where each several virtual machine runs on server consists of cell introduced by HP and "Virtual machine Introspection" introduced by IBM are two techniques applied to maintain security in cloud.[3]. Parsi Kalpana, Sudha Singaraju has applied RSA in cloud dopmian.[4]. Neha Jain and Gurpreet Kaur has applied DES algorithm in cloud environment to secure the data[5]. Hybrid symmetric encryption algorithm proposed by Dr. L. Arockiam, S. Monikandan use both substitution and transposition techniques for encryption.[6]. Identity based encryption technique is another approach in cloud security. Boneh and Franklin has proposed an efficient Identity based encryption technique in 2001[7]. Multi finger security model is a technique where users, during registration can register with three finger templates of their choice and assign a single digit number for each of these three fingers. These recorded images are encrypted using Elliptical algorithm and stored at the service provider's end [8].Private tongue recognition technique is also applied in cloud security[9].Data stored in cloud can also be secured through face matching.[10]. Sanjoli Singla, Jasmeet Singh has used the CHAP (Challenge-Handshake Authentication Protocol) for achieving data security and authentication in cloud.

Homomorphic encryption is another way that can be applied to achieve security over cloud. It was first proposed by Ronald Rivest, Leonard Adleman and Michael Dertouzos in the year of 1978[11]. Maha TEBAA et al also proposed a methods of encryption which was homomorphic.[12]. Reem Alattas has applied Algebraic Homomorphic Encryption Scheme based on Fermat's Little Theorem on cloud computing for better security.[13]

II. PROPOSED ALGORITHM

In this paper we propose a multiplicative homomorphic algorithm through with user data can be stored in encrypted form and operation of multiplication can also be done over encrypted data so the raw data will need not to be revealed.

$$E(d1d2) = E(d1)E(d2) \quad (1)$$

A. Encryption –

i. Store two numbers digit wise in an array.

Input: d1[n] and d2[m] where n1 and n2 are the number of digits of two numbers

ii. Add zero(0) at every even position of the number .

Encrypted_Number1=Ed1[n1]

Encrypted_ Number2=Ed2[n2]

Where n1=2*n and m1=2*m.

iii. Form two long number form the arrays.

D1 and D2 are two numbers after encryption

B. Multiplication operation over encrypted data –

i. Encrypted_Multiplication EM=D1*D2

C. Decryption –

A. i. Divide the encrypted multiplication with 100 to discard two extra zeroes in encrypted result.

Multiplication_Decryption1 M_D1=EM/100.

ii. Store the number digit wise in an array.

M_D2[n3] where n3 = number of digits.

iii. Start traversing the array M_D2 form (len-2) position. Store result in a list L.

Let initially h=len-2;

a. Add the current position value with its previous value.
m = M_D2[h]+M_D2[h-1] where initially i=2

b. If added value greater than 9 , then add the remainder to previous number and add 1 to the List L.
m1=m%10
m2=1;
L← m2.

c. Else add m in the List.
L← m.

Repeat the above steps until h<=0

d. Reverse the List L
Rev_L=Reverse(L)

e. Add M_D3[0] at the end of the Reverse List Rev_L

iv. Create a long number from the Rev_L. That is the actual multiplication result after decryption.

Actual Result=Multiplication_Decryption2 M_D2.

Dec[E(d1)*E(d2)]=Dec[EncryptedMultiplication]=d1*d2.

III. Experiment and Result

Following two figuares show the exteriment result over data 123,234 and 345 ,456.

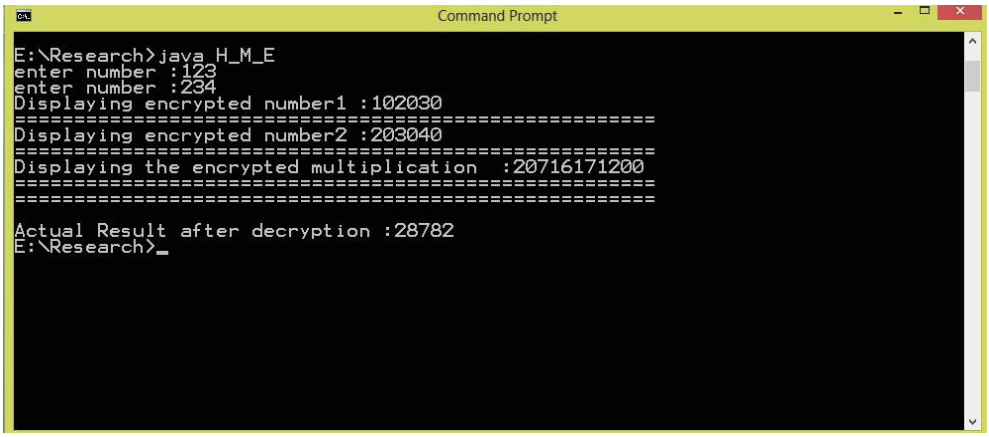

Figure 3. Test Result

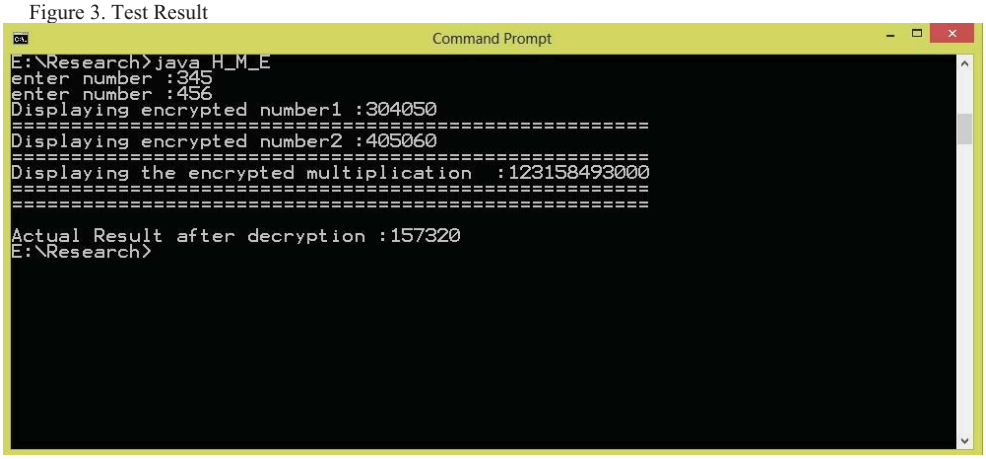

Figure 4. Test Result

IV.CONCLUSION

Cloud computing provides lots of advantages in domain of computing still struggling against security threats. Marinating data confidentiality is the huge concern of cloud. In this propose method can help a little in domain of cloud security tom achieve data confidentiality.

REFERENCES

[1] The NIST Definition of Cloud Computing NIST Special Publication 800-145

[2] Top Threats To Cloud Computing V1.0 Prepared by the Cloud Security Alliance March 2010

[3] G. Anthes. (2010, November). "Security in the Cloud." Communications of the ACM. Vol. 53, no 11. pp.16-18

[4] Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA http://www.mytestbox.com/miscellaneous/cloud computing-grid-computing-utility- computing-list-top-providers/

[5] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.

[6] Dr. L. Arockiam, S. Monikandan Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[7] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Proceedings of Cryptography 2001, LNCS 2139, pages 213–229, Springer-Verlag, 2001

[8] Multiple Biometric Security in Cloud Computing D.Pugazhenthi, PG and Research Department of Computer Science, Quaid-E-Millath College for Women, Chennai, India B.Sree Vidya, Research Scholar, Bharathiyar University, Coimbatore, India
International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[9] Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security Sowmya Suryadevara, Shuchita Kapoor, Shweta Dhatterwal, Rohaila Naaz and Anan Sharma 2011 International Conference on Information and Network Technology IACSIT Press, Singapore 73 IPCSIT vol.4 (2011) © (2011)

[10] Secure Data Storage in Cloud Environment Using Biometrics K.Govind Yannick Ngabirano International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 5, May 2012 ISSN: 2277 128X

[11] Ronald L. Rivest, Leonard Adleman, and Michael L. Dertouzos. On Data Banks and Privacy Homomorphisms, chapter On Data Banks and Privacy Homomorphisms, pages 169-180. Academic Press, 1978.

[12] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol 1 WCE 2012, July 4 - 6, 2012, London, U.K

[13] Reem Alattas Cloud Computing Algebraic Homomorphic Encryption Scheme International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 8 No. 2 Sep. 2014, pp. 191-195

[14] Sanjoli Singla, Jasmeet Singh Cloud Data Security using Authentication and Encryption Technique International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013