IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 2 (Jan. - Feb. 2013), PP 46-50
www.iosrjournals.org

Fully homomorphic encryption equating to cloud security: An approach

[1]Bhabendu Kumar Mohanta, [2]Debasis Gountia
[1,2]CET, Bhubaneswar

Abstract: *As the data storage challenge continues to grow for insurers and everyone else, one of the obvious solutions is cloud technology. Storing data on remote servers rather than in-house is definitely a money-saver, but in insurance circles, the worry has been that having critical data reside outside the physical and virtual walls of the insurance enterprise is a risky situation. As the IT field is rapidly moving towards Cloud Computing, software industry's focus is shifting from developing applications for PCs to Data Centers and Clouds that enable millions of users to make use of software simultaneously.*

"Attempting computation on sensitive data stored on shared servers leaves that data exposed in ways that traditional encryption techniques can't protect against," the article notes. "The main problem is that to manipulate the data, it has to be decoded first". Now a new method, called fully homomorphic encryption (FHE) that performs computation with the encrypted data and send to the client and offers a realistic hope that such calculations can be performed securely in the cloud.

Keywords: *Cloud computing, fully homomorphic encryption, security threats.*

I. Introduction

"Homomorphic" is an adjective which describes a property of an encryption scheme. That property, in simple terms, is the ability to perform computations on the cipher text without decrypting it first.

Our ultimate goal is to used a fully homomorphic encryption scheme $_E$. Let us discuss what it means to be fully homomorphic. At a high-level, the essence of fully homomorphic encryption is simple: given cipher texts that encrypt $m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_t$, fully homomorphic encryption should allow anyone (not just the key-holder) to output a cipher text that encrypts $f(m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_i)$ for any desired function f, as long as that function can be efficiently computed. No information about $m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_t$ or $f(m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_t)$ or any intermediate plaintext values, should leak; the inputs, output and intermediate values are always encrypted.

Formally, there are different ways of defining what it means for the final cipher text to "encrypt" $f(m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_i)$. The minimal requirement is correctness. A fully homomorphic encryption scheme *E* should have an efficient algorithm $Evaluate_E$ that, for any valid $_E$ key pair (sk; pk), any circuit C, and any cipher texts $\Psi i \leftarrow Encrypt_E (pk;m_i)$ outputs

$\Psi \leftarrow Evaluate_E (pk; C; \Psi_1 \Psi_2 \Psi_3\ldots\ldots\ldots.. \Psi_t)$ such that

$Decrypt_E (sk;\Psi)=C(m_1,m_2,m_3,\ldots\ldots\ldots\ldots\ldots\ldots m_{t)}$.

Security threats in cloud

Cloud computing as a concept is the result of the natural evolution of our everyday approach to using Technology delivered via the Internet. Cloud computing came into the foreground as a result of advances in virtualization (e.g. VMWare) [1], distributed computing with server clusters (e.g. Google) [2] and increase in the availability of broadband Internet access. Industry leaders describe cloud computing simply as the delivery of applications or IT services, which are provided by a third party over the Internet (Rackspace, Microsoft, IBM) [3, 4,5]. Ironically, the recent global economic recession served as a booster for interest in cloud computing technologies as organizations sought for ways to reduce their IT budget, while keeping up with performance and profits [6]. The cloud computing buzz began in 2006 with the Launch of Amazon EC2, gaining traction in 2007 as seen in the Figure 1.

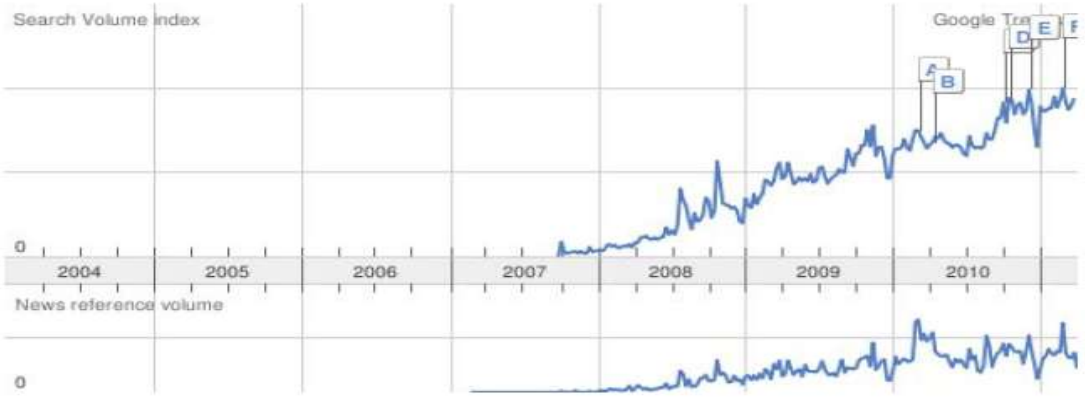

Figure 1: Search and News Volume for Cloud Computing as at April 2011

The National Institute of Standards and Technology defines cloud computing as follows: "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." [7]
Cloud computing is currently characterized by having an on demand access to elastic resources via a tenancy model.

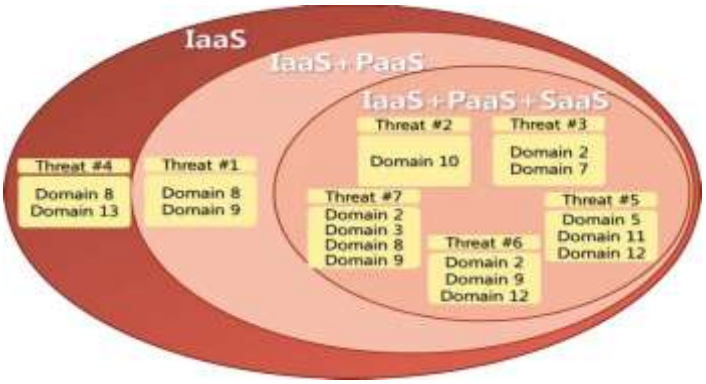

Figure 2. Security Threats and Domains

According to reports of CSA (Cloud Security Alliance), the 13 security domains [18] and the 7 top threats [17] on cloud computing were defined as follows Table 1 and Table 2.

Table 1. Security domains in cloud computing

No	**Domain definition**
1	Cloud Computing Architectural Framework
2	Governance and Enterprise Risk Management
3	Legal and Electronic Discovery
4	Compliance and Audit
5	Information Lifecycle Management
6	Portability and Interoperability
7	Traditional Security, Business Continuity, and Disaster Recovery
8	Data Center Operations
9	Incident Response, Notification, and Remediation
10	Application Security
11	Encryption and Key Management
12	Identity and Access Management
13	Virtualization

Table 2. Threats in cloud computing security

No	Threat definition
1	Abuse and Nefarious Use of Cloud Computing
2	Insecure Interfaces and APIs
3	Malicious Insiders
4	Shared Technology Issues
5	Data Loss or Leakage
6	Account or Service Hijacking
7	Unknown Risk Profile

Related Homomorphic Encryption Algorithm

If all data stored in the cloud were encrypted, that would effectively solve issues like Availability, Data Security, and Third-Party Control. However, a user would be unable to leverage the power of the cloud to carry out computation on data without first decrypting it, or shipping it entirely back to the user for computation. The cloud provider thus has to decrypt the data first (nullifying the issue of privacy and confidentiality), perform the computation then send the result to the user. What if the user could carry out any arbitrary computation on the hosted data without the cloud provider learning about the user's data - computation is done on encrypted data without prior decryption. This is the promise of homomorphic encryption schemes which allow the transformation of cipher texts *C(m)* of message m, to cipher texts *C(f(m))* of a computation/function of message m, without disclosing the message.

The idea was first suggested by Rivest, Adleman and Dertouzos in 1978, referred to as privacy homomorphisms [9]. RSA (invented by Rivest, Shamir and Adleman '78) [10] had multiplicative homomorphism (you could compute a cipher text which is the product of plaintexts) and over the next 30 years, researchers such as Yao '82 [11], Goldwasser and Micali '82 [12], ElGamal '85 [12 - 33] and Paillier [14] came up with partially homomorphic cryptosystems. A survey of homomorphic encryption schemes can be found in [15,16].

An encryption scheme can be said to be fully homomorphic if:

$E(M_1 \Theta M_2) \leftarrow E(M_1) \Theta E(M_2)$; Where for all $M_1, M_2 \in M$. M is the set of plain text.

After the development of fully homomorphic encryption from partially homomorphic encryption, now we can compute the encrypted data into the cloud without knowing the secret key. Few developed FHE scheme listed below.

- GENTRY'S FHE using ideal lattice
- Van Dijk Et al, fully homomorphic encryption over the integer
- FHE based on approximate matrix GCD

Implementing FHE algorithm into Cloud Environment

Applying fully homomorphic encryption we can assure data secure for cloud computing. The key concept is that the data is encrypted by homomorphic encryption and stored in cloud server, through this we can get the big benefit: deal with the cipher text directly in server and assure the data's security because anyone else who doesn't know the key can't decrypt it. We use homomorphic symmetric encryption [8] to construct the data secure scheme.

The symmetric homomorphic encrypt scheme:

Select encrypt parameter: r, p and q, $r \sim 2^n$, $p \sim 2^{n2}$, $q \tilde{} 2^{n5}$ and p is prime

P is the secret key

Encrypt: for plain text m

Compute $c=pq+2r+m$ where c is the cipher text

Decrypt: $m=(c \bmod p) \bmod 2$

Correctness: because pq is larger than 2r+m so $(c \bmod p) = 2r+m$

Finally $(c \bmod p) \bmod 2 = (2r+m) \bmod 2 = m$

Homomorphic: for two cipher text

$C_1=q_1p+2r_1+m_1$

$C_2=q_2p+2r_2+m_2$

Compute:

$C_1 + C_2 = (q_1+q_2)\, p+2(r_1+r_2) +m_1+m_2$

So if $2(r_1+r_2) +m_1+m_2 << p$

Then $(c_1+c_2) \bmod p = 2(r_1+r_2) +m_1+m_2$

So its additive homomorphic.

And $c_1 * c_2 = [q_1 * q_2 p + (2r_1+m_1) + (2r_2+m_2)]\, p+2(2r_1\, r_2+r_1 m_1+r_2\, m_1) +m_1\, m2$

So if $2(2r_1\ r_2+r_1m_1+r_2\ m_1) +m_1\ m2<<p$
Then
$(c_1*c_2)\ \text{mod}\ p=2(2r_1\ r_2+r_1m_1+r_2\ m_1) +m_1\ m2$

Apply above encrypt scheme, we design the following cloud data secure scheme:

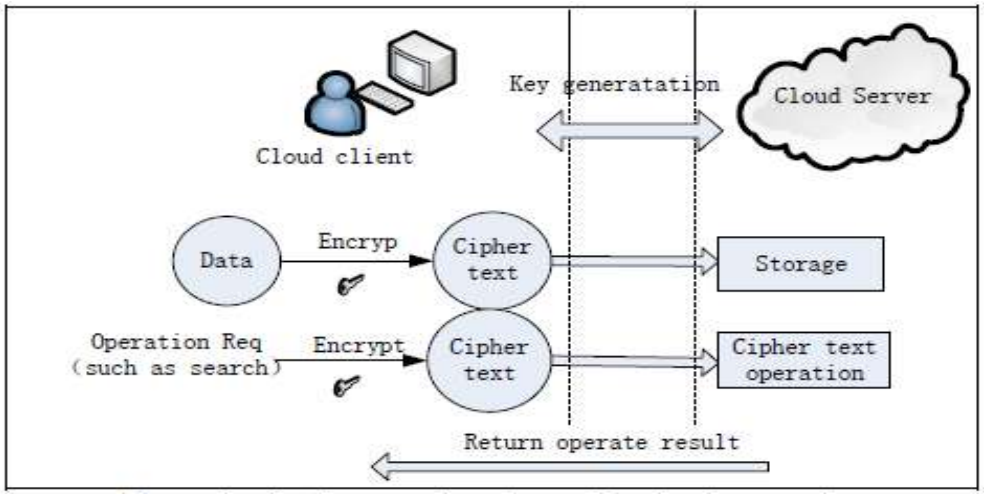

Fig 3. The data security scheme for cloud computing

As the figure 3 show, our scheme uses symmetric homomorphic encrypt to enhance data security. First, the user login and the server assign a key-generation seed to user; then user generate the secret key at client using this seed, so the server don't know the secret key at all. This procedure can be repeated then it enables the user get the same secret key at any time. Secondly the user can use this key to encrypt data which the user wants to transmit and save it in the cloud server. While transmitting also other cryptograph technology such as digital signature can applied to assure the integrity and nonrepudiation. At last, the user can send request to cloud server (also encrypted) and the server do the operation even without know the content of the operation. With this scheme, not only the stored data but also the transmitted data is encrypted, so we don't worry about the data is eavesdropped or stolen. It also can provide secure data audit service because the third audit party can deal with the encrypted data directly. And the encryption we use is symmetry so we can compute it with less MIPS which are very important for thin client.

II. Conclusion:

In this paper we have analyzed the different security issue present .when client send information to the server in encrypted form to perform any computational operation to that encrypted data server need the private key from the client. If client give that private key then the privacy is not ensured, again how to ensure that nobody will perform any unauthenticated operation with the data. In this paper we have given some fully homomorphic encryption scheme developed by researchers which allow us to perform computation on encrypted data without using secret key of client. It is nothing but a new layer applied to the cloud computation.

Future Work:

As cloud computing is a large area and use of cloud computing is increasing daily. Again cloud having 3 service model that are software as a service (saas), platform as a service (paas), and infrastructure as a service (iaas) so everyone is looking to move into the cloud as it give more flexibility and reduced cost. Here we have implement fully homomorphic encryption scheme where all type of operation are can be performed without knowing secret key. The main defect of this scheme is that after encrypt the size of data become very large which will cause heavy burden for network and storage.

Reference:

[1] Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2011, available at: http://www.vmware.com/pdf/virtualization.pdf
[2] Web Search For A Planet: The Google Cluster Architecture. Retrieved April 6, 2011, available at: http://labs.google.com/papers/googlecluster-ieee.pdf
[3] What is Cloud. Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/whatis- cloud/
[4] What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.microsoft.com/business/engb/ solutions/Pages/Cloud.aspx
[5] What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.ibm.com/developerworks/cloud/newto.html#WHATIS

[6] Recession is good for cloud computing – Microsoft agrees - http://www.cloudave.com/2425/recession-is-goodfor- cloud-computing-microsoft-agrees/
[7] National Institute of Standards and Technology - Computer Security Divisionhttp://csrc.nist.gov/groups/SNS/cloud-computing/
[8] Bhaskar P., Admela J·, Dimitrios K·, Yves G.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. J. Grid Computing 9(1), 3-26 (2011)
[9] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.
[10] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. In Comm. of the ACM, 21:2, pages 120–126, 1978
[11] A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.
[12] S. Goldwasser and S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984
[13] T. ElGamal, "A prublic key cryptosystem and a signature scheme based on discrete logarithms," in Advances in Cryptology (CRYPTO '84), vol. 196 of Lecture Notes in Computer Science, pp. 10–18, Springer, New York, NY, USA, 1985.
[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT '99), vol. 1592 of Lecture Notes in Computer Science, pp. 223–238, Springer, New York, NY, USA, 1999.
[15] C. Fontaine , F. Galand, A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007, p.1-15, January 2007
[16] D. Micciancio and O. Regev. Post-Quantum Cryptography, chapter Lattice-based Cryptography. Springer, 2008
[17] Cloud Security Alliance, Top Threats To Cloud Computing V1.0, http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
[18] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/csaguide.pdf.