A Survey of the Homomorphic Encryption Approach for Data Security in Cloud Computing

Ms.Parin.V.Patel
C.S.E. Department, GIT Gandhinagar
patelparinv@gmail.com

Mr Hitesh D Patel
C.S.E. Department, GIT Gandhinagar
hitupatel2002@gmail.com

Abstract— In present days cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet. But there is a big problem of security in cloud computing. When client is providing their data to the cloud because of security they use different encryption and decryption algorithms. Through these algorithms we can provide security to client's data on the cloud. In this survey paper we are discussing the approach of homomorphic encryption which provides security in cloud computing. Homomorphic encryption is the method which performs operation on encrypted data which will provide result without decrypting that data. This method provides the same result as operation performs on row data.

Index Terms— Cloud Computing, security, Homomorphic Encryption, RSA

I. INTRODUCTION

The term "cloud" originates from the world of telecommunications when providers began using virtual private network (VPN) services for data communications [1]. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "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. [2]".So through this cloud computing there is no need to store the data on desktops, portables etc.You can store the data on servers and you can access the data through internet.

Cloud computing provides better utilization of distributed resources over a large data and they can access remotely through the internet.

.

II. HISTORY

The underlying concept of cloud computing was introduced way back in 1960s by John McCarthy. His opinion was that "computation may someday be organized as a public utility [3]". Also the characteristics of cloud computing were explored for the first time in 1966 by Douglas Parkhill in his book, The Challenge of the Computer Utility[3].

The history of the term cloud is from the telecommunications world, where telecom companies started offering Virtual Private Network (VPN) services with comparable quality of service at a much lower cost. Initially before VPN, they provided dedicated point-to-point data circuits which were wastage of bandwidth. But by using VPN services, they can switch traffic to balance utilization of the overall network. Cloud computing now extends this to cover servers and network infrastructure [4].

Many players in the industry have jumped into cloud computing and implemented it. Amazon has played a key role and launched the Amazon Web Service (AWS) in 2006. Also Google and IBM have started research projects in cloud computing. Eucalyptus became the first open source platform for deploying private clouds [4].

III. CLOUD ARCHITECTURE

Cloud computing system is divided into two sections: the front end and the back end. Front end through which user can interact with the server and backend is the server which provides data to the client. Between server and client network is working as middleware.

IV. LAYERS AND SERVICES OF CLOUD COMPUTING ARCHITECTURE

The below diagram shows the different layers of cloud Computing architecture [3].

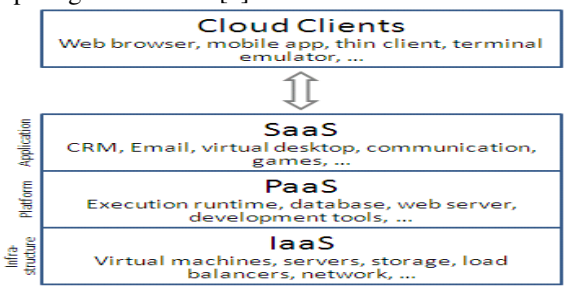

Figure1.Layers and services of Cloud Computing[3]

A cloud client consists of computer hardware and/or computer software which relies on cloud computing for application delivery, or that is specifically designed for delivery of cloud services [9].

(Cloud) Infrastructure as a Service (IaaS) is also referred as Resource Code, provide (managed and scalable) resources as services to the user- in other words, they basically provide enhanced virtualization capabilities. Accordingly, different resources may be provided via a service interface [5].

(All right reserved by www.ijedr.org)

(Cloud) Platform as a Service (PaaS) is provides computational resources via a platform upon which applications and services can be developed and hosted. Example: Google Docs, SAP business by design [5].

(Clouds) Software as a Service (SaaS) is also sometimes referred to as Service or application clouds. These clouds are offering implementation of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications/services using a cloud. infrastructure or platform, rather than providing cloud features themselves [5].

V. Deployment of Cloud Computing Service

For deploying a cloud computing solution, the major task is to decide on the type of cloud to be implemented. Presently three types of cloud deployment takes place - public cloud, private cloud and hybrid cloud Figure below shows the overview of the deployment of these three clouds [6]:

Public cloud allows the user to access cloud via network. This cloud is publicly available on internet so security is the big problem. In this cloud upgradation and maintenance is difficult. This cloud is on "Pay and Use" basis. You need to pay only the time duration that you have use.

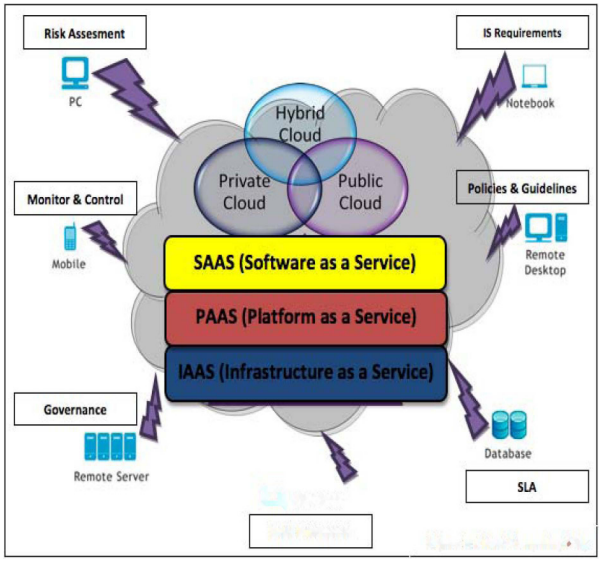

Figure 2.Deployment of Cloud Services[6]

Private Cloud is within an organization. This stores the internal data of organization. It is more secure and maintenance is also easy. Only the internal user can access that data.

The Hybrid Cloud is a combination of any two (or all) of the three models discussed above. Standardization of APIs has lead to easier distribution of applications across different cloud models. This enables newer models such as "Surge Computing" in which workload spikes from the private cloud is offset to the public cloud [7].

Community cloud is constructed by many organizations according to their requirements. Cloud infrastructure is managed by third party or one of the organizations.

VI. Homomorphic Encryption

Homomorphic encryption alludes to encryption where plain texts and cipher texts both are treated with an equivalent algebraic function. Now the plain text and cipher text might also be not related but the emphasis is on the algebraic operation that works on both of them [5].

Structured Encryption: A structured encryption scheme encrypts structured data in such a way that it can be queried through the use of a query-specific token that can only be generated with knowledge of the secret key. In addition, the query process reveals no useful information about either the query or the data. An important consideration in this context is the efficiency of the query operation on the server side [5].

Homomorphic encryption [8] allows operations on encrypted data; thus, cloud servers may use encrypted data without access to the original data. Figure 3 shows the general framework. Homomorphic encryption is considered too expensive and remains an academic curiosity [8].

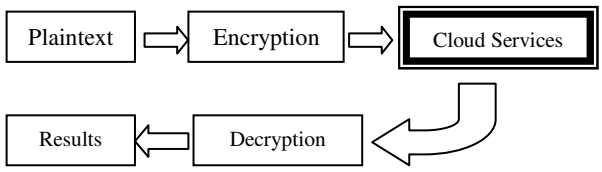

Figure 3. A general framework for cloud service with data protection[8]

Data are encrypted before being sent to the cloud server. The server performs computation on the encrypted data. The results are obtained by decrypting the data from the server. The solid lines represent the data owner; the dashed line means the server is not trusted [8].

Below Figure 2(a) and (b) illustrate the concept of homomorphic encryption. Suppose x =< x1; x2; ..; xn >

is a sequence of n elements as the original unprotected data, also called plaintext. An operation f can be performed on x to obtain result r = f(x) =< r1; r2;….; rm >. Let y =< y1; y2; ….; yn > be the corresponding ciphertext; y =< e(x1); e(x2);……; e(xn) > and e is the encryption operation. We can obtain x through decryption x = d(y). We call the encryption and the operation homomorphic if d(f(y)) = r. In other words, the same operation can be applied to encrypted data and the result can be obtained after decryption, as illustrated in Figure 2(b). Homomorphic encryption is not another encryption algorithm (like AES or RSA). Instead, it is a property of some encryption algorithms; some encryption algorithms cannot be homomorphic, for example, if they are non-malleable [8]. The encryption algorithm illustrated in Figure 2 (b) is deterministic: for a plaintext x, a unique ciphertext y is created. Many encryption algorithms are non-deterministic: a plaintext x may be mapped to one of many possible ciphertexts. Non-deterministic encryption can provide better protection because it is difficult to know whether two different y's correspond to the same x. This is illustrated in Figure 2 (c). The sidebar Example of Homomorphic Encryption using Non-Deterministic Encryption gives a numeric example. The sidebar also shows an example when h(x) = x3 produces a

(All right reserved by www.ijedr.org)

wrong result for x =< x1 >=< 2 >, illustrated by point a in Figure 2(d) [9].

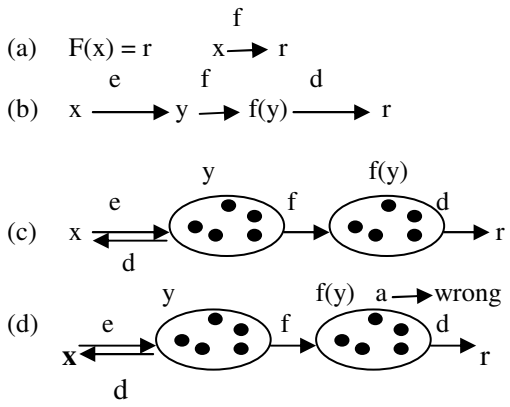

Figure 4. Overview of homomorphic encryption.

VII. ADDITIVE HOMOMORPHIC ENCRYPTION

A Homomorphic encryption is additive, if: [10]

$Enc(x \oplus y) = Enc(x) \otimes Enc(y)$

$$Enc\left(\sum_{i=1}^{l} mi\right) = \prod_{i=1}^{l} Enc(mi)$$

Example: Paillier Cryptosystem (1999):

Suppose we have two ciphers C1 et C2 such that:

$C1 = g^{m1} \cdot r1^n \bmod n^2$

$C2 = g^{m2} \cdot r2^n \bmod n^2$

$C1.C2 = gm1.r1^n.g^{m2}.r2^n \bmod n^2 = g^{m1+m2} (r1r2)^n \bmod n^2$

So, Pailler cryptosystem realizes the property of additive Homomorphic encryption. An application of an additive Homomorphic encryption is electronic voting: Each vote is encrypted but only the "sum" is decrypted [10].

Key Generation: KeyGen(p,q)	
Input: $p,q \in \mathbb{P}$	
Compute	$n = pq$
Choose $g \in \mathbb{Z}^*_{n^2}$ such that	$\gcd(L(g^\lambda \bmod n^2), n) = 1$ with $L(u) = \frac{u-1}{n}$
Output: (pk, sk) public key: $pk = (n, g)$ secret key: $sk = (p, q)$	

Encryption: Enc(m, pk)	
Input: $m \in \mathbb{Z}_n$	
Choose	$r \in \mathbb{Z}^*_n$
Compute	$c = g^m \cdot r^n \bmod n^2$
Output: $c \in \mathbb{Z}_{n^2}$	

Decryption: Dec(c, sk)	
Input: $c \in \mathbb{Z}_{n^2}$	
Compute	$m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$
Output: $m \in \mathbb{Z}_n$	

Figure 5. Paillier Algorithm[9]

VIII. MULTIPLICATIVE HOMOMORPHIC ENCRYPTION

A Homomorphic encryption is multiplicative, if: [10]

$Enc(x \otimes y) = Enc(x) \otimes Enc(y)$

$$Enc\left(\prod_{i=1}^{l} mi\right) = \prod_{i=1}^{l} Enc(mi)$$

Example: RSA Cryptosystem (1978)

Key Generation: KeyGen(p,q)	
Input: $p,q \in \mathbb{P}$	
Compute	$n = p \cdot q$ $\varphi(n) = (p-1)(q-1)$
Choose e such that	$\gcd(e, \varphi(n)) = 1$
Determine d such that	$e \cdot d \equiv 1 \bmod \varphi(n)$
Output: (pk, sk) public key: $pk = (e, n)$ secret key: $sk = (d)$	

Encryption: Enc(m, pk)	
Input: $m \in \mathbb{Z}_n$	
Compute	$c = m^e \bmod n$
Output: $c \in \mathbb{Z}_n$	

Decryption: Dec(c, sk)	
Input: $c \in \mathbb{Z}_n$	
Compute	$m = c^d \bmod n$
Output: $m \in \mathbb{Z}_n$	

Figure 5. RSA Algorithm[10]

Suppose we have two ciphers C_1 et C_2 such that:

$C1 = m1^e \bmod n$

$C2 = m2^e \bmod n$

$C_1.C_2 = m1^e\, m2^e \bmod n = (m1m2)^e \bmod n$

RSA cryptosystem realize the properties of the multiplicative Homomorphic encryption, but it still has a lake of security, because if we assume that two ciphers C_1, C_2 corresponding respectively to the messages m_1, m_2, so:

$C1 = m1^e \bmod n$

$C2 = m2^e \bmod n$

The client sends the pair $(C_1.C2)$ to the Cloud server, the server will perform the calculations requested by the client and sends the encrypted result $(C_1 \times C_2)$ to the client[10].

If the attacker intercepts two ciphers C_1 et C_2, which are encrypted with the same private key, he/she will be able to decrypt all messages exchanged between the server and the client. Because the Homomorphic encryption is multiplicative, i.e. the product of the ciphers equals the cipher of the product [10].

(All right reserved by www.ijedr.org)

IX. Conclusion

In this paper we have survey on various homomorphic encryption schemes. In a cloud computing fully homomorphic based security is new concept. In this concept client encrypt the data using client's private key and that encrypted data is received by the server. Without decrypting that data server performs the operation and sends result back to the client. Now client decrypt that data and get the result.

So, security problem is overcome through this Homomorphic algorithm. Data confidentiality is managed by this algorithm.

X. References

[I] John Harauz, Lorti M. Kaufinan. Bruce Potter, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Copublished by the IEEE Computer and Reliability Societies, July/August 2009.

[2] National Institute of Standards and Technology- Computer Security Resource Center -www.csrc.nist.gov

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4] Yashpalsinh Jadeja and Kirit Modi, "Cloud Computing - Concepts, Architecture and Challenges", International Conference on Computing, Electronics and Electrical Technologies [ICCEET], IEEE-2012

[5] Samerjeet kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, VSRD-IJCSIT, Vol. 2 (3), 2012

[6] Ramgovind S, Eloff MM, Smith E, 'The management of security in cloud computing", IEEE – 2010

[7] Aderemi A. Atayero and Oluwaseyi Feyisetan," Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption" Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011

[8] Caroline Fontaine and Fabien Galand,"A Survey of Homomorphic Encryption for Nonspecialists",EURASIP Journal on Information Security, pages 1 to15, January 2007.

[9] Jibang Liu, Yung-Hsiang Lu and Cheng-Kok Koh," Performance Analysis of Arithmetic Operations in Homomorphic Encryption", *ECE Technical Reports* Paper 404, 2010

[10] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI,"Homomorphic Encryption Applied to the Cloud omputing Security", Proceedings of the World Congress on Engineering, Vol I, London, U.K. July 4 - 6, 20

(All right reserved by www.ijedr.org)