International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 6; Issue: 3; March -2017

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

Dhananjaya .V
Asst.Prof,CSEDept, SKIT, Bengaluru, Karnataka, India

Dr.Balasubramani .R
Prof & HOD,ISE Dept, NMAMIT, Nitte. Karnataka, India

Dr.JagadeeshGowda .K .S
Prof & HOD, CSE Dept, SKIT, Bengaluru, Karnataka, India

Naveen Ghorpade
Asst.Prof,CSEDept, SKIT, Bengaluru, Karnataka, India

Abstract: In present days dispersed figuring is one of the best stages which gives stockpiling of data into a great degree cut down cost and open for untouched over the web. Regardless, there is a noteworthy issue of security in disseminating registering. Exactly when the client is giving their data to the cloud by virtue of security they use various encryption and unscrambling estimations. Through these figurings we can offer security to client's data on the cloud. In this diagram paper, we are discussing the approach of homomorphic encryption, which gives security in appropriated processing. Homomorphic encryption is the technique which performs operation on mixed data which will give happen without unscrambling that data. This methodology gives an unclear result from operation performs on line data.

Keywords- Cloud Computing, Security, Homomorphic Encryption, RSA

I. INTRODUCTION

The expression "cloud" starts from the universe of media interchanges when providers began using a virtual private framework (VPN) organizations for data correspondences [1]. The significance of disseminated registering gave by the National Establishment of Standards and Technology (NIST) says that: "Circulated processing is a model for enabling accommodating, on demand campus access to a typical pool of configurable figuring resources (e.g., frameworks, servers, stockpiling applications and organizations) that can be immediately provisioned and released with immaterial organization effort or pro center correspondence. [2]". So through this appropriated processing there is no compelling reason to store the data on desktops, portables, etc.. You can store the data on servers and you can get to the data through the web. Distributed registering gives better use of passed on resources over a gigantic data and they can get to remotely through the web.

II. HISTORY

The concealed thought of appropriated processing was exhibited course in the 1960s by John McCarthy. His decision was that "figuring may eventually be made as an open utility [3]". In like manner the traits of dispersed processing were examined unprecedented in 1966 by Douglas Parkhill in his book, The Challenge of the Computer Utility [3]. The recorded setting of the term cloud is from the communicate correspondences world, where telecom associations started offering Virtual Private Network (VPN) organizations with the equivalent nature of the organization at a much lower cost. At first, before VPN, they gave submitted demonstrate point data circuits which were wastage of transmission limit. In any case, by using VPN, organizations, they can change development to alter utilization of

the general framework. Circulated registering now extends this to cover servers and framework establishment [4]. Numerous players in the business have bounced into cloud figuring and completed it. Amazon has expected a key part in addition, moved the Amazon Web Service (AWS) in 2006. Excessively Google and IBM have started to investigate endeavors in cloud preparing. Eucalyptus transformed into the primary open source arrange for passing on private fogs [4].

III. CLOUD ARCHITECTURE

Appropriated processing system is confined into two ranges: the front end and the back end. Front end through which customer can participate with the server and backend is the server which offers data to the client. Among server and client orchestrate is filling in as middleware.

IV. LAYERS AND SERVICES OF CLOUD COMPUTING ARCHITECTURE

The beneath outline demonstrates the diverse layers of cloud Processing engineering [3].

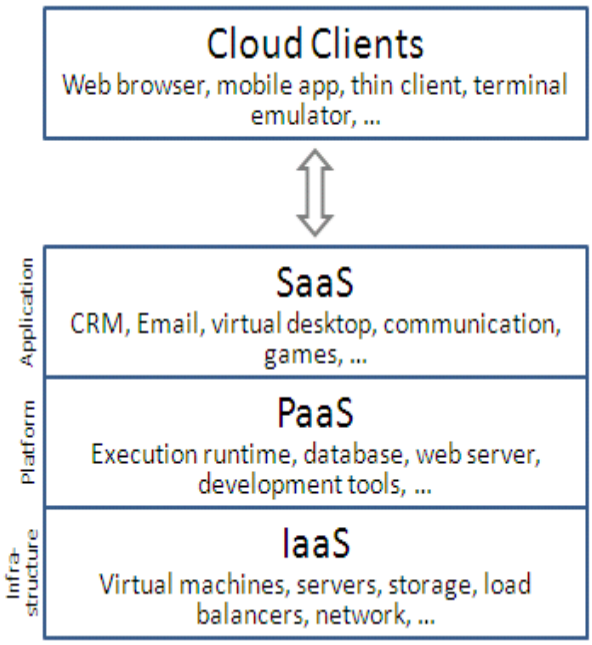

Figure1.Layers and services of Cloud Computing [3]

A cloud client involves PC gear and in addition PC programming which relies on upon dispersing figuring for application movement, or that is especially expected for transport of cloud organizations [9]. (Cloud) Infrastructure as a Service (IaaS) is in like manner insinuated as Resource Code, give (managed and flexible) resources as organizations to the customer thusly, they on a very basic level give overhauled virtualization limits. In like manner, unprecedented resources may be given by method for an organization interface [5].

(Cloud) Platform as a Service (PaaS) gives computational resources by method for a phase whereupon applications and organizations can be created and facilitated. Illustration: Google Docs, SAP business by blueprint [5].

(Fogs) Software as a Service (SaaS) is in like manner at times insinuated as a Service or application fogs. These fogs are putting forth use of specific business limits and business frames that are outfitted with specific cloud capacities, i.e. they give applications/organizations using a cloud. System or stage, instead of giving cloud highlights themselves [5].

V. DEPLOYMENT OF CLOUD COMPUTING SERVICE

For sending an appropriated figuring game plan, the genuine task is to settle on the kind of cloud to be realized. Before long three sorts of cloud association happens - open cloud, private cloud and crossbreed cloud Figure underneath shows the chart of the course of action of these three fogs [6]: Open cloud allows the customer to get the opportunity to cloud by a method for mastermind. This cloud is uninhibitedly open on the web so security is the gigantic issue. In this cloud upgradation and upkeep is troublesome. This cloud is on "Pay and Use" preface. You need to pay only the time length that you have used.

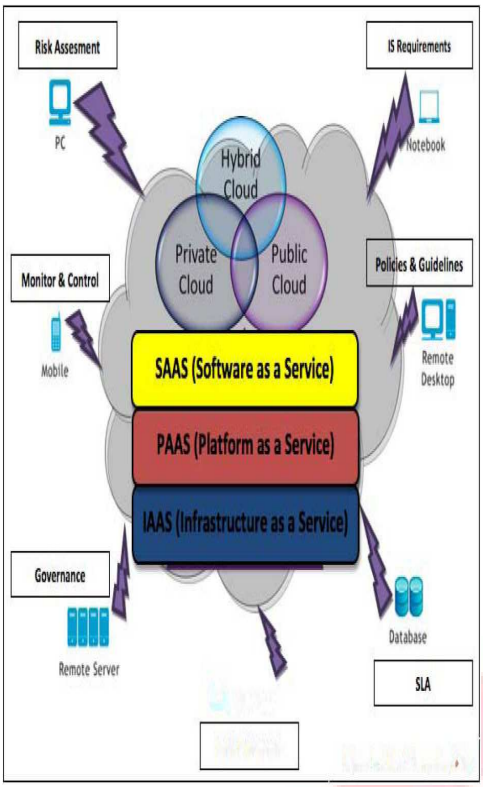

Figure 2. Deployment of Cloud Services [6]

Private Cloud is inside an affiliation. This stores within the date of affiliation. It is more secure and support is furthermore straightforward. Simply the internal customer can get to that data.

The Hybrid Cloud is a mix of any two (or all) of the three models discussed previously. Systematization of APIs has provoked to less complex assignment of usages transversely over different cloud models. This enables more present models, for instance, "Surge Registering" in which workload spikes from the private cloud is counteracting the overall public cloud [7].

Aggregate cloud is created by various relationships as shown by their necessities. Cloud system is regulated by untouchable or one of the affiliations.

VI. HOMOMORPHIC ENCRYPTION

Homomorphic encryption infers encryption where plain messages and figure works both are treated with an equivalent logarithmic limit. By and by the plain substance and figure substance may moreover be not related yet rather the highlight is on the arithmetical operation that takes them to [5].

Sorted out Encryption: A composed encryption scheme scrambles sorted out the data in a way that it can be addressed utilizing a request specific token that must be done with learning of the secret key. Besides, the request gets ready reveals no accommodating information about either the request or the data. A key thought in this setting is the profitability of the request operation on the server side [5].

Homomorphic encryption [8] grants operations on mixed data; as needs be, cloud servers may use encoded data without access to the primary data. Figure 3 exhibits the general structure. Homomorphic encryption is considered also exorbitant and remains an academic intrigue [8].

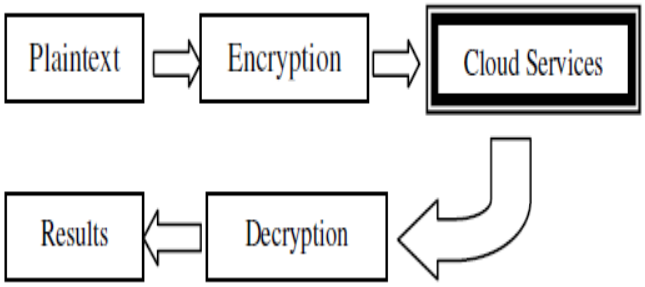

Figure 3. A general framework for cloud service with data protection [8]

The information is scrambled before being sent to the cloud server. The server performs calculation on the scrambled information. The outcomes are gotten by decoding the information from the server. The strong lines speak to the information proprietor; the dashed line implies the server is not put stock in [8].

Beneath Figure 2 (a) and (b) represent the idea of homomorphic encryption. Assume x =< x1; x2; ..; Xian >is a grouping of n components as the first unprotected data, also called plaintext. An operation f can be performed on x to get result r = f (x) =< r1; r2;… .; rm>. Let my =< y1; y2; … .; in > be the relating ciphertext; y =< e (x1); e

(x2);……; e (Xian) > and e is the encryption operation. We can acquire x through unscrambling x = d (y). We call the encryption and the operation homomorphic if d (f (y)) = is. As such, a similar operation can be connected to encode information and the outcome can be gotten after decoding, as shown in Figure 2 (b). Homomorphic encryption is not another encryption algorithm (like AES or RSA). Rather, it is a property of some encryption calculations; some encryption calculations can't be homomorphic, for instance, on the off chance that they are non-pliable [8]. The encryption calculation outlined in Figure 2 (b) is deterministic: for a plain text x, a remarkable ciphertext y is made. Numerous encryption calculations are non-deterministic: a plain text x might be mapped to one of numerous conceivable ciphertexts. Non-deterministic encryption can give better insurance since it is hard to know whether two different relate to a similar x. This is outlined in Figure 2 (c). The sidebar Example of Homomorphic Encryption utilizing Non-Deterministic Encryption gives a numeric case. The sidebar likewise demonstrates a case when h (x) = x3 produces a wrong outcome for x =< x1 >=< 2 >, delineated by point an in Figure 2 (d) [9].

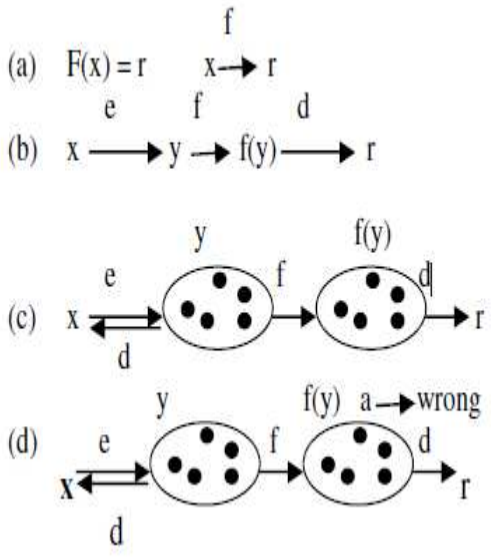

Figure 4. Overview of homomorphic encryption.

VII. ADDITIVE HOMOMORPHIC ENCRYPTION

A Homomorphic encryption is added substance, if: [10]

Enc (x⊕y) = Enc(x) ⊗Enc(y)

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

Illustration: Paillier Cryptosystem (1999): Assume we have two figures C1 et C2 with the end goal threat:

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

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

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

In this way, Pailler cryptosystem understands the property of added substance Homomorphic encryption. An utilization of an added substance Homomorphic encryption is electronic voting: Each vote is encoded yet, just the "aggregate" is unscrambled [10].

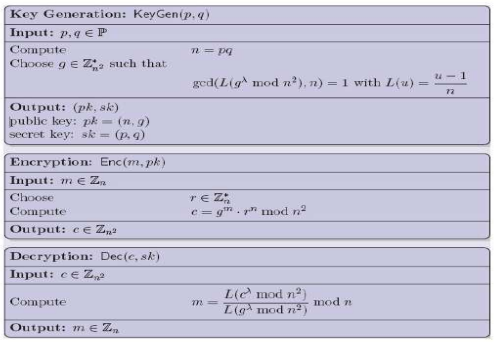

Figure 5. Pillar Algorithm [9]

VIII. MULTIPLICATIVE HOMOMORPHIC ENCRYPTION

A Homomorphic encryption is multiplicative, if: [10]

Enc (x⊗y) = Enc(x) ⊗Enc(y)

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

Illustration: RSA Cryptosystem (1978)

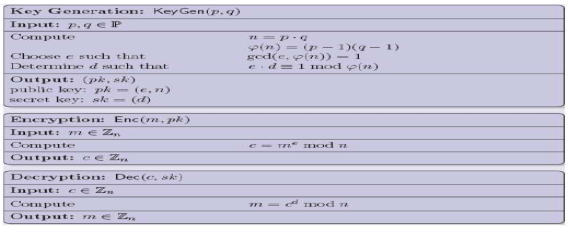

Figure 5. RSA Algorithm [10]

Assume we have two figures C1 et C2 with the end goal threat:

$$C1 = m1^e \bmod n$$
$$C2 = m2^e \bmod n$$
$$C1.C2 = m1^e\, m2^e \bmod n = (m1m2)^e \bmod n$$

RSA cryptosystem understand the properties of the multiplicative Homomorphic encryption, however, despite everything it has a pool of security, since on the off chance that we expect that two figures C1, C2 comparing separately to the messages m1, m2, so:

$$C1 = m1^e \bmod n$$
$$C2 = m2^e \bmod n$$

The customer sends the combine (C1, C2) to the Cloud server, the server will play out the computations asked for by the customer what's more, sends the encoded result (C1 × C2) to the client [10]. In the event that the assailant catches two figures C1 et C2, which are scrambled with a similar private key, he/she will have the capacity to decode all messages traded between the server and the customer. Since the Homomorphic encryption is multiplicative, i.e. The result of the figures, squares with the figure of the item [10].

IX. Conclusion

In this paper, we have audit on various homomorphic encryption arranges. In a dispersed figuring total homomorphic based security is a new thought. In this tight client scramble the data using a client's private key and that mixed data are gotten by the server. Without disentangling that data server plays out the operation and sends results back to the customer. Presently client decipher that data and gets the outcome. Along these lines, the security issue is overcome through this Homomorphic estimation. Characterization data is regulated by this figuring.

X. References

[I] John Harauz, Lorti M. Kaufman. 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] YashpalsinhJadeja and KiritModi, “Cloud Computing - Concepts, Architecture and Challenges”, International Conference on Computing, Electronics and Electrical Technologies [ICCEET], IEEE-2012

[5] Samerjeetkaur, “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 OluwaseyiFeyisetan,” 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-KokKoh," Performance Analysis of Arithmetic Operations in Homomorphic Encryption", ECE Technical Reports Paper 404, 2010

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