International Journal of Pure and Applied Mathematics
Volume 116 No. 8 2017, 145-150
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A STUDY ON INFORMATION SECURITY IN CLOUD COMPUTING UTILIZING FULLY HOMOMORPHIC ENCRYPTION TECHNIQUES

[1]B.Sundarraj, [2]M.Sriram
[1,2]Asst. Professor Dept.of CSE,BIST,BIHER, Bharath University, Chennai.
[1]sundarraj.cse@bharathuniv.ac.in, [2]sriramm.cse@bharathuniv.ac.in

Abstract: Distributed computing gives a route to the business to deal with the figuring assets on the web. The term has developed over late years, and can be utilized to depict the utilization of an outsider for your capacity and figuring needs. The mechanical improvement of distributed computing has helped the business to develop as well as the wellbeing of information has turned into a noteworthy issue. Numerous encryption procedures are utilized as a part of information security in cloud. They are especially powerful when the information is away state and in transmission state. Be that as it may, in handling state the information must be unscrambled so that the operations can be performed. Once the information is unscrambled it is accessible to the cloud supplier henceforth these customary encryption systems are insufficient to secure the information. The information will be protected if the operations are performed in the decoded information. This can be accomplished if the information is encoded utilizing homomorphic encryption strategies. This paper examines about the homomorphic encryption method, its disadvantages and future improvements.

Keywords: Cloud Computing; Data Security; Encryption, Decryption; Homomorphic Encryption

1. Introduction

Distributed computing is a technique for conveying innovation to the buyer by utilizing Internet servers for handling and information stockpiling, while the customer framework utilizes the information. Along these lines customers can get to the administrations/assets from any area in pay-per-utilizes strategy. Distributed computing has turned into a quickly developing innovation that expanded the ability of IT administrations. Distributed computing conveys administrations/assets by " X as a Service" to the clients[1-3]. Real administrations gave by distributed computing are: PaaS, SaaS and IaaS.

Platform as a Service (PaaS): In a PaaS show, a cloud supplier conveys equipment and programming instruments, more often than not those required for application improvement to its clients as an administration. A PaaS supplier has the equipment and programming all alone foundation[4].

Softwareas a Service (SaaS): With SaaS, a supplier licenses an application to clients either as an administration on request, through a membership, in a "pay-as-you-go" demonstrate or at no charge. Applications are associated with the client's framework through web and applications are claimed by customers. Google Apps, Salesforce are cases of SaaS[5-7].

Infrastructure as a Service (IaaS): Cloud foundation administrations, referred to as Infrastructure as a Service (IaaS), are self-benefit models for getting to, checking, and overseeing remote datacenterframeworks, for example, stockpiling, organizing, and organizing administrations (e.g. firewalls). Rather than purchasing equipment out and out, clients can buy IaaS in view of utilization, similar to power or another utility charging[8].

One of the key components of Cloud Computing is the organization display. There are four noteworthy sending models exist.

Open: The most widely recognized and surely understood sending model is Public Cloud. A Public Cloud is an enormous server farm that offers similar administrations to every one of its clients. The administrations are available for everybody and highly utilized for the customer section. Cases of open administrations are Facebook, Google and LinkedIn. For purchasers, Public Cloud offerings are normally for nothing out of pocket, for experts there is generally a for each per-utilize (or client) valuing model. The Public Cloud is constantly facilitated by an expert Cloud provider[9].

Private: The other ordinarily utilized arrangement model is Private Clouds. A client's inside facilitated server farm is viewed as a Private Cloud. In the event that we include virtualization and robotization, such a setup might just be viewed as a Private Cloud. An expert Cloud merchant may likewise offer a Private Cloud to their clients by

supporting a different equipment condition in the server farm. A Private Cloud is in this way generally suited for touchy information, where the client is reliant on a specific level of security. Private Clouds, to a specific degree, free the economy of scale contrasted with a Public Cloud [10].

Group: An approach to save the advantages of economy of scales with the Private Cloud is a Community Cloud. This is collaboration between clients who share a few concerns like security, application sorts, administrative issues and productivity requests. As it were, a Community Cloud is a shut Private Cloud for a gathering of clients. For governments, this is called Government Cloud and is a sort of Cloud that is increasingly adjusted. Because of authoritative issues, a Government Cloud might be the response to nation particular legal concerns.

Half breed: The Hybrid Cloud is a blend of both Private and Public. This is a setup that is greatly utilized for expansive organizations. Fundamental information is normally favored in a Private Cloud and supporting administrations in Public, for example seek, email, web journals, CRM and so forth. At the end of the day, key applications are run independently[11].

In the cloud condition, there are numerous security dangers are found. [12]. One of the security issues is information security and it has been recognized as the real security issue in cloud condition.

In the cloud condition, there are numerous security dangers are found. [13]. One of the security issues is information security and it has been distinguished as the real security issue in cloud condition. Center of this paper is guaranteeing the security of the information in cloud. The standard encryption procedures require the unscrambled information for the operations. This will make the information accessible to the specialist co-op. In the event that the operations are performed on the scrambled information, then the information won't be accessible to the specialist organization. Homomorphic encryption permits the clients to work on the encoded information. In this paper, we have broke down the idea of homo morphic encryption[14-17].

2. Related Work

In cloud the information will be in secured state just if the operations are done on the scrambled information. This is conceivable with the assistance of Homomorphic encryption procedure. The Paillier cryptosystem or RSA systems can't be utilized as a part of cloud as they bolster just constrained operations. Craig Gentry grew first Fully Homo morphic encryption conspire in 2009, yet that was not executed till 2010 in light of equipment constraints[18].

Be that as it may, on execution of this method set aside long opportunity to play out the operation. Later the time was diminished by Homomorphic Encryption Library(Helib). This likewise had a few restrictions as it didn't perform well over the web. Helib is a product library created by IBM which executes the completely homomorphic encryption system. As of now accessible Helib is the execution of Brakerski-Gentry-Vaikunthanathan conspire [19].

3. Problem Statement: Data Security

Clients when go for the cloud condition, they are given Infrastructure as a Service for the storage room. Clients store the business information and additionally the individual information on the cloud. Be that as it may, if the information is not secured for the operations then the reason for information stockpiling in cloud is crushed.

The following are the three necessities of information security.

Information Confidentiality: It is one of the significant parts of information security. It alludes to just the approved clients can get to the information. An extremely key segment of ensuring data classification would be encryption. Encryption guarantees that lone the ideal (individuals who knows the key) can read the data [20].

Information Integrity: Integrity of data alludes to shielding data from being changed by unapproved parties. information uprightness ought to be executed on cloud with the goal that information can't be changed misguidedly.

Information Availability: Availability of data alludes to guaranteeing that approved gatherings can get to the data when required. Data just has esteem if the ideal individuals can get to it at the correct circumstances. Denying access to data has turned into an extremely normal assault these days.

There are numerous encryption systems proposed [21] for the information encryption. Creators of these papers recommended that the information must be scrambled and put away back to the customer machine. The information will be decoded for the operations on the information. Once the operations are done, the information can be scrambled again and put away back to the cloud machine. The trading of information from cloud and customer machine for some number of times won't be a decent arrangement and this will be exorbitant one. Utilizing this approach the trading of information over the system prompts information powerlessness issue. Recommendation of going for an outsider [22] was additionally proposed. Be that as it may, these all will work just if the information is away condition of transmission state. Yet, in the event that information is in

handling state these recommended arrangements won't work.
A superior method for accomplishing information security will be play out the operations on the scrambled information. Growing such an answer leads another strategy for encryption known as Homomorphic encryption. This sort of encryption permits performing operations on the encoded information on the cloud [23].

4. Homomorphic Encryption

Homomorphic encryption (HE) alludes to a unique kind of encryption method that takes into account calculations to be done on scrambled information, without obliging access to a decoding key. While customary encryption plans can be utilized to secretly outsource information stockpiling to outsiders, the information can't be utilized for calculations without first decoding it, bringing about an enormous loss of utility. Homomorphic encryption permits calculations to be performed without first unscrambling the information. The consequences of the calculations remain encoded, and must be perused and translated by somebody with access to the unscrambling key[24].

The homomorphic rationale is clarified. At the point when two components are included nonhomomorphic idea it is straightforwardly included. In homomorphic idea the components which are to be included are encoded and included and put away in the scrambled frame. On decoding, all the scrambled components are acquired in the plain content .On the off chance that in the event that we need just the additional component that can be unscrambled and acquired leaving others in scrambled shape[25].

Homomorphic encryption has two sorts to be specific fractional and completely. In completely homomorphic encryption it underpins self-assertive number of both operations expansion and increase. Halfway homomorphic encryption underpins either expansion or duplication operation as it were. Paillier cryptosystem [26] plan is a halfway encryption sort which bolsters just expansion operation. RSA cryptosystem [27] underpins just duplication operation.

A. Paillier Cryptosystem

This is a public key crytosystemIts a partial homomorphic encryption scheme which supoorts only addition operation.

Choose two prime numbers p & q and calculation =p*q and λ = lcm(p-1,q-1) such that gcd(p*q,(p-1)*(q-1)) = 1
2) Select g Є Z*n^2 and calculate μ = (L(g^λ mod n^2))^(-1) mod n where L(x) = x-1/n
3) n, g acts as a public key
4) λ, μ acts as a private key

Encryption Algorithm:
1) Let m Є Zn be the message
2) Choose r Є Z*n
3) Required Cipher text is c = g^m *r^n mod n^2

Decryption Algorithm:

1) Compute m = L(c^λ mod n^2)*μ mod n

B. RSA Cryptosystem

This is a public key cryptosystem Its a partial homomorphic encryption scheme which supports only addition operation.

Choose two prime numbers p & q and calculation =p*q and λ = lcm(p-1,q-1) such that gcd(p*q,(p-1)*(q-1)) = 1

2) Select g Є Z*n^2 and calculate μ = (L(g^λ mod n^2))^(-1) mod n where L(x) = x-1/n

3) n, g acts as a public key

4) λ, μ acts as a private key

Encryption Algorithm:

1) Let m Є Zn be the message

2) Choose r Є Z*n

3) Required Cipher text is c = g^m *r^n mod n^2

Decryption Algorithm:

Compute m = L(c^λ mod n^2)*μ mod n

C. Boneh-Goh-Nissim Cryptosystem

Boneh-Goh-Nissim Cryptosystem is completely homomorphic encryption framework. It is an open key cryptosystem that was proposed by D.Boneh, E.Goh and K.Nissim in 2005. It underpins boundless expansion operation yet one augmentation operation.

Algorithm;

Key Generation;

Take two prime numbers q1,q2 ε Z,n = q1 * q2

Two generator g,u ε G and h= Uq2

Select Pk (n,g,h,e,G,G1) as public key and Sk (q1) as private key.(G,G1 : multiplicative group of order n and e: G X G1 -> G1 is bilinear map)[28]

Encryption:

Encrypt m using public key Pk ,C = gm .hr mod n

Decryption:

To decrypt C using private key Sk (q1) perform

Cq1 = (gq1)m, ie message m is discrete logarithm of Cq1 to the base of gq1.

Additive Homomorphic property.

If C1 and C2 are two ciphers

$C1 = g^{M1} \cdot h^{r1} \bmod n$

$C2 = g^{M2}.h^{r2} \bmod n$

$C1.C2 = g^{(M1+M2)}.h^{(r1+r2)} \bmod n$

4. Advantages and Disadvantages

Advantage:

- very fast,very simple encryption and verification.
- Easier to implement than elliptical curve cryptography(ECC)
- Easier to Understand
- Widely deployed, better industry support.

Disadvantage:

- very slow key generation.
- slow decryption,which is slightly tricky to implememt securely.
- Two part key is vulnerable to GCD attack if poorly implemented[29-30].

6. Conclusion

Homomorphic Encryption will convey another measurement to distributed storage. It gives classification to the information as the plain content is never uncovered in the cloud. In this paper, we saw Homomorphic encryption's RSA Cryptosystem advantage and disadvantage. However completely homomorphic encryption runs moderate and it should be upgraded to accomplish speedier outcomes. At last, we presume that the completely homomorphic encryption calculation must be upgraded with the goal that it can deal with every one of the operations on the encoded information and also the execution can be moved forward.

References

[1] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues", Future Generation Computer Systems Elsevier journal, vol. 28, pp. 583-592, 2012.

[2] M. Zhou, R. Zhang, W. Xie, W. Qian and A. Zhou, "Security and Privacy in Cloud Computing: A Survey", pp. 105-112.

[3] S. Subashini and V. Kavitha, "A Survey on Security issues in Service delivery models of Cloud Computin" in Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011, Elsevier.

[4] C.Yang, W.Lin and M.Liu " A Novel Triple Encryption Scheme for Hadoop based Cloud Data Security", in proceeding of IEEE International Confernece on Emerging Intelligent Data and Web Technologies, Xi'an, Chinna, pp:437-442,2013.

[5] P.Rewargad and Y.Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption algorithm to Enhance Data security in Cloud Computing", in proceeding IEEE InternatonalCOnference on Communication Systems and Network Technologies, Gwalior, India,pp:437-439,2013.

[6] S.Han and J.Xing, "Ensuring Data Storage Security Through A Novel Third Party Auditor Scheme in Clooud Computing", in proceeding IEEE International Confernece on Cloud Computing and Intelligent Systems, Beijing, China,pp:264-268,2011..

[7] Craig Gentry, A Fully Homomorphic Encryption Scheme,Sep-2009,available at http://crypto.stanford.edu/craig/craig-thesis.pdf.

[8] R.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-key Crytosystem",Communications of the ACM, vol.21, pp;120-126,1978.

[9] S.Halevi and V.Shoup, "Design and Implemetation of a Homomorphic-Encrytion :ibrary", April-2013, available at http://people.csail.mit.edu/shaih/pubs/he-library.pdf.

[10] S.Halevi and V.Shoup, "Design and Implemetation of a Homomorphic-Encrytion :ibrary", April-2013, available at http://people.csail.mit.edu/shaih/pubs/he-library.pdf.

[11] D. Smith, M. Eggen, R. St.Andre, Transition to Advanced Mathematics, 7th ed., Boston, MA: Brooks/ Cole,2011.

[12] Encrypting Numerical Values [Picture]. Retrieved November 4.2012, from: http://www.americanscientist.org/issues/pub/alice-and-bob-in-cipherspace

[13] Homomorphic Concatenation [Picture]. Retrieved November 4, 2012, from: http://blogs.teamb.com /craigstuntz/2010/03/18/38566

[14] B. Sundarraj1 , K.G.S. Venkatesan2, M. Sriram3 , Vimal Chand4 ,An Iaas Cloud System with Federation Threshold: International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015.

[15] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[16] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[17] Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[18] Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[19] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[20] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[21] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[22] Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[23] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[24] Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[25] R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
[26] R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[27] R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[28] Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[29] Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[30] Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.