International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S2, August 2019

Information Security in Cloud Computing utilizing Fully Homomorphic Encryption Techniques

K. Sivaraman, R. Kavitha, C. Anuratha.

Abstract*: Flowed enlisting gives a course to the business to deal with the figuring assets on the web. The term has made over late years, and can be utilized to outline the utilization of a pariah 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. [19],[20],[21]

***Keywords* : Distributed computing; Data Security; Encryption, Decryption; Homomorphic Encryption**

I. INTRODUCTION

Circulated processing is a strategy for ephemeral on encroachment to the purchaser by using Internet servers for intriguing mind of data amassing, while the user system uses the data. 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. [14],[16], [18]

Real administrations gave by distributed computing are:
PaaS, SaaS and IaaS.Stage as a Service (PaaS): In a PaaS show up, a cloud supplier passes on apparatus and programming instruments, when in doubt those required for application improvement to its clients as an association. A PaaS supplier has the apparatus and programming in isolation foundation.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
K.Sivaraman, Department of CSE,Bharath Institute of Higher education and research, Tamilnadu, India. Email: sivaraman2006@gmail.com
R.Kavitha, Department of CSE,Bharath Institute of Higher education and research, Tamilnadu, India.. Email: kavis_happy@yahoo.co.in
C.Anuradha, Department of CSE,Bharath Institute of Higher education and research, Tamilnadu, India.. Email: anuradha.ak23@gmail.com

Softwareas a Service (SaaS): With SaaS, a provider licenses an application to customers either as an organization on solicitation, through a participation, in a "pay-as-you-go" exhibit or at no charge. Applications are associated with the client's framework through web and applications are claimed by cutomers. Google Apps, Salesforce are cases of SaaS.
System as a Service (IaaS): Cloud foundation associations, suggested as transportation as a Service (IaaS), are self-improvement models for getting to, inspection, and coordinating remote datacenterframeworks, for example, aggregating, masterminding, and dealing with associations (for instance firewalls). Rather than gaining equipment unmitigated, clients can buy IaaS in context on use, similar to control or another utility charging. One of the key pieces of Cloud Computing is the affiliation appear. There are four fundamental sending models exist. [13], [15] ,[17]

Open: The most for the most part saw and no ifs, ands or buts grasped sending model is Public Cloud. A Public Cloud is a gigantic server farm that offers practically identical associations to the majority of its clients. The associations are available for everybody and exceptionally utilized for the customer region. Examples of open associations are Facebook, Google and LinkedIn. For purchasers, Public Cloud commitments are usually to no closure out of pouch, for masters there is usually a for each per-use (or punter) regarding replica. The communal obscure is regularly supported by a pro obscure supplier[8],[10] ,[12]
Undisclosed: The previous ordinarily utilized arrangement model is personal exhaust A client's inside supported server estate is viewed as a Private Cloud. On the off chance that we fuse virtualization and robotization, such a course of action might just be viewed as a Private Cloud. A master Cloud vendor may comparably offer a Private Cloud to their clients by supporting an other equipment condition in the server farm. A Private Cloud is thusly ordinarily fitting for dubious information, where the buyer is focus to a precise point of safety. personal haze, to a specific degree, free the wealth of extent separated from a open blur
Social event: An advance to manage save the upsides of wealth of balance with the secret shade is a commune obscure. This is participation linking patrons who offer two or three concerns like defence, relevance sorts, organizational issues and effectiveness requirements. As it were, a society confuse is a shut personal shade for a get-together of patrons. For governments, this is called Government obscure and is a sort of shade that is dynamically attuned Because of conclusive issues, a Government Cloud might be the retort to country explicit official concerns. 22],[23],[24]

Mutt: The cross shade is a merge of equally Private and community. This is a course of action that is immensely utilized for magnanimous affiliations. indispensable in sequence is normally upheld in a personal Cloud and following associations in communal, for instance search for, email, web journals, CRM, and so on. Close to the day's end, key applications are run self-governingly.In the cloud condition, there are numerous security dangers are found. [1][2][3]. One of the security issues is information security and it has been recognized as the real protection concern in cloud condition.

In the cloud condition, there are numerous security dangers are found. [1][2][3]. 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 document, we have broke down the design of homomorphic encryption. [25],[27],[29]

II. 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 Homomorphicencryption conspire in 2009, yet that was not executed till 2010 in light of equipment constraints. 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 [10].

III. 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. [7],[9] ,[11]

Information Confidentiality: It is one of the colossal bits of information security. It proposes just the embraced clients can get to the information. A key portion of guaranteeing information strategy would be encryption. Encryption ensures that solitary the perfect (people who knows the key) can examine the information.

Information Integrity: veracity of facts proposes shielding data from mortal changed by unapproved parties. information uprightness ought to be executed on cloud with the target that information can't be changed misguidedly. [2],[4],[6]

Information Availability: Accessibility of information proposes ensuring that attested get-togethers can get to the information when required. Information basically has regard if the perfect people can get to it at the right conditions. Denying access to information has changed into an uncommonly regular strike nowadays.There are numerous encryption systems proposed [4][5] 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 [6] 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. [1],[3],[5]

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. [26],[28],[30]

IV. HOMOMORPHIC ENCRYPTION

Homomorphic encryption (he) suggests a remarkable sort of encryption strategy that considers figurings to be done on mixed data, without obliging access to an unraveling 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. 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. 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 [7] plan is a halfway encryption sort which bolsters just expansion operation. RSA cryptosystem [8] underpins just Paillier Cryptosystem

his is an open key crytosystemIts an incomplete homomorphic encryption plot which supoorts just expansion task.
Pick two prime numbers p and q and figuring =p*q and λ = lcm(p-1,q-1) with the end goal that gcd(p*q,(p-1)*(q-1)) = 1

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

3) n, g goes about as an open key

4) λ, μ goes about as a private key

A. Encryption Algorithm:

1) Let m Є Zn be the message

2) Choose r Є Z*n

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

Unscrambling Algorithm:

1) Compute m = L(c^λ mod n^2)*μ mod n

B. RSA Cryptosystem

This is an open key cryptosystem Its a fractional homomorphic encryption conspire which supports just expansion task.

Pick two main numbers p and q and calculation =p*q and λ = lcm(p-1,q-1) with the ultimate objective that gcd(p*q,(p-1)*(q-1)) = 12) Select g Є Z*n^2 and figure μ = (L(g^λ mod n^2))^(- 1) mod n where L(x) = x-1/n

3) n, g goes about as an open key

4) λ, μ goes about as a private key

Encryption Algorithm:

1) Let m Є Zn be the message

2) Choose r Є Z*n

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

Unscrambling Algorithm:

Register m = L(c^λ mod n^2)*μ mod n

C. Boneh-Goh-Nissim Cryptosystem

Boneh-Goh-Nissim Cryptosystem is totally homomorphic encryption structure. It is an open key cryptosystem that was proposed by D.Boneh, E.Goh and K.Nissim in 2005. It supports vast development task yet one expansion activity.

Calculation;

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 open key and Sk (q1) as private key.(G,G1 : multiplicative social affair of solicitation n and e: G X G1 - > G1 is bilinear guide)
Encryption:

Encode m utilizing open key Pk ,C = gm .hr mod n

Decoding:

To decode C utilizing private key Sk (q1) perform

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

Added substance Homomorphic property.

On the off chance that C1 and C2 are two figures

C1 = gM1 .hr1 mod n

C2 = gM2.hr2 mod n

C1.C2 = g(M1+M2).h(r1+r2) mod n

V. ADVANTAGES AND DISADVANTAGE

A. Bit of leeway

- Very fast, very basic encryption and check.
- Easier to execute than circular bend cryptography(ECC)
- Easier to comprehend
- Widely deployed, better industry support.

B. Weakness:

- Very moderate key age.
- Slow decryption, which is marginally dubious to implememt safely.
- Two part key is defenseless against GCD assault if ineffectively executed.

VI. 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. Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Weight ward change region plummeting change for square based image huffman coding", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4313-4316.
2. Gowri Sankaran, B., Karthik, B. & Vijayaragavan, S.P. 2019, "Image compression utilizing wavelet transform", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4305-4308.
3. Kandavel, N. & Kumaravel, A. 2019, "Offloading computation for efficient energy in mobile cloud computing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 4317-4320.
4. Vinoth, V.V. & Kanniga, E. 2019, "Reversible data hiding in encrypting images-an system", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3051-3053.
5. Selvapriya, B. & Raghu, B. 2019, "Pseudocoloring of medical images: A research", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3712-3716.
6. Senthil Kumar, K. & Muthukumaravel, A. 2019, "Bi-objective constraint and hybrid optimizer for the test case prioritization", International Journal of Engineering and Advanced Technology, vol. 8, no. 6, pp. 3436-3448.
7. Kavitha, G., Priya, N., Anuradha, C. & Pothumani, S. 2019, "Read-write, peer-to-peer algorithms for the location-identity split", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 445-447.
8. Kaliyamurthie, K.P., Michael, G., Anuratha, C. & Sundaraj, B. 2019, "Certain improvements in alzheimer disease classification using novel fuzzy c means clustering for image segmentation", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 599-604.
9. Kaliyamurthie, K.P., Sundarraj, B., Geo, A.V.A. & Michael, G. 2019, "RIB: Analysis of I/O automata", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1019-1022.
10. Velvizhi, R., Rajabhushanam, C. & Vidhya, S.R.S. 2019, "Opinion mining for travel route recommendation using Social Media Networks (Twitter)", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 508-512.
11. Kavitha, R., Sangeetha, S. & Varghese, A.G. 2019, "Human activity patterns in big data for healthcare applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1101-1103.
12. Pothumani, S., Anandam, A.K., Sharma, N. & Franklin, S. 2019, "Extended VEOT framework - Implemented in a smart boutique", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 762-767.
13. Kaliyamurthie, K.P., Michael, G., Krishnan, R.M.V. & Sundarraj, B. 2019, "Pseudorandom techniques for the internet", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 915-918.
14. Aravindasamy, R., Jeffrin Rajan, M., Rama, A. & Kavitha, P. 2019, "Deep learning provisions in the matlab: Focus on CNN facility", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 990-994.
15. Theivasigamani, S., Linda, M. & Amudha, S. 2019, "Object sensing and its identification & motion sensing", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 545-549.
16. Mary Linda, I., Vimala, D. & Shanmuga Priya, K. 2019, "A methodology for the emulation of IPv4", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 848-852.
17. Velvizhi, R., Priya, D.J., Vimala, D. & Linda, I.M. 2019, "Increased routing algorithm for mobile adhoc networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1606-1608.
18. Sangeetha, S., Anuradha, C. & Priya, N. 2019, "DNS in real world", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 937-940.
19. Geetha, C., Vimala, D. & Priya, K.S. 2019, "Constructing multi-processors and spreadsheets with SKIVE", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 516-519.
20. Yugendhar, K., Sugumar, V. & Kavitha, P. 2019, "A novel method of univac using fuzzy logic", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 435-437.
21. Kaliyamurthie, K.P., Michael, G., Elankavi, R. & Jijo, S.A. 2019, "Implementing aggregate-key for sharing data in cloud environment using cryptographic encryption", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 957-959.
22. Jeffrin Rajan, M., Aravindasamy, R., Kavitha, P. & Rama, A. 2019, "A novel method of object orientation variation in C++ and java", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 708-710.
23. Nayak, R., Dinesh, S. & Thirunavukkarasu, S. 2019, "A novel method improvement of rapid miner for the data mining applications", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 457-460.
24. Sivaraman, K., Krishnan, R.M.V., Sundarraj, B. & Sri Gowthem, S. 2019, "Network failure detection and diagnosis by analyzing syslog and SNS data: Applying big data analysis to network operations", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 883-887.
25. Vimala, D., Linda, I.M. & Priya, K.S. 2019, "Decoupling online algorithms from erasure coding in DNS", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 950-953.
26. Rama, A., Kumaravel, A. & Nalini, C. 2019, "Preprocessing medical images for classification using deep learning techniques", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 711-716.
27. Sangeetha, S., Srividhya, S.R., Anita Davamani, K. & Amudha, S. 2019, "A procedure for avoid overrun error in universal synchronous asynchronous receiver transmitter (usart) by utilizing dummy join and interrupt latency method", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 657-660.
28. Aravindasamy, R., Jeyapriya, D., Sundarajan, B. & Sangeetha, S. 2019, "Data duplication in cloud for optimal performance and security", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 1156-1158.
29. Aravindasamy, R., Jeffrin Rajan, M., Sugumar, V. & Kavitha, P. 2019, "A novel method on developing superblocks and the transistor using apodryal", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 9 Special Issue 3, pp. 982-985.
30. Sasikumar, C.S. & Kumaravel, A. 2019, "E-learning attributes selection through rough set theory and data mining", International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 3920-3924.

AUTHORS PROFILE

K.Sivaraman, Assistant Professor, Department of CSE,Bharath Institute of Higher education and research, Tamilnadu, India.

R.Kavitha, Assistant Professor, Department of CSE, Bharath Institute of Higher education and research, Tamilnadu, India.

C.Anuradha, Assistant Professor, Department of CSE,Bharath Institute of Higher education and research, Tamilnadu, India.