Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 1992-2001
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.226

Security in Cloud Computing using Homomorphic Cryptography

Savita A Harkude, Research Scholar**,** Dept. of ETE, Sir MVIT, Bangalore, India, Savita.harkude@gmail.com
Dr. G N Kodanda Ramaiah, Professor**,** Dept. of E&CE**,** Kuppam Engineering College**,** Kuppam, India**,** gnk.ramaiah@gmail.com

Abstract: Cloud computing is very wide phenomenon in computer science. Users will be permitted to store great deal of knowledge based on storage in cloud. The varied issues of security associated with confidentiality, privacy, data security, authentication and integrity must be taken care. The cloud service provider mostly will store information in format of plain text and a particular user's encryption algorithm can be used to secure data. The decryption of information will be carried out. The paper presents cloud storage with encrypted format by homomorphic encryption. Storage of the information is done in DynamoDB of AWS cloud(public). User can perform all the operations and computation on data encrypted cloud(public). The required outputs can be retrieved on user's machine when the case stands as the data on the cloud(public) is not stored in plaintext.

Keywords: Cloud Computing, Homomorphic Cryptography, DynamoDB of AWS

I. INTRODUCTION

• Cloud Computing has major issues in security that has to be addressed. One need to implement a strong and efficient shield of security at each of the infrastructure levels. Namely reserachers talk about - Network level, Host level, Application level. Data associated with each of levels must reside with proper security. This paper describes implementation of secure methodology of cloud data at rest.

• The issues related with security associated that are encountered due various intruders attacks is a must to be resolved for the store to be confidential and at the same time public. Few of the security issues in cloud computing:

• Availability –Available data means whenever and wherever required must be provided and the user must have the control over the same so, availability is in major threat in security. So, issue related to data availability must be attended keenly especially when services are to be accomplished for neighbor cloud service provider. Currently, there are three major threats to availability:a) network based attack, b)cloud service providers availability and c) backup of stored data by cloud service provider. One need to provide efficient and effective techniques to the great datafor it to possess strong authentication, access control and authorization.

• Data remanence–This is situation when data gets public or to a party not meant for when after it is deleted in an unauthorized way. Security of knowledge in actual is a lifecycle that presents complete sequence from data formation toobliteration depicted in Fig. 1. Security measures should inculcate when the data is obliterated.

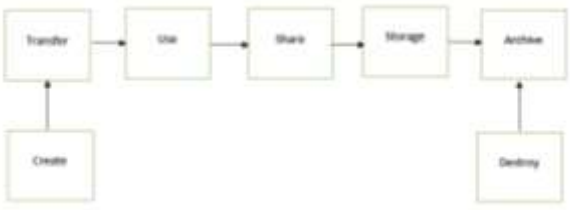


Fig 1: Knowledge Security Lifecycle

• Privacy and Legal Issues- Another major issue is cloud stores are sighted by Pearson. Location of data in the cloud store is matter of ignorance for the user. In each country Cyber legalities and laws are different in each of the countries and has serious concern regarding confidentiality and legality of knowledge.

• X-Party Control- Managers of the user data are Cloud Service providers. X-party reach to the confidential information and business secrets may lead to leakage of the same and the data is very much available for the threat of corporate spying.

• Cloud computing includesvarious technologies eg. network structure, databases, virtualization scenario, load balancing factor,operating systems, transaction management,resources and processes scheduling, memory management, etc. A small spare in security in any of these technologies may bring fall down to the entire system.[26]

A security layout that may ensure security against "Loss of Data" and 'Account Hijacking' attacks, can be enriched with the following keywords: Credential Lookup, Strengthen Authentication, and Key Management.

II. LITERATURE REVIEW

Much of account holder's were cracked into leaking much of information such as mastercard details, passwords, physical addresses and many other personal details when in April 2011, Sony's playStation network was hijacked. Authorities took over the responsibility for this unexpected incidentand admitted that they should have been taking some special protective measures by encoding the network information. During the clock hour same, Dropbox was discovered that stored plaintext user files. Consequently, users protest against angry at the corporate company for have their confidential files as plaintexts and not encrypted[22].

MahaTebba et al. reviewed the application scenario of Homomorphic Encryption cryptography on a environment based on cloud computing. The main four specialities "Data Privacy", "Secure keys used" and "Homomorphic Encryption type"[2]. ReemAlattas et al. [3] has presented the mechanism of Homomorphic Encryption on the basis of algebraic and Fermat's Little Theorem for security upgrades. The troubleshoot the issue of knowledge privacy with confidentiality, mechanism of FHE is explained that handles the information in encrypted format. The fully homomorphic encryption is slower mode which create a need for faster homomorphic encryption.

An encryption mechanism was proposed by Gentry is fully homomorphic still of slow performance. Various mechanisms are discussed in recent past to speedup the performance of fully homomorphic encryption methods. The multiprocessing of provided information is one of the way of encryption execution for Gentrysthat was explained Ryan Hayward et al. [4] in paper and was testeddomain of a private cloud computing. Frederik A. et al. [5] showed structured wide definition in the homomorphic encryption, presently new applications exit in homomorphic encryption as solution for problems. In1978,Rivestetal. [6] introduced first only homomorphism technique. Rivest et al. [7] introduced the RSA, that provide multiplicative homomorphism. Yao [8] presented partial homomorphic encryption methods.[9][10] [11] [12] introduced the work in homomorphic encryption mechanism used in past years. Craig Gentry [13] presented fully homomorphic encryption in the thesis which talks on cryptographic mechanisms. [14] proposes Homomorphic encryption on size smaller than cipher text. Van Dijk et al. [15] presented implements arithmetic operation over integer. [16] introducesGentry's model for faster improvement. Ramaiah et al.[17]presented New way of public key type of homomorphic encryption than integer plaintext.

III. PROBLEM STATEMENT

Loss of Data and Account Hijacking attacks must and should be erased in Cloud Storage as a Service as a special microservice. One has to implement the following techniques such as Kerberos for strengthen authentication,credential Lookup and key management several authentication options e.g., OTP, digital certificates, Standard Network Encryption e.g., SSL/TLS, IKE, VPN. However, implementation of these independent techniques for cloud storage services do not ensureany great level of security against various threatsor provide cost-effective implementation. So, what if the "Data in Rest" is within the focus and not the client of the "Data in Rest". The cloud data storage must be encrypted and manipulations(operation) by the clients should be performed on the ciphertext(data) on cloud without tampering the encrypted form.

IV. PRELIMINARIES

Some of the basic understandings required in this paper are placed below:

1. Encryption – Decryption

Encryption:Encryption enables the data as the cipher text that provides protection.

Key Management: Unlike encryption key management that allows the protected data access.

It is a very must insight that researchers recommend the data at rest, data over networks in transit and data on backup medium must always be in encrypted format. Encoded data at rest are the special taken cares of those should be capable of avoidingmalicious multi-tenants abuse and threat of malicious cloud providers. Equivalently at the same point in time implementation of key stores and access to key stores should be done with proper secure ensured.

Access Control and Identity Management: It is always advised not to share account credentials, to be availed be very strong authentication that credits you with multiple factors and to trust delegated authentication and manage the reliance on overall cloud services. Management of access control and identity in secure systems also stands out to be critical factor in account and repair hijacking.

2. Full homomorphic encryption scheme:

in 1978 Rivest first proposed Homomorphic Encryption (HE) with the "privacy homomorphism" [1] concept. HE is an encryption technique that allows one to manipulate ciphertext directly. The key concept points the fact that the encryption value of plaintext before manupaltion or any operation is the same as that of ciphertext after encryption.

HE supports direct retrieval, confidential data management, count and calculate the encrypted data inside the cloud and return the results to users within the sort of encrypted data. HE is that the prime technology that ensures the privacy protection of knowledge in cloud environments. [20]

IBM in 2009 proposed the primary fully homomorphic encryption technique that supported ideal lattices, that recovered re-encrypted data. FHE is an encryption algo that is characteristic with additive homomorphism and multiplicative homomorphism and is capable of executing any of the multiple addition and also multiplication operations.

It says, we are on edge that one can perform certain operations on data in the cloud store without the decryption into the plain text. This data is always in encrypted format at almost all the stages of the cloud store. The various operations on the database of the cloud store can be accomplished by inculcating Fully Homomorphic Encryption (FHE) technique.

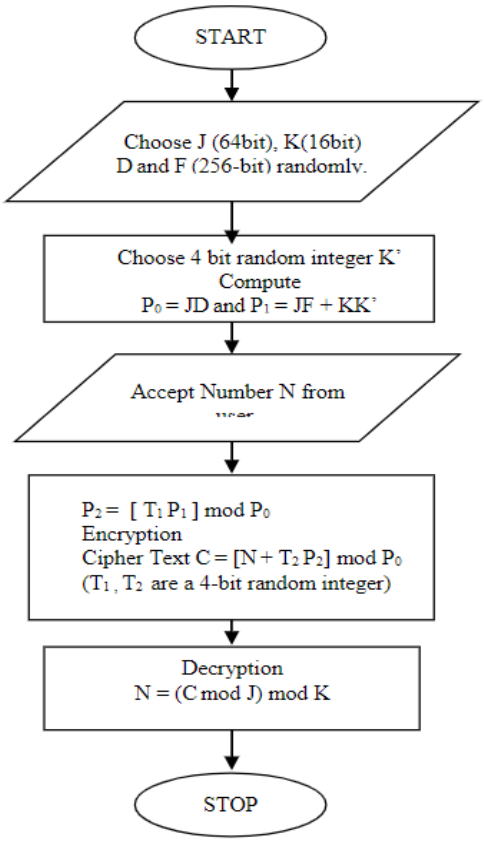


Fig 2: Flowchart for Fully homomorphic scheme:

3. MapReduce Algorithm

Introduced by Google MapReduce here acts as processing or parallel programming model. In MapReduce model, the computation can be specified by a user havingtwo functions, Map and Reduce. Mapping phase, in this phase MapReduce gets the input data and passes on to each data item to the mapper. Reducing phase, in this phase all the outputs gained from the mapper are processed by the reducer and reaches at outcome . In other word, the mapper is aims at filtering and transforming the input into segments that the reducer can aggregate over. [19]

The MapReduce is one of the foremost well-known and significant multiprocessing techniques in cloud computing. MapReduce could also be a programming model for largescale multiprocessing. MapReduce can also act as a software framework in distinct platforms. MapReduce inculcate distinct properties for a specific province for each of the platform used. [18]

V. PROPOSED SYSTEM

The Proposed system is comprised as follows:

1. Methodology

The proposed algorithm uses the combination of public-private key encryption and homomorphic scheme. We propose framework using map reduce scheme to automatically encrypt the data for transit as well as rest in cloud.

Let polynomial algorithm PHE (Data,En,De,Che) where (Data,En, De) are part of private key encryption

Che=H(frame,map,part,read,merge) are map reduce algorithm explained as below.

Let E be the probabilistic algorithm where it takes value ''e'' as a security parameter and returns E

E = Data(1e) ---------- 1

Let C be the cipher text which based on probabilistic function which uses value of E and input data D to provide a ciphered text

C=En(E,D) ---------- 2

Let (I1,V1) be the input pairs calculated by deterministic function which takes values C and input function f to get input sequeces.

(Ii,Vi) = Frame (f,C) ---------- 3

Let (α,β) be the intermediate pairs calculated by probabilistic function using input pairs.

(α,β) = map(Ii,Vi) ---------- 4

Let M be the probabilistic model which takes intermediate pairs and produce value M for space h.

M= part(α,β) ---------- 5

Let (α,μ) is probabilistic model which takes α as input and μ be probabilistic value and output would be

(α,Ʈ)= read(α,μ) ---------- 6

Let z be deterministic algorithm which takes input in set of output using merge operation

Z= merge (αi,Ʈi) ---------- 7

Finally let H be map reduce function and finally

Z = H(e,x)

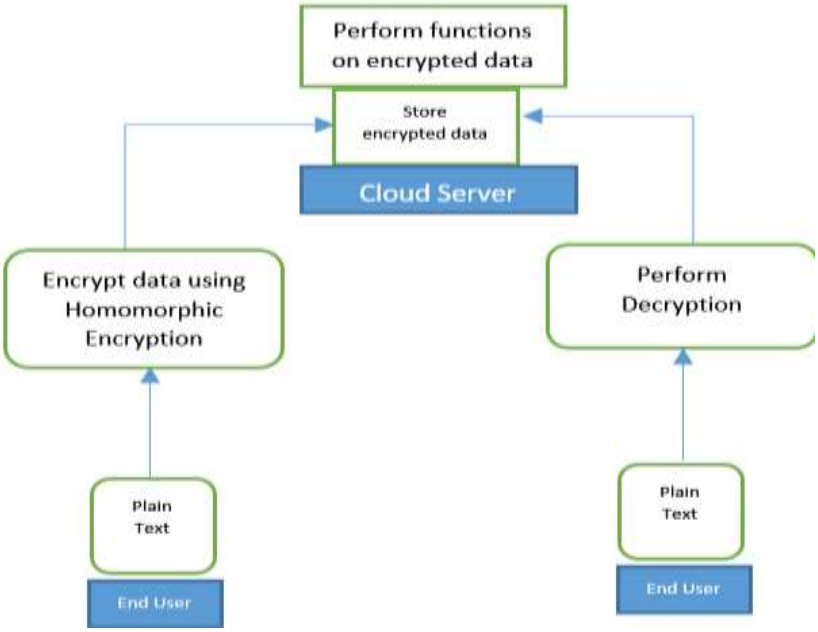


Fig. 3 The proposed system.

2. Implementation

The AWS DynamoDB services are availed by the users through a credentials based login developed using the Eclipse IDEand then based on the requirements the user can perform operations on the data in the cloud. Theuser may go for system exit once he / she is done with all the tasks.

The sequence stated above can be implemented as:

Step 1: An instance of DynamoDB on Amazon Web Server is created.

Step 2: Tables of Database are created with an appropriate schema

Step 3: AWS provides credentials to execute access controls.

Step 4: Python SDK is installed after AWS Software Development Kit is installed.

Step 5: Go on with step in23AWS Software Development Kit.

Code based on python will be built for interaction with Dynamo D and will be able to execute in former platform. Using the above python platform all the data manipulation needed in the transactions such as addition, deletion or check balance are performed. An interface is provided for users that avail them to log-in to the system. Then after perform all the tasks and fulfill the requirements that system may provide. The user can access the database until the extent owner of the database may provide.

Step 6: Exit.

3. Principle of working

a. Client Machine:The client will send access request to cloud server from client machine.

b. Login- The login page will help user to sign-in to system with username and password that is authorized by server.

c. Key Selection- The key selection is done based on user logged into the system with encryption and decryption of data.

d. Query- Here the user will select the task to be executed once the user logs into the system with proper credentials.

e. Computations –On the basis of task selected, computations are executed and outcomes of execution are moved to encryption components.

f. Encrypt and store- The encryption is performed on the user dataor system executed data are stored in cloud.

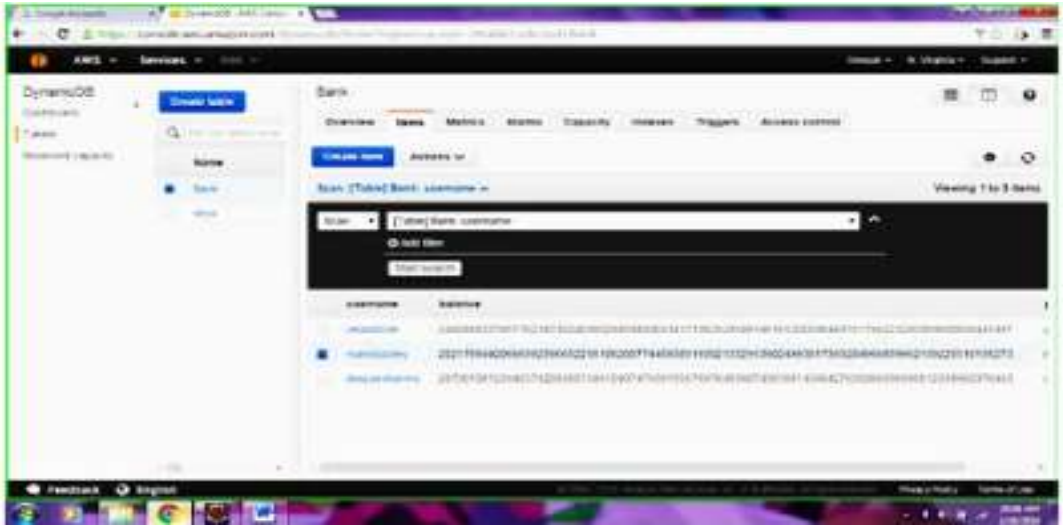
g. Retrieve and decrypt- This section displays the data requested by the user at the clients end by retrieving the same from the cloud store.

h. AWS Cloud (DynamoDB)- This section is the actual cloud store/database wherein the entire incoming data are system executed data is stored. This data get available to the clients through log-in module to verify the credentiality of the user and keyselectionsection for retrieval of keys stored in cloud store/database, encryption section storing the data in encrypted form. The decryption section for the retrieval of data and decrypt it and also, computations executed on the user data as required or as flashed query.

VI. RESULTS

1. Screenshots

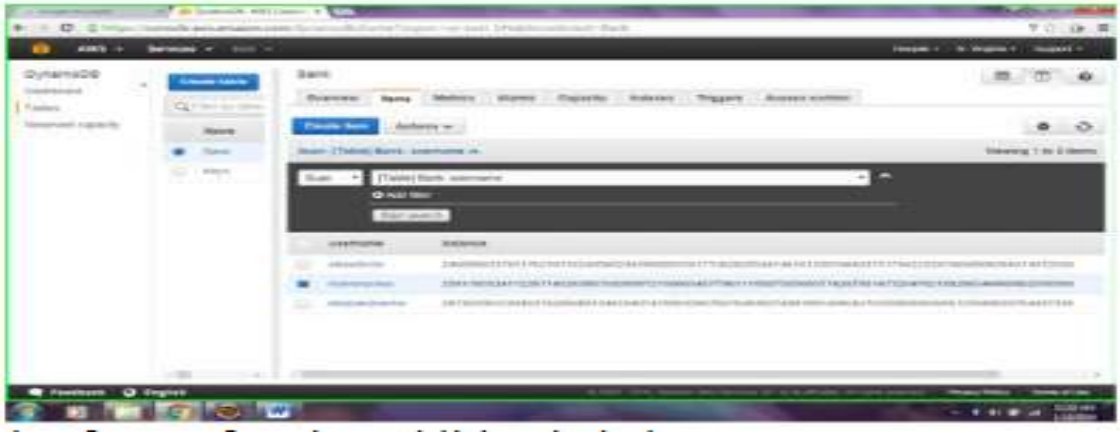
The DynamoDB comprise of two tables. The homomorphic encryption scheme encrypt the balance stored, users can add or subtract encrypted balance and check the same in plaintext as shown on fig.



DynamoDB Database

The Client code will be executed with sample operations as shown in figure.

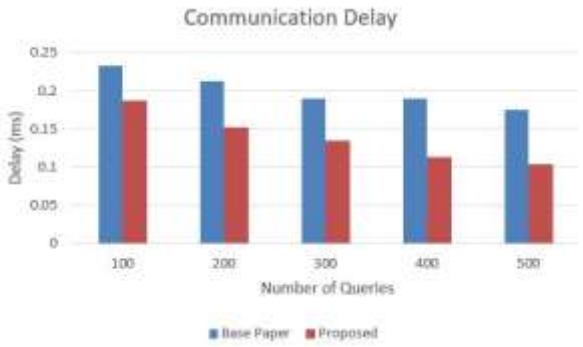
As shown in Figure, The execution of code will be done at client side and data will be updated on AWS DynamoDB table.



Data present in table of DynamoDB with inclusion of balance.

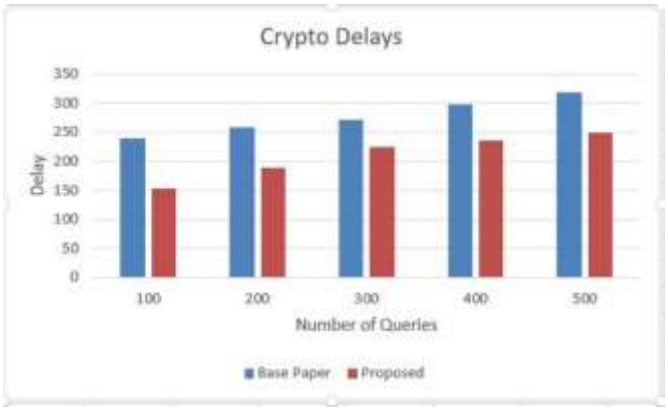
Graphs:

Communication delay:



The above figure depicts communication delay between proposed algorithm with the base paper and we can see that delay is decreased by 10% to 15% for number of queries.

Crypto delay:



Above fig is the comparison of only crypto delays between proposed and base paper we can see the reduction in the delay with number of queries.

Query Processing:

Query processing delay in above figure show algorithm works better with least delay in processing queries.

VII. CONCLUSION:

Cloud computing demand for storageof data is an absolute increase in demand graph and so the enhanced trends the various ways of data storage within the cloud is also gains a prime importance. If not protected in a rightful manner with a right technique data in cloud are eventually in danger.

This paper says about the problems and security attacks on data within cloud and also says how FHE can ensure the data confidentiality within the cloud without changing encrypted format. FHE allows the user to perform subtraction and addition operation on the encrypted data within the cloud and retrieve the data in the plain text at the user end's. The prime concerns of the paper issecurity of data and threat attacks and effective solutions to those in cloud computing. Data in several states has been discussed in conjunction with the techniques that are quite a bit more efficient for encryption of data within the cloud.

The data encryption and decryption will not be easy for any unauthorized person. For learning things better decryption will be done first and main issues are solved by encryption. Cloud computing will provide facility for carrying out task on encrypted data.

VIII. REFERENCES:

[1] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[C] Foundations of Secure Computation. New York: AcademicPress,1978:169-179

[2] Maha TEBAA, Said EL HAJII, "Secure Cloud Computing through Homomorphic Encryption", International Journal of AdvancementsinComputingTechnology(IJACT),Volume-5, Number-16, December 2013.

[3] ReemAlattas, Khaled Elleithy, "Cloud Computing Algebra Homomorphic Encryption Scheme Based on Fermat's Little Theorem", The American Society of Engineering Education, ASEE 2013, Northfield, VT, USA, 09 December 2016.

[4] Ryan Hayward, Chia-Chu Chiangb, "Parallelizing fully homomorphic encryption for a cloud environment", Journal of Applied Research and Technology 13 (2015), 245-252.

[5] FrederikArmknecht et. al., "A Guide to Fully Homomorphic Encryption", iacr, 2015.

[6] Rivest, Ronald L., Len Adleman, Michael L. Dertouzos, "On databanksandprivacyhomomorphisms.",Foundationsofsecure computation 4.11 (1978): 169-180.

[7] Rivest, Ronald L., Adi Shamir and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystems.", Communications of the ACM 21.2 (1978): 120- 126.

[8] A.C.Yao,"Protocolsforsecurecomputations"(extendedabstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.

[9] Goldwasser, Shafi and Silvio Micali, "Probabilistic encryption", Journal of computer and system sciences 28.2 (1984): 270-299.

[10] ElGamal, Taher, "A public key cryptosystem and a signature scheme based on discrete logarithms", Advances in cryptology. Springer Berlin Heidelberg, 1985.

[11]Paillier,Pascal,"Public-keycryptosystemsbasedoncomposite degree residuosity classes", Advances Heidelberg, 1999, in cryptology-EUROCRYPT99.

[12] Fontaine, Caroline, Fabien Galand, "A survey of homomorphic encryption for nonspecialists", EURASIP Journal on Information Security (2007).

[13] Craig G., "Fully homomorphic encryption using ideal lattices", STOC. Vol. 9. 2009.

[14] Smart, Nigel P., FrederikVercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes", Public Key Cryptography-PKC, Springer Berlin Heidelberg, 2010, P-(420-443).

[15] Van Dijk, Marten, "Fully homomorphic encryption over the integers", Advances in cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010. 24-43.

[16] Stehle, Damien, Ron Steinfeld, "Faster fully homomorphic encryption", Advances in Cryptology-ASIACRYPT 2010. Springer Berlin Heidelberg, 2010. 377-394. 4International Journal of Computer Applications (0975 - 8887) Volume 160 - No.6, February 2017

[17]Ramaiah,Y.GovindaandG.VijayaKumari,"Efficientpublic key homomorphic encryption over integer plaintexts", Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.
[18] SeyedNima, KhezrNima, JafariNavimipour. MapReduce and Its Applications, Challenges, and Architecture: a Comprehensive Review and Directions for Future Research(2017). J Grid Computing
[19] Rabi Prasad Padhy .International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.1, February 2013, pp. 16~27 ISSN: 2089-3337
[20] Min Zhao, Yang Geng.Homomorphic Encryption Technology for Cloud Computing8th International Congress of Information and Communication Technology, ICICT 2019
[21] V. Biksham, D Vasumati Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey International Journal of Computer Applications (0975 - 8887) Volume 160 - No.6, February 2017
[22] Monique Ogburna, Claude Turnerb, PushkarDahalc. Homomorphic Encryption, Procedia Computer Science 20 (2013) 502 – 509