International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Fuzzy Based Fully Homomorphic Encryption Scheme for Security in Cloud Computing

Navjeet Singh[1], Rimple Ahuja[2]

[1]CGC, Research Scholar, Department of Computer Science Engineering, Gharuan, SAS Nagar, India

[2]Chandigarh University, Assistant Professor, Department of Computer Science Engineering, Gharuan, SAS Nagar, India

Abstract: ***Cloud Computing is a model which is used for the delivery of appropriate and on-demand network access. Cloud Computing enables a user to accumulate the data in the cloud and access it directly from anywhere with the help of internet without the use of any hardware storage device. But, while the storage and accessing of data, Cloud Computing faces many complications such as security, congestion or traffic or management of resources. The security to the cloud can be provided by the means of data, storage and network. Hence, to provide the secure data storage and retrieval, many techniques have been proposed in the form of symmetric several cryptographic algorithms like symmetric and asymmetric key algorithms which encrypts the message to be sent. But, the previous techniques also faces some of the drawbacks which diminishes the functionality of Cloud Computing. To provide, secure data storage and retrieval, Fully Homomorphic encryption is being used in this paper which works on the concept of asymmetric key algorithm. This encryption technique provides specific types of computations to be taken out on ciphertext and also to obtain the outcomes in the form of encryption which then matches with the original text after the decryption. But, to reduce the size of data after the encryption in fully homomorphic scheme, the fuzzy rules are put into practice for the reduction of encrypted data in fully homomorphic scheme. The simulator used in this paper is MATLAB. The simulation results reveal that the proposed algorithm outperforms the previous one by reducing the size of encrypted and compressed data.***

Keywords: Cloud Computing, Fully Homomorphic Encryption (FHE), Encryption, Decryption, Security, Fuzzy Rules.

1. Introduction

Cloud Computing is an efficient technique which enables a user to store and retrieve the data on a cloud without the use of any type of utility devices. In, Cloud Computing the resources are reallocated on demand in a random manner among the multiple users and the users can share them easily. The concept of Cloud Computing is supplied rapidly and liberated with minimal management endeavors or an interaction of service provider. This scheme has many advantages for many of the businesses which include the state to start a new service in small instant of time. Cloud Computing has many outstanding achievements in the field of tasks which work on the concept to reduce the operational costs and utilization of services through cloud without the use of physical presence of resources such as memory and storage devices etc. Cloud Computing also exhibits the properties of grid computing also by addressing the Quality of Service (QOS) and the matters regarding reliability. Many tools and technologies have been provided by Cloud Computing for the construction of numerous computational applications [1]. The various famous clients of Cloud Computing are laptops, smartphones and many of the computer devices etc. Cloud Computing is composed of four diverse set of models such as Private, Public, Community and Hybrid models. The Private model is intended for the single organization and can be hosted internally or externally. The concept of Public model is provided for the usage by a particular organization as open model. The Community model is third type of model used in Cloud Computing which can be shared by various organizations. This type of model can be hosted externally and can only be hosted internally by any one of the organization [2].

Hybrid model is the fourth and last type of Cloud Computing model which is formed by the integration of two or more than two clouds which can be public or private in nature. This type of model can be hosted internally or externally [2].

1.1 Characteristics of Cloud Computing

Although, Cloud Computing shows its application with various technologies, it deals with many of adventurous models yet. The various types of models are listed below which deals with the concept of Cloud Computing in many ways.

- **Client-Server Model** – In the concept of Client-Server model, Cloud Computing concerns with many of the distributed applications which are implemented to get difference between servers which are used to provide the service and clients which are intended as service requestors [3].
- **Grid Computing** – The concept of grid computing is refers to a task which is perform particularly in distributed systems where many computer resources are combined to form a network named as Cluster to attain a common destination. The systems used in the formation of cluster are loosely coupled with each other.
- **Peer to Peer Process** – The idea of Cloud Computing is entirely based on the phenomenon of Peer to Peer strategy, where there exists no need for the central coordination. i.e. no need of administration point in the middle of client and server [3] [4].

1.2 Service Models of Cloud Computing

Cloud Computing is a three layered structure model which are named as Infrastructure, Platform and Application layers intended to provide many services to client and the server. These layers are also called Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (Iaas) [5]. The service model of Cloud Computing is

explained as follows.

- **Software as a Service –** This service of Cloud Computing is used to get access to application software and other databases. Saas is also referred to as on-demand software. Yahoomail and Hotmail are one of the famous examples of Saas.
- **Platform as a Service (Paas) –** This is one of an important paradigm of Cloud Computing in which many of the system software solutions are provided to the user such as operating system and the execution of programming language. The web servers are also included in this service of Cloud Computing. Microsoft Azure and Google App Engine are famous resources of Paas.
- **Infrastructure as a Service (Iaas) -** Google Drive and Amazon are some of the important services provided by Cloud Computing in the form of Iaas. As, the storage of huge quantity of data in many of GBs are only be stored in hard drives or large number of disk storages which are not easy to carry to certain places all the time. Hence, to overcome this issue, Iaas service is used by many organizations or companies with which the clients or users can get the data at any place without the use of hard drives etc [5] [6].

2. Literature Survey

In the year 1982, a scheme a scheme was proposed by Goldwasser and Micali [7]. On the proposed scheme, homomorphic encryption scheme is based. In the proposed scenario the computations of two large prime numbers i.e. n=p.q was used. This scheme of encryption is convenient in nature because it employs the product and a square. The main drawback of this scheme is that the input of this scheme is consisting of only one bit. In the year 1998, Okamoto and Uchiyama proposed a scheme which improved the performance of the schemes proposed in past upto a certain extent [8]. The values of n in this scheme changed to p^2q, and, the security in this scheme changed to the factorization value of n. The obtained value of expansion in this scheme is 3.

In the year 1999, a novel additive in nature scheme was proposed by pailler [9] which performed various improvements over exiting solutions and was able to reduce the value of expansion from 3 to 2. After this, Cramer and Shoup in 2002 proposed an efficient approach in the field of homomorphic schemes which provides a high security to the data [10]. In the year 2012, the authors use the fuzzy logic scheme for load balancing in cloud computing [4]. Load balancing method is used for improving the job response time by reassigning the total load to the individual nodes of the collective system. The author tried to implement the new load balancing technique based on Fuzzy logic. Where the fuzzy logic is natural like language through which one can formulate their problem. The author take the two input parameters considered the processor speed and load in virtual machine and make the better value to balance the load in cloud using fuzzy logic. It also contains rule-based structure of fuzzy logic, a series of IF-THEN rules.

The authors in the year 2013 discussed the homomorphic scheme [11] which has the capability to perform computations on the cipher text without decrypting it first. This encryption allows the transformation of cipher texts C (m) of message m, to cipher texts C (f (m)) of a computation/function of message m, without disclosing the message. The main drawback of this scheme is that after the encryption the size of data becomes large which becomes the cause for the heavy load or congestion for the network and storage of data.

3. Fully Homomorphic Encryption: An Approach

Although, Cloud Computing has many salient features, but it is facing various problems in the field of security as well as safety of data storage and retrieval. Hence, security to data in Cloud Computing has become an imperative concern which has to be reduced or minimized in order to get a secure and safe transmission [11]. Various techniques have been put forward to provide security and safety to Cloud Computing. Among all the proposed schemes, Fully Homomorphic Encryption (FHE) Scheme is one of the most widely used encryption scheme which is used to encrypt the data to be sent or stored into the cloud [12]. Homomorphic is the property or scheme which means the concept of encrypting the cipher data text before its decryption. On the other hand, FHE is a scheme which enables a user to do computations on that data which has been encrypted without decrypt it. FHE enables a user to perform the numeric calculations or some of simple aggregations on the encrypted data and also enables a user for the computation of random functions on the encrypted data [13] [14].

FHE scheme is based on the concept of asymmetric key encryption scheme which is used to secure the data from a diverse set of tasks. The plain as well as cipher text both are considered with the same algebraic function. In FHE scheme, a user can perform an operation on encrypted data without having the knowledge regarding the actual data [15]. In FHE scheme, the plaintext is changes to encrypted data and after the encryption the services of cloud comes into practice to provide the safe and secure storage of data.

Definition: An encryption is homomorphic, if: from Enc (x) and Enc (y) it is possible to compute Enc (f (x, y)), where f can be: +, ×, ⊕ and without using the secret key [16].

The flow of encryption and decryption of data in FHE and protection of data is explained as follows.

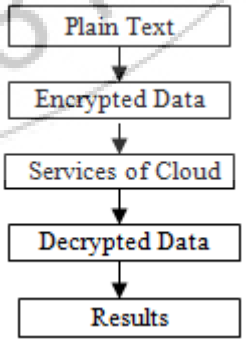

Figure 1: Protection of Data in FHE Scheme

Figure 1 clearly shows the work flow in FHE scheme which is used to protect the data to be encrypted.

4. Implementation of Fully Homomorphic Encryption Algorithm in Cloud Computing.

By the implementation of FHE mechanism, the secure and safe storage of data can be assured easily. By using FHE algorithm the ciphertext can be accessed directly by the user without knowing about the plain or actual text. In this work, FHE algorithm has been used for the construction of secure transmission of data scheme.

Select encrypt parameter: a, p and b, $a \sim 2^{n}$, $p \sim 2^{n2}$, $b \sim 2^{n5}$ where **p** is prime number

P is the secret key which is provided after the encryption without which the encrypted data can never be decrypted to get its original form.

Encrypt: for plain text **m**

Compute c=pb+2a+m where **c** is the cipher text

Decrypt: m=(c mod p) mod 2

Correctness: because pb is larger than 2a+m,

so (c mod p) =2a+m

Finally (c mod p) mod 2= (2a+m) mod 2=m

Homomorphic: for two cipher text

C1=b1p+2a1+m1

C2=b2p+2a2+m2

Compute:

C1+ C 2= (b1+b2) p+2(a1+a2) +m1+m2

So if 2(a1+a2) +m1+m2<<p

Then (c1+c2) mod p=2(a1+a2) +m1+m2

Hence, this is an additive homomorphic.

And c1*c2= [b1*b2p+ (2a1+m1) + (2a2+m2)] p+2(2a1

a2+r1m1+a2 m1) +m1 m2
So if 2(2a1 a2+a1m1+a2 m1) +m1 m2<<p
Then
(c1*c2) mod p=2(2a1 a2+a1m1+a2 m1) +m1 m2 [11]

5. Proposed Methodology

Cloud Computing plays one of the significant role for the storage and retrieval of data over the network without the use of drivers like hard disc drive etc. To secure the storage of data in Cloud Computing various schemes have been put forward among which FHE algorithm is one of the most efficient scheme which provides the security to the data to be stored or retrieved. But, by doing compression of data, the size of data becomes very large which act as a burden over the network. To overcome this issue, Fully Homomorphic Encryption Scheme using Fuzzy Rules is being proposed in this paper which reduces the load over the network while the compression of data.

The proposed scheme is then integrate with the Cloud Computing to provide security over the network. The flow of work is discussed in the flowchart which is described as follows.

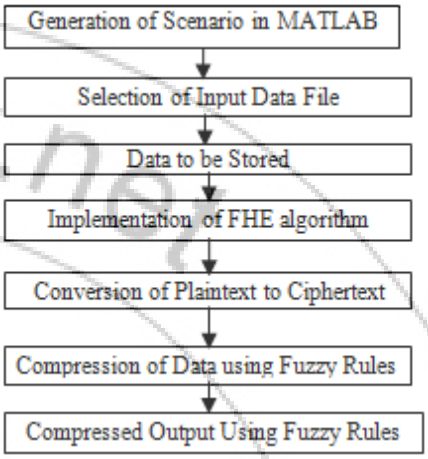

Figure 2: Flow of Work

Figure 2 represents the flow of work which is composed of five major steps. In Step 1, the selection of input data file which has to be comes into consideration. The Step 2 is the phase where the storage of data takes place. The implementation of proposed FHE algorithm is done in the Step 3 for the secure transference and compression of data. The conversion of plaintext into ciphertext takes place in the step 4. The last step is the step 5 where the proposed and novel algorithm FHE using Fuzzy Rules are integrated with whole of the system of Cloud Computing which compresses the data and reduces its size upto an efficient extent. In our proposed work, the seven fuzzy rules are used which are shown as follows.

1. If (e is NB) and (ec is NB) then (kp is PB)(ki is NB)(kd is PS) (1)
2. If (e is NB) and (ec is NM) then (kp is PB)(ki is NB)(kd is NS) (1)
3. If (e is NB) and (ec is NS) then (kp is PM)(ki is NM)(kd is NB) (1)
4. If (e is NB) and (ec is Z) then (kp is PM)(ki is NM)(kd is NB) (1)
5. If (e is NB) and (ec is PS) then (kp is PS)(ki is NS)(kd is NB) (1)
6. If (e is NB) and (ec is PM) then (kp is Z)(ki is Z)(kd is NM) (1)
7. If (e is NB) and (ec is PB) then (kp is Z)(ki is Z)(kd is PS) (1)

Figure 3: Fuzzy Sets

6. Simulation Results and Discussion

In this section, the simulation results have been carried out by using the proposed algorithm FHE using Fuzzy Rules. The simulator used for the compression of data and to provide security is MATLAB 7.11. We have to browse the input file in the first step by clicking on data button and then encoded it.

The representation is shown in the Figure 2.

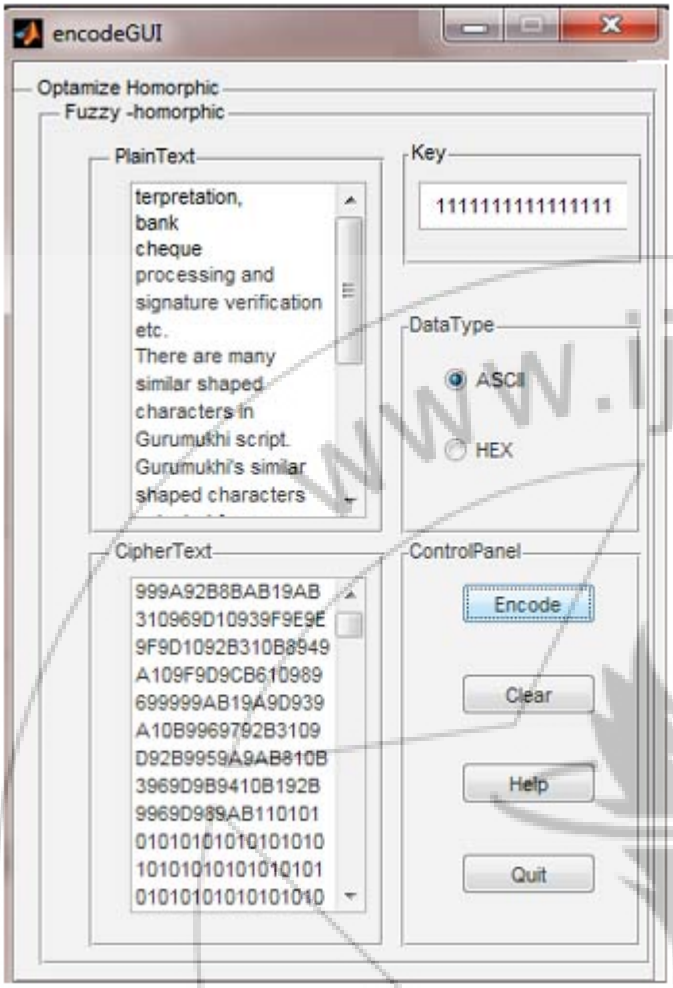

Figure 4: Encoding

Figure 5: Compressed Sizes

From figure 5, it can easily be shown that after the process of encoding the file is being compressed. The above figure is showing the compressed size of the file.

7. Conclusion and Future Scope

The concept of cloud computing is one of the most important concept which enables the user to store and retrieve the data on or from a cloud respectively via internet and without the use of any storage device. The main issue in terms of security is a major concern in Cloud Computing. Hence, for the secure transmission of data, various schemes has been used in past. In the proposed work, FHE algorithm using Fuzzy Rules is being used which reduces the size of the compressed data after encryption. This algorithm also shows significant results over previous algorithms.

Hence, from the above results obtained in the figures, it can easily be concluded that the proposed algorithm i.e. FHE algorithm has major advantages over conventional works which are used in Cloud Computing to provide security and safe transmission over the network.

References

[1] I. Ahmad, A. Khandekar, "Homomorphic Encryption Method Applied to Cloud Computing," International Journal of Information & Computer Technology, 15, pp. 1519-1530, 2014.
[2] A. Patrascu, D. Maimu, Emil Simion, "New Directions in Cloud Computing: A Security Perspective", IEEE, 2012.
[3] M. Creeger, "CTO Roundtable: Cloud Computing," ACM Queue, pp. 1-2, 2009.
[4] S. Sethi, A. Sahu, S.K. Jena, "Efficient Load Balancing in Cloud Computing using Fuzzy Logic," IOSR Journal of Engineering (IOSRJEN), 2(7), pp. 65-71, 2012.
[5] R. Buyya, Chee Shin Yeo, S. Venugopal, J. Broberg,, I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems, 25(6), pp. 599-616, 2009.
[6] A. Iosup, S. Ostermann, N. Yigitbasi, R. Prodan, T. Fahringer, D. Epema, "Performance Analysis of Cloud Computing Services for Many-Tasks Scientific Computing", IEEE TPDS, MANY-TASK COMPUTING, 2010.
[7] S. Goldwasser, S. Micali, "Probabilistic encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
[8] T. Okamoto, S. Uchiyama, "Security of an Identity-Based Cryptosystem and the Related Reductions" in Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, 1403, pp. 546–560. Springer, Heidelberg.
[9] P. Paillier,"Public-Key Cryptosystems Based on Composite Degree Residuosity Classes" in Stern, J. (ed.) EUROCRYPT 1999. LNCS, 1592, pp. 223–238. Springer, Heidelberg.
[10] R. Cramer, V. Shoup, "Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption," in Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, 2332, pp. 45–64. Springer, Heidelberg.
[11] B.K. Mohanta, D. Gountia, "Fully homomorphic encryption equating to cloud security: An approach," IOSR Journal of Computer Engineering, 9(2), PP 46-50, 2013.
[12] Parin V. Patel, Mr. Hitesh D. Patel, Prof. Pinal J. Patel, "A Secure Cloud using Homomorphic Encryption Scheme", International Journal of Computer Science Research & Technology (IJCSRT) Vol. 1 Issue 1, June-2013.

[13] Jing-Li Han, Ming Yang, Cai-Ling Wang, Shan-Shan Xu,"The Implementation and Application of Fully Homomorphic Encryption Scheme", IEEE 2012.
[14] Z. Brakerski, V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe" in FOCS, IEEE, pp. 97–106, 2011.
[15] S. Ravindram, P. Kalpana, "Data Storage Security Using Partially Homomorphic Encryption in a Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), 2013.
[16] M. TEBAA, S.E. Hajji, A.E. Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", WCE 2012, London, U.K

Author Profile

Er. Navjeet Singh has completed his B.Tech in Computer Science and Engineering from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India in the year 2012. He is currently pursuing M.Tech in Computer Science and Engineering, CGC, Gharuan. His area of Interest is Cloud Computing.

Rimple Ahuja is presently working as a Asst. Prof in ICS ASM Group of Institutions, PUNE. She has completed her M.Tech degree in CSE from Bansathali university. Her areas of Interest are in Cryptography and Steganography.