www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 3 March 2018, Page No. 23785-23789
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i3.22

Homomorphic Encryption Using Enhanced BGV Encryption Scheme For Cloud Security

S.V.Suriya prasad[1], K.Kumanan [2]

[1]M.E Student: Department of Computer Science and Engineering
Sri Venkateswara College of Engineering
Sriperumbudur, India
suriyaprasadsv95@gmail.com
[2]Assistant Professor: Department of Computer Science and Engineering
Sri Venkateswara College of Engineering
Sriperumbudur, India
kkumanan@svce.ac.in

Abstract
Fully Homomorphic Encryption is used to enhance the security incase of un-trusted systems or applications that deals with sensitive data. Homomorphic encryption enables computation on encrypted data without decryption. Homomorphic encryption prevents sharing of data within the cloud service where data is stored in a public cloud . In Partially Homomorphic Encryption it performs either additive or multiplicative operation, but not both operation can be carried out at a same time. Whereas , in case of Fully Homomorphic Encryption both operations can be carried out at same time. In this model , Enhanced BGV Encryption Technique is used to perform FHE operations on encrypted data and sorting is performed using the encrypted data

Keywords—FHE, BGV.

I. Introduction

Homomorphic encryption is a form of encryption which performs arbitrary computations on encrypted data. In cloud computing we may keep our sensitive data in encrypted format, but if you want do any calculation on ciphertext, the key must be share with cloud service providers which may cause to exploit our data. So that to avoid share the key to CSP's instead use the Homomorphic Encryption technique. The computations include searching, sorting, addition, multiplications performed on ciphertext. There are two type of homomorphic encryption techniques.
Partially homomorphic technique, operations are performed on the encrypted data. These operations either additive or multiplicative operation, but not both operation can be carried out at a same time.

In Fully Homomorphic encryption both operations can be carried out at same time. Due to this security mechanism for encrypted data is improved. The first system is a lattice-based encrypted system developed by Craig Gentry in 2009.Fully homomorphic encryption (FHE) and is more powerful technique compared to Partially homomorphic encryption. Ideal lattices provide both additive and multiplicative homomorphisms. A cryptosystem that braces arbitrary computation on ciphertexts is known as Fully homomorphic encryption.

Craig Gentry implemented fully homomorphic encryption based on bootstrapping over partially homomorphic encryption by using ideal lattices. It is limited because each ciphertext is noisy in some sense, and this noise grows as one adds and multiplies ciphertexts.Gentry showed that any bootstrappable Somewhat Homomorphic Encryption scheme can be converted into a Fully Homomorphic Encryption through a self-embedding recursion. In case of Gentry's "noisy" scheme , the bootstrapping procedure effectively "refreshes" the

ciphertext by applying to it the decryption procedure homomorphically, thereby obtaining a new ciphertext that encrypts the same value as before but has lower instance of noise. The ciphertext is periodically "refreshed" whenever the noise grows too complex .

Enhanced BGV encryption scheme is used to perform fully homomorphic operations using the encrypted data within the cloud environment.Data remains in encrypted state all throughout the cloud environment, by this confidentiality of the data is maintained.In the proposed BGV scheme , new sorting technique was constructed in order to sort encrypted data within the cloud encryption.

II. Literature Survey

The survey of related works and techniques used in other papers are listed below.

Alhassan Khedir et al (2016) proposed a paper "SHIELD: Scalable homomorphic Implementation of Encrypted Data-Classifiers". In this work, they described about optimized Ring Learning With Errors (RLWE) based implementation of a variant of the HE system recently proposed by Gentry, Sahai and Waters (GSW). Although this system was widely believed to be less efficient than its associates, they demonstrated quite the opposite behaviour for a huge classes of applications. They first highlight and carefully exploit the algebraic features of the system to achieve significant speedup over the state-of-the-art HE implementation, namely the IBM homomorphic encryption library (HElib). They commenced various optimizations on top of HE implementation, and used the resulting scheme to construct a homomorphic Bayesian spam filter, secure multiple keyword search, and a homomorphic evaluator for binary decision trees [1].

Ayantika Chatterjee et al (2017) proposed a paper "Sorting of Fully Homomorphic Encrypted Cloud Data: Can Partitioning be effective?" In this work, they have considered sorting on encrypted data, which is a frequently required database operation. They have investigated the feasibility of performing comparison as well as partition based sort on CPA resistant FHE data and highlight an important observation that time requirement of partition based sort on FHE data is no better than comparison based sort owing to the underlying security of the cryptosystem. They proposed a FHE specific two stage sorting technique termed as Lazy sort with reduced recrypt operation, which proves to be better in terms of performance on FHE data in comparison to partition as well as comparison sort. Finally, they provided some multi-core implementation results to show that with proper implementation tricks performance of FHE computations can be improved further [2].

Ayantika Chatterjee et al (2015) proposed a paper "Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud",they made an initial effort to highlight the problem of translating algorithms that can run on unencrypted or normal data to those which operate on encrypted data. They also showed that although FHE provides the ability to perform arbitrary computations, its complete benefit can only be obtained if they also allow to execute arbitrary algorithms on encrypted data [3].

Devavrat Bapat et al (2015) proposed a paper "A Cloud Computing Security Solution Based on Fully Homomorphic Encryption". Cloud computing security becomes the main research focus and it is also this paper's research focus. In order to solve the issues of data security in cloud computing system, they introduced fully homomorphism encryption algorithm in the cloud computing data security. A new kind of data security solution to the insecurity of the cloud computing is proposed and the scenarios of this application is hereafter constructed. This recent security solution is fully fit for the processing and retrieval of the encrypted data, and effectively leading to the broad applicable prospect, the security of data transmission and the storage of the cloud computing [4].

Ihsan Jabbar et al(2016) proposed a paper "Using Fully Homomorphic Encryption to Secure Cloud Computing"This paper deals with the use of homomorphic encryption to encrypt the client's data in cloud server and also it enables to execute required computations on this encrypted data.The concept of cloud computing receiving a great deal of attention both in publication and among users. Cloud computing is the delivery of computing services over the Internet.The distance between the client and the physical location of his data creates a barrier because this data can be accessed by a third party and this would affect the privacy of client's data [5].

Iram Ahmad et al (2014) proposed a paper "Homomorphic Encryption Method Applied to Cloud Computing" in this work ,when the data is transferred to the Cloud they used a standard encryption methods to secure this data, but when they wanted to do the calculations on data located on a remote server, it is necessary that the Cloud provider has access to the raw data, and then it will decrypt them. In this paper they proposed the application of a method to perform the operation on encrypted data without decrypted and provide the same result as well that the calculations were carried out on data[6].

Jung Hee Cheon et al (2015) proposed a paper "A Hybrid Scheme of Public Key Encryption and Somewhat Homomorphic Encryption" In this model, messages are encrypted with a PKE and computations on encrypted data are carried out using SHE or FHE after homomorphic decryption. To obtain efficient homomorphic decryption, our hybrid scheme combines IND-CPA PKE without complicated message padding with SHE with a large integer message space. Furthermore, if the underlying PKE is multiplicative, the proposed scheme has the advantage that polynomials of arbitrary degree can be evaluated without bootstrapping. They constructed this scheme by concatenating the ElGamal and Goldwasser-Micali schemes over a ring ℤN for a composite integer N whose message space is ℤN×.To accelerate the homomorphic evaluation of the PKE decryption, they introduced a method to reduce the degree of the exponentiation circuit at the cost of additional public keys [7]

III. Proposed System

The main aim of the proposed system is to perform fully homomorphic operations (Additive, Multiplicative) and to develop a Sort technique to fetch encrypted data. The proposed system is shown in fig1; it will be explained detail as follows,

A. Key Generation

Key Generation is used to generate both public key and secret key which are required for the encryption of the data. Secret key is generated randomly from n bits(large odd number) and public key is generated randomly from n^5 bits which are fused along with less noise.

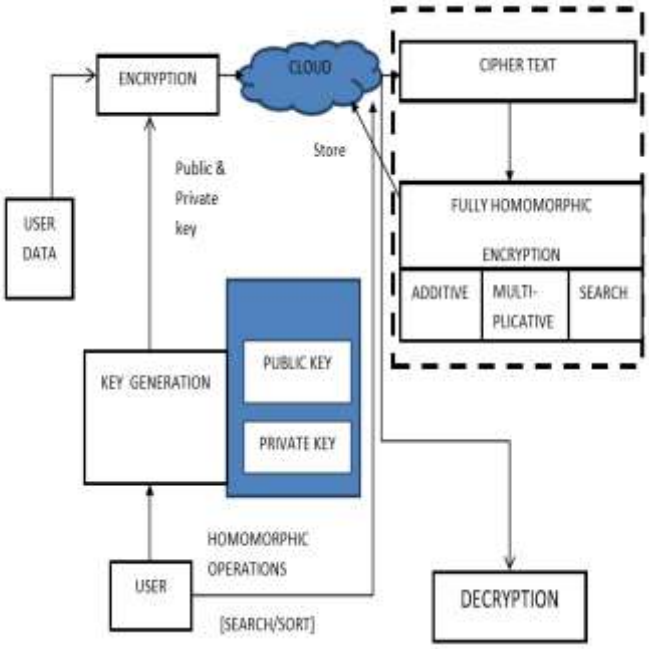


Fig1. Block diagram for enhanced BGV Encryption scheme

B. Encryption

Encryption is a very important step in Cloud Security. Proper Encryption will increase the Security. In the proposed Encryption Scheme the data given by the user are encrypted along with both the keys.Encrypted data is stored in the Cloud. .

Encryption:

Sk :A large odd number (n bits)

To encrypt a bit M

Q:Random large multiple of p (n^5 bits)

R:Random small even number 2.r(noise)

CT: Q*Sk+2R+M

Sk	Secret Key
Q	Public Key
R	Noise
CT	CipherText
M	Message

C. Computational Module

Based on the fully homomorphic operation selected, computations are performed and stored on the cloud.

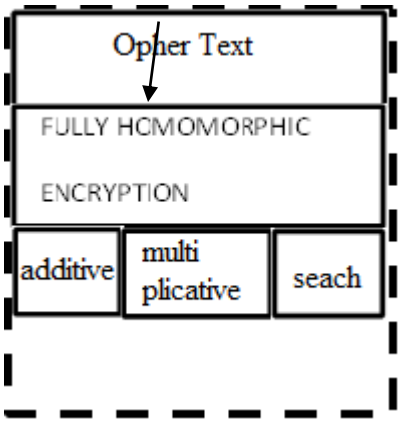


Fig2. Block diagram for Computational Module

Additive module

This module performs addition operation between the encrypted messages and stores the result in the cloud.

Multiplicative Module

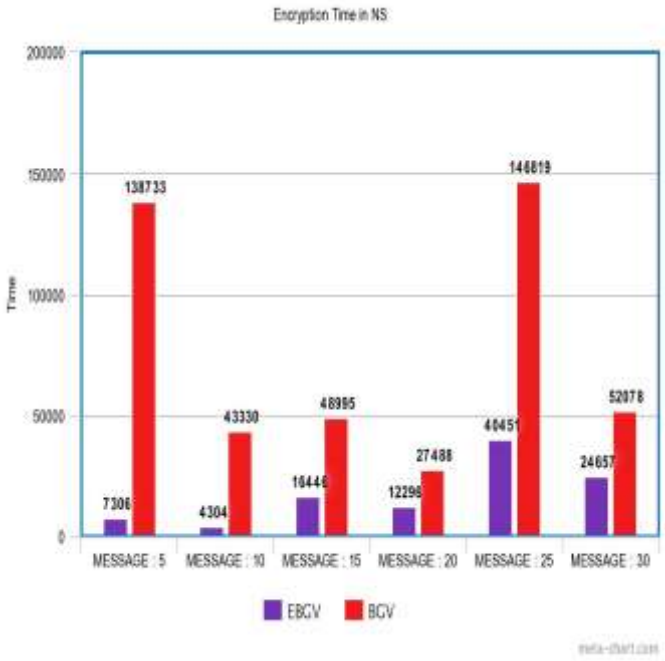
This module performs multiplication operation between the encrypted messages and stores the result in the cloud.

Search Module

This module performs search operation over the encrypted data.

IV. Experimental Study

The proposed model is analyzed by executing set of experiments in the open source eucalyptus tool. The experiments are carried out in a cloud setup using eucalyptus tool which contains cloud controller and walrus as storage controller on a 5 node cluster.Each node has two 3.06 GHz Intel (R) Core TM Processors, i-7 2600, CPU @3.40GHZ, 4 GB of memory and 512 GB hard disks, and running eucalyptus in it.



V. Conclusion

Homomorphic cryptosystems allow for the same level of privacy as any other cryptosystem, while also allowing for operations to be performed on the data without the need to see the actual data with Enhanced BGV encryption scheme.The security of Cloud Computing helps to analyze and improve the existing cryptosystem to allow servers to perform various operations requested by the client and to improve the complexity of the homomorphic encryption algorithms.

REFERENCES

1. Alhassan Khedr (2016)" SHIELD: Scable homomorphic Implementation of Encrypted Data-Classifiers" ,in IEEE Transactions on computers,, Volume: 65, Issue: 9, Page (s):2848-2858
2. Ayantika Chatterjee and Indranil Sengupta (2017) "Sorting of Full Homomorphic Encrypted Cloud Data: Can Partitioning be effective?" DOI 10.1109/TSC.2017.2711018, IEEE Transactions on Services Computing
3. Ayantika Chatterjee and Indranil Sengupta (2015) "Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud" DOI 10.1109/TCC.2015.2481416, IEEE Transactions on Cloud Computing
4. Devavrat Bapat, Aakash Patil ,Dashrath Degavat , Gaurav Deshpande , Shwetambari

Chiwhane(April 2015)“A Cloud Computing Security Solution Based on Fully Homomorphic Encryption ”International Journal of Advanced Engineering and Global Technology.

5. IramAhmad andArchanaKhandekar (2014) ”HomomorphicEncryption Method Applied to cloud computing” International Journal of Information & Computation Technology.
6. IhsanJabbar, SaadNajim (May 12, 2016)”Using Fully Homomorphic Encryption to Secure Cloud Computing ” Internet of Things and Cloud Computing.
7. Jung HeeCheon and JinsuKim(2015)“A Hybrid Scheme of Public Key Encryption and Somewhat HomomorphicEncryption”,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,VOL.10,NO. 5
8. Suraj Sheshrao Gaikwad, Amar R. Buchade(Sep-2016)”Homomorphic Encryption Approach For Cloud Data Security”International Research Journal of Engineering and Technology (IRJET).