Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Homomorphic Encryption Security for Cloud Computing

J.Phani Prasad

Received: 16 December 2018 Accepted: 3 January 2019 Published: 15 January 2019

Abstract

As the Data and Technology is increasing day by day the security and privacy issues are becoming a major concern now a days, with the advent of different security mechanisms there are some bottlenecks. In this work we are giving the essence and importance of an encryption scheme called homomorphic encryption and its related issues.

Index terms— encryption, homomorphic encryption, RSA, security.

1 Introduction

ecurity of the Data or information is a primary concern of the day to day transactional process. There are various domains in which security can be provided as a part of protecting the things and systems, some of the security areas or domains are: home automation and security, providing the security to data pertaining to different organizations. The nominal and quite common security providing methods is usage of passwords in the form of text to our data and having some sort of security to it.

Another form of password protection other than text is providing captcha, or one time passwords now a days. In search engines like Google we can keep multiple authentication schemes like each time one enters in to his Gmail account one can put two factor authentication.

Apart from the above methods we can encrypt our data while storing it/sometimes whenever we send our information to someone, lot of encryption algorithms and methods are available like DES, AES, RSA, Blow fish and many more, and at the other side the receiver will use a method called decryption to receive the actual data from sender. Cryptography is the method of converting plain text to cipher text. By this method one can just read our data and use it for his purpose without altering that data. Liu (2012) has introduced some cloud computing system and also analyzes cloud computing security problem. He suggested that single security technique cannot be used to solve the cloud security problem therefore, many traditional and some new strategies are required to use together to provide the total security in cloud.

2 II

Ustimenko and Wroblewska (2013) proposed an idea for homomorphic encryption and multivariate key for cloud security. They have given detailed discussion on Key Dependent Message (KDM) encryption scheme can be used for cloud security.

Ramgovind et al. (2010) highlighted key security considerations currently faced by industry.

Aderemi and Oluwaseyi (2011) discussed about the security issues in cloud computing and the potentials of homomorphic encryption, and proposed an encryption layer on top of the encrypted data on the cloud.

3 III.

4 HOMOMORPHIC ENCRYPTION

Homomorphic encryption is a Technique that permits the calculation on encrypted data without prior decryption and after operation, if the data is decrypted by user which is in encrypted form it gives actual result without knowing the actual plain text (yang et al. 2014).

Suppose if plain text is M.

5 Operation(M) decrypt(Operation(encrypt(M))).

In figure1 (below) homomrphic encryption is applied on some set of integer values using some algorithm. For encryption algorithm is implemented as 7*2=14 where 2 is the encrypted element in the above operation, and for 5 ie 5*2=10. The reverse process is followed for decryption of data here after multiplication (14*10)/2 =70 it is divided by 2 because of homomorphic encryption property, after decryption of result we will get 7*5=35 which is actual result.

6 IV. Homomorphic Encryption and Types

There are three types of Homomorphic encryption available:

7 Partial Homomorphic Encryption(PHE)

In this encryption technique it performs single operation on encrypted data i.e either multiplication or addition but not both.

8 Some What Homomorphic Encryption(SWHE)

In this technique it support limited number of addition and multiplication operations on encrypted data.

9 Fully Homomorphic Encryption(FHE)

In this technique it support both multiplication and addition operations and also any other computations also possible on encrypted data.

10 a) RSA and Homomorphic Encryption

RSA is a asymmetric algorithm used for encryption of the data , which was introduced by Ron Rivest, Shamir and ad leman , it is mainly used for encryption using public and private key concepts till now, but it can be combined with homomorphic encryption. End.

11 The properties of

V.

12 Partial Homomorphic Encryption

Partial homomorphic encryption can be implemented in various domains like network security, cloud computing, Big data and many other fields where security of data and storage is the major concern.

For example if we take cloud to secure the data, so many encryption and decryption algorithms are in to practice, but among them the Partial Homomorphism is the technique which reduces the amount of computation when compared with other algorithms.

VI. Implementation of RSA as PHE using a Case Study on Cloud

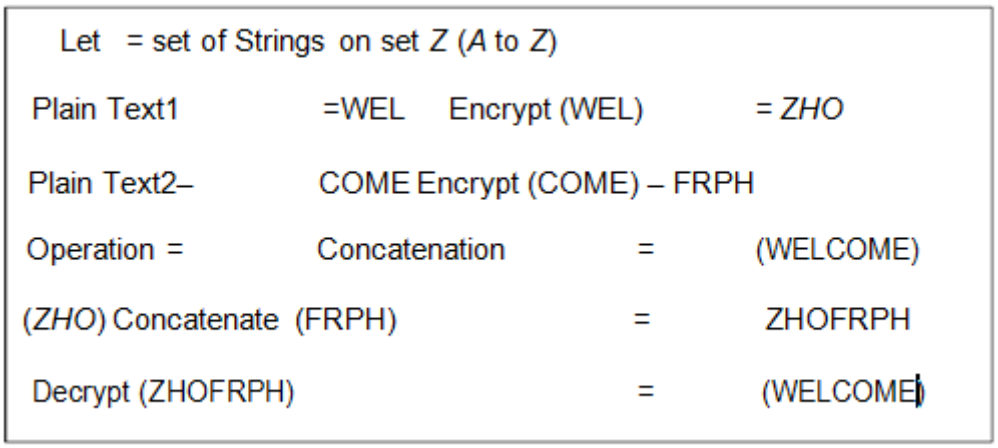
We are implementing a small case study by taking the length and breadth of 50 grounds and the number of persons visiting the ground for playing and other activities. Ground shape is assumed to be different i.e (rectangle or square). The data is encrypted and it is stored in a cloud by the user, and whenever it is required user can compute the area of the ground. cloud, and the area is computed with the help of encrypted data by the formula (encrypt (length)*encrypt(breadth)) and the computed result is sent to user. The user takes the encrypted form of data and decrypts it by using private key as {27,33} to get the actual area of the ground.

13 VII. CONCLUSION

In this work we have discussed about the homomorphic encryption technique as a method of providing security to the data in various fields, and mainly on cloud. We have also implemented RSA as a partial homomorphic technique on cloud by taking a case study. In future it may be extended and the research directions to be driven towards fully homomorphic encryption technique. [1] [2]

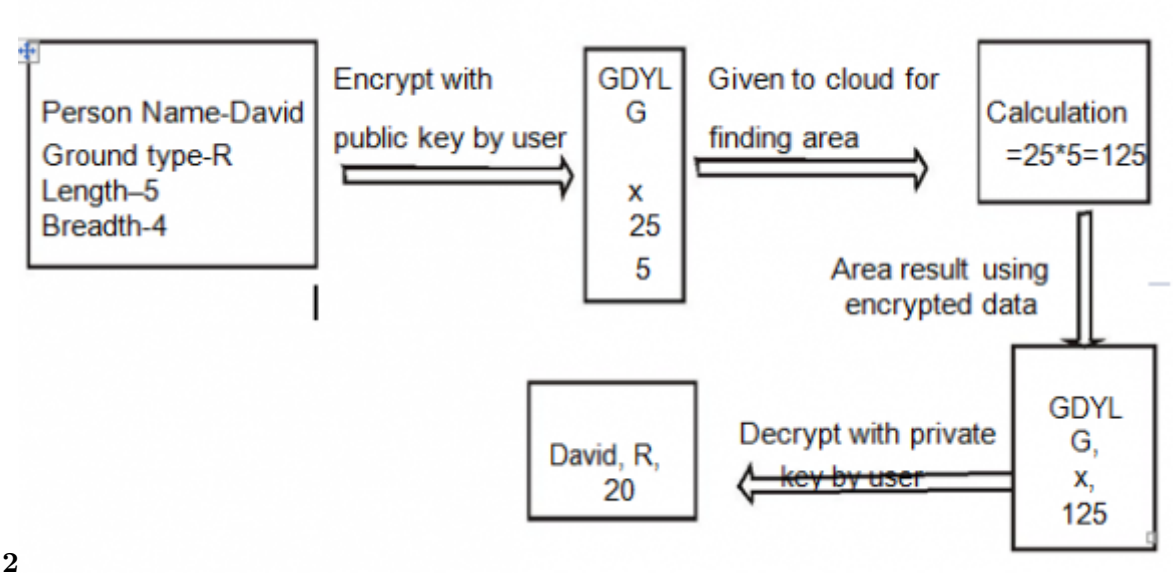
[1] © 2019 GlobalHomomorphic Encryption Security for Cloud Computing

[2] © 2019 Global JournalsHomomorphic Encryption Security for Cloud Computing



1

Figure 1: Figure 1 :



2

Figure 2: Figure 2 :

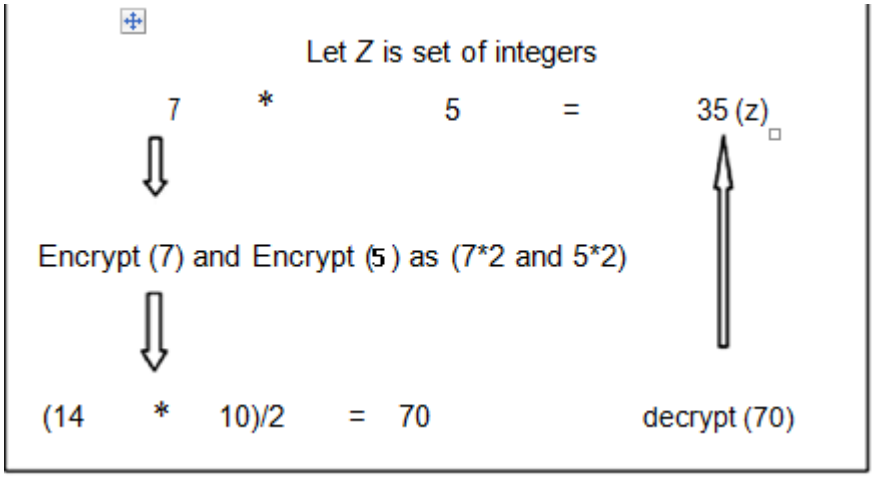


Figure 3:

Bin (2013) surveyed on specific security issues and use of cryptography in cloud computing.
Carlos et al. (2013) discussed about the recent advances in homomorphic encryption techniques. They have done survey on recent advances in Somewhat Homomorphic Encryption (SWHE) Homomorphic Encryption (FHE) algorithms.
LITERATURE REVIEW
Rivest et.al.(1978) introduced for the first time the concept of Homomorphic encryption. Taher (1985) introduced an algorithm based on multiplicative property.
Shahzadi et al (2012) done the study on the three homomorphic encryption algorithms. Naser and
Author ?: Assistant Professor, Vardhaman College of Engineering, Hyderabad. e-mail: phanimtechcse@gmail.com
Author ?: Professor, Vardhaman College of Engineering, Hyderabad.

Figure 4:

[Gamal ()] 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms'. Taher El Gamal . *Advances in Cryptology*, (Berlin Heidelberg) 1985. Springer. p. .

[Farah ()] *An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms*, Shahzadi Farah . 2012. (Recent Advances in Information Science, Proceeding of the 3 rd European Conf. of Computer Science, (EECS-12)

[Garima and Rama ()] 'Cloud Computing Implementation: Key Issues and Solution'. Rastogi Garima , Sushil Rama . *Proceedings of IEEE Conference INDIACOM*, (IEEE Conference INDIACOM) 2015. p. .

[Rastogi and Sushil ()] *cloud computing security and homomorphic Encryption*, Garima Rastogi , Rama Sushil . 2015. p. .

[Gentry ()] 'Fully Homomorphic Encryption Using Ideal Lattices'. C Gentry . *ACM Symposium on Theory of Computing*, 2009. p. .

[Monique et al. ()] 'Homomorphic Encryption'. Ogburn Monique , Turner Claude , Dahal Pushkar . Proceeding Computer Science 2013. 20 p. .

[Ronald et al. ()] 'On Data Banks and Privacy Homomorphism'. Rivest Ronald , L , Adleman Leonard , M , Dertouzos Michael . *Foundations of Secure Computation* 1978. 4 (11) p. .

[Aguilar Melchor et al. (2013)] 'Recent Advances in Homomorphic Encryption'. Carlos Aguilar Melchor , Simon Fau , Caroline Fontaine . *IEEE Singal Processing Magazine* 2013. March. p. .

[Wentao ()] 'Research on Cloud Computing Security Problem and Strategy'. Liu Wentao . *Proceedings of IEEE Conference*, (IEEE Conference) 2012.

[Ramgovind et al. ()] 'The Management of Security in Cloud Computing'. S Ramgovind , M Eloff , E Smith . *Proceedings of IEEE Conference*, (IEEE Conference) 2010.

[Naser A W S And Bin Md Fadli ()] 'Use of Cryptography in Cloud Computing'. Naser A W S And Bin Md Fadli . *Proceedings of IEEE International Conference on Control System*, (IEEE International Conference on Control SystemMalaysia) 2013. p. .