International Journal of Engineering & Technology, 7 (3.3) (2018) 110-113

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Novel Homomorphic Encryption Scheme in Cloud Computing

C.Veena[1]*, Dr M. Hanumanthappa[2]

1 Scholar, Rayalaseema University, Kurnool, A.P
[2]Professor & Chairman Dept of Computer Science & Applications, Bangalore University, Bangalore.[3]Affiliation of the third author
**Corresponding author E-mail: cveena30@gmail.com*

Abstract

Cloud computing is an indispensable technology for any business organization, such as banking, e-commerce, etc. Although technology has advantages in many areas; The protection of stored data is a major concern for all stakeholders in the architecture. Provide data security with respect to network security, control strategies and access to the service, data storage. Despite the efforts of service providers to build customer trust in data security, users need a passion for using technology for their business skills. Homomorphism coding is a data protection technique in which tasks can be performed on encrypted data themselves. In this article, we present an exploration of new homomorphism encryption methods with respect to data security and their use in cloud computing.

Keywords: *Cloud Data storage, Data Security, Fully Homomorphic Encryption, Homomorphism Encryption, HomomorphicKey.*

1. Introduction

As per the National Standards and Technology (NIST) definition, Cloud Computing is a model for universal, helpful, and on-request organize access to a mutual pool of configurable processing assets that can be sent and discharged rapidly with insignificant exertion. Administration exertion or collaboration with a specialist co-op. He additionally characterized five key highlights of distributed computing: on-request self-benefit, wide system get to, asset pooling, quick elasticity, and measured service [1]. There are three types of services offered by cloud providers. They are i) infrastructure-like-service where core computing resources, storage and processing power are offered as a service, ii) platform-service where users can define their applications in the tools offered by them. service providers with the development language and iii) software is the service are the services in which client applications are run on the infrastructure provided by the service providers. For all these services, users do not need to manage or manage the cloud infrastructure, including the network, server, operating system, storage, and even application functions [2]. The fact that technology users use the services offered by service providers is partly due to the fact that confidentiality of data storage confidentiality is not fully known to users [3]. We, the users, use traditional cryptographic techniques to make sure that the safety of the data while distribution data the cloud also the data is store in the same design. But for service providers to be able to perform the operations requested by the customer, the data must be available in clear format. This requirement of suppliers raises the question of confidentiality. To solve this problem, service providers must use techniques that ensure confidentiality and ensure that customers never affect the data in attack time. The solution to this problem is to code everything all the time, that is, to code Homomorphically. With Homomorphism Encryption, the data will not be clear in the complete treatment [4]. The main objective of this article is to analyze the utility and threats that service provider's face when incorporating homomorphism encryption schemes to ensure the confidentiality of stored data.

2. System study

1.1. Homomorphic Encryption Schemes

Data clouds, in that not encrypted design. If the encrypted storage space in the form of, such as the availability of the problems, it can be given to the third, in safety and in the power of it is solved. However, a problem with the cloud service provider to offer a user cannot rely on the data. The computation the user, that had been sent on to this end was arranged. And so, for the first time, and real intimacy with the secret of the cloud and eliminate elite decode, and then send the user account. In this salad, the coding homomorphic receives a call credit. [5] Homomorphic encryption methods are thought to process through the web Cypsum 100 (1000) of 100 to 1000 word in the text encode (f (1000)), the computation / 1000 function of the word without revealing the message. In general, an encryption algorithm contains a three-step system. are,

1. Key Generation - generates two key, key private and public key SK T.
2. Encryption - in readable text into encrypts the public key pk to provide basic code c.
3. Decoding - c decodes the code word with a secret key SK to recover readable in.

Apart from the three stages, Holomorphic encryption schemas includes four stages, in storage, application, assessment and response. The thing about the new encryption Holomorphic can be summarized as follows and are illustrated in Figure I.

Google Translate Community Mobile

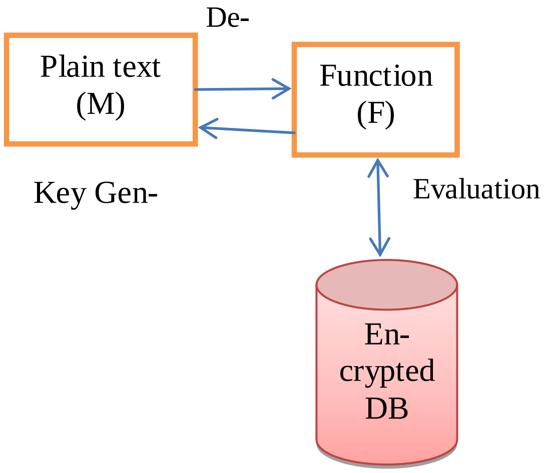

Figure 1. Structure of Holomorphic Encryption Method

One of them is coded with the key to store the information in the database. When we want to work, ask for a service provider. It would also be in the process of the process itself the appeal of the service provider; mechanism at the demand of the slave server. The service provider has then processed to result in a response time of the customer. And finally back to the customer service provider deciphering result is the surreptitious key SK. Under homomorphic coding is perform on the data on which the banking data can be classified into three types: homomorphic encryption part (Phe), Some What Homomorphism encryption (SWHE) and fully homomorphic encryption (FHE) [6].

• Increasing Phe does not allow partial homomorphism encryption (Phe) as far as I go, also data is not encrypted or

• Some What Homomorphic Encryption (SWHE) SWHE makes much more than going, but it was incomplete in number.

• Fully homomorphic encryption (FHE) EHF also adds the number of increase procedure to be performing on encrypted data.

2.2. He Schemes In Cloud Storage-Challenges

Here are some of the challenges offered by higher education systems that we have taken into account in our work: a) effectiveness b) durability c) delays. The PHE algorithms are very effective in providing model application and data security, where data can be encrypted during data transmission. They are very useful for the SaaS or PaaS cloud service model, but they are not particularly useful in the IaaS model product because they require the sending of a secret key at a specific time, usually when the VM starts.] Their robustness depends on the size of the encryption key. But using a large key, the system is too slow. Large public keys affect the coding text size, encryption time, decoding time and data processing time.

Parameters to consider when using homomorphic encryption systems are

a) That the size of the encryption key

b) That the size of the effect encryption key in the code text

c) It is time to encode

(d) Decoding time and

e) Private Key;

Current work focuses on data security when the noise level is linearly increased compared to the multiplicative depth of the estimated data. To solve this problem, a method called modulus switching was used. In order for c to be a valid encoding m under s in module q, and s is a small vector. Suppose it is also a simple scale c. that is, c'c mod 2 means that it is a valid encoding m under s module p with a normal decryption equation. With this method, the internal module can be changed in the decoding equation. Here is the decoding accuracy according to the same secret key. This method is called Module Switching Technology. The formal method can be defined as follows: for an integer in the vector x and integer's q> p> m, x 'is defined as x' ← Scale (x, q, pr, r) and x 'is the vector R, which is closer (p / q .x, corresponding to x '= x mod r [2]

3. PROPOSED ARCHITECTURE

Consider the system scenario of the client and the cloud service source, as given away in Figure 2, which shows the working mode with the HE client and the cloud packet.

1. The main response time in regular in service mode is strong-minded by TR = 2 * Ttr + Tpr

2. That the response time in operational mode with HE approval is determined by TRH = Ten + 2 * Ttr + Tpr + Tde

3. The broadcast time is the time elapse between the beginning and end of the transmission of the message. It can be calculated using the formula, transmission time = message size / data rate

In our work we have used the mixed homomorphic technique proposed by Zwick Brackersky, Craig Gentry and Vinod Vaikunthanathan [10], whose basic functions are presented below as the main work and our method builds

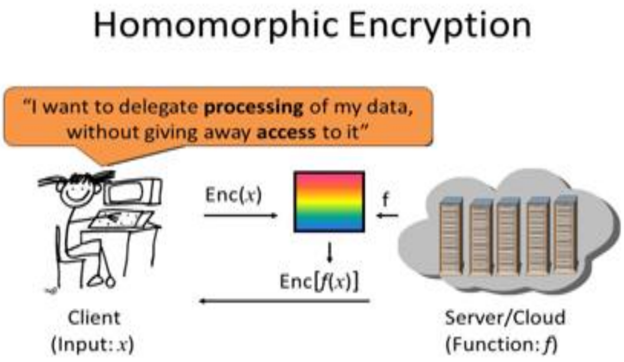

Figure 2.operative mode with HE adoption

Holomorphic encryption preserves at least one operation: addition, multiplication etc.. As our improved homomorphic scheme which consists of hybrid HE Scheme in which key switching matrices are generatedThe base idea is to use BGV scheme as a primary source and add byte level automorphism to the data. The procedure for generating key switching matrices also presented.

Encrypt (PT, PUpub):C_{ct}

Level shifting Operation

Rescale (C_{ct}*):*C_{ct}^{I}

Switch key (Augmented C_{ct}*):* C_{ct}^{I}

Holomorphic encryption

Add (C_{c1},C_{c2}*):*C_{csum}

Mul (C_{c1},C_{c2}*):*C_{cmul}

Procedure for Key switching

Despite the fact that the tensored cipher text for augmentation empowers us to accomplish the property of homomorphism duplication, there is an issue that the measurement of the cipher text increments from n+1 to (n+1)2 after a homomorphism increase: We utilize the key changing strategy to take care of this issue. Key exchanging comprises of two techniques, in particular Switch Key Gen (s1, s2 ,n1 , n2 , q) and Switch Key(τ , c1, n1 , n2 , q). The objective of Key changing is to change a cipher text c1 under a mystery key s1 to another cipher text c2 under a mystery key s2, in which c1 and c2 encode a similar message. On the off chance that the measurement of c2 and s2 is lower than the measurement of c1 and s1, the measurement of the key and cipher text vectors is lessened by key exchanging.

4. Experimental Results

We have selected three text files of different sizes which are given as input to the RSA and Our proposed scheme. The experimental analysis was performed on Intel(R) Core(TM) i5 machine with 8GB RAM with Java Implementation. The TABLE 1.below show the size of generated cipher text in bits for different plain texts and the graph depicting the same is as shown in Figure 4.
Table 1.size of generated cipher text in bits

1. Size of generated cipher text in bits

Size of Plain Text	**RSA**	**Proposed Scheme**
10	**28**	**20**
15	**26**	**21**
25	**30**	**25**

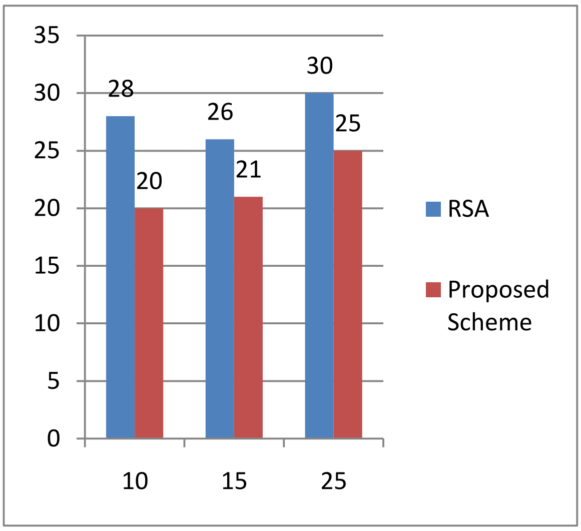

Figure 3. Size of Cipher Text

Table 2 presents the encryption time taken by the algorithms under study and the graph decpicting the same is as shown in Figure 5.

Table 2. Encryption time taken by the algorithms

Plain text in Bits	RSA	Proposed Scheme
10	3.5	1
15	9	4
25	12.9	4.6

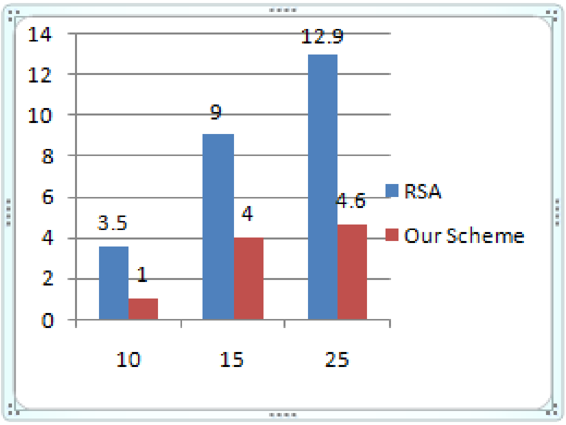

Figure 4. Encryption Time

Table 3. Decryption time:

Plain text in Bits	**RSA**	**Proposed Scheme**
10	**2.6**	**0.9**
15	**4.42**	**1.5**
25	**6**	**2.6**

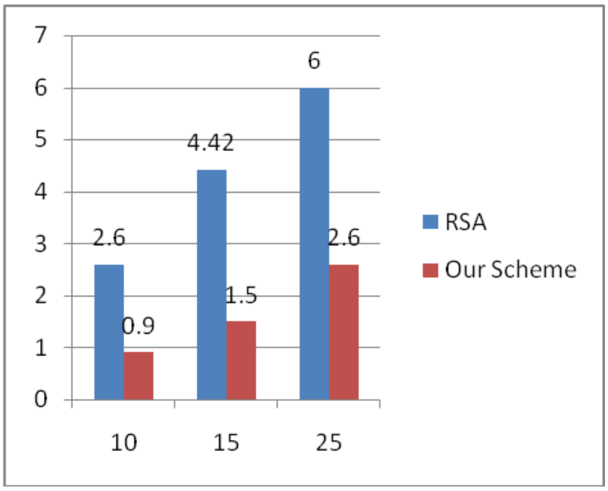

Figure 5: Decryption Time

The results show that the data will become larger, coding and decoding increases, that is, the transmission time of the process in Holomorphic encryption is much higher than the normal transmission time of Marcus TRH >> Although the reasons for running homomorphic encryption data storage data confidentiality and integrity of the transmission time delay important reason to consider a critical issue in front of his active life. In order to better system performance, you get a range of information we intend to introduce in an internal automorphism idea of work is still in its infancy and integrate our future.

5. Conclusion

Homomorphic encryption schemes are forced to cover that new data in the cloud, the cloud service providers allow customers to work with more information about the integrity of travel secret agents. Although a large proportion they exist, the noise of the thoughts of the increase is not a complete consequence of the FHE.

References

[1] P.Mell,T.Grance ,"The NIST Definition of Cloud Computing",National Institute of Standards and Technology,U.S.Department of Commerce,September 2011.

[2] R.Kanagavalli and Dr.Vagdevi S,"A Mixed Homomorphic Encryption Scheme for Secure Data Storage in Cloud", IEEE Intemational Advanced Computing Conference IACC2015,2015,D.O.I:10.1109/IADCC.2015.7154867.

[3] K.Lauter,M.Nachirg,V.Vaikuntanathan,"Can Homomorphic Encryption be Pratical?,"CCSW'11,October 21,2011,Chicago,Illinois,USA,pp.113-124.

[4] M.TEBAA and S.ELHAJII,"Secure cloud computing through Homomorphic Encryption ",International Journal of Advancments in Computing Technology, Vol.5,No.16, 2013,pp.29-38.

[5] Payal V.Parmar,et.al ,"Survey of Various Homomorphic Encryption algorithms and Schemes",Interational Journal of Computer Applications(0975-8887), Vol.91,No.8, April 2014,pp.26-32.

[6] M.Ogburn,C.Turner,P.Dahal,"Homomorphic Encryption In Complex Adaptive Systems",Publication 3, Baltimore,MD,Elsevier,2013,pp.502-509.

[7] R.Rivest,A.Shamir,and L.Adleman,"A method for obtaining digital signatures and public key cryptosystems",Communication of the ACM,21(2):120-26,1978.ComputerScience,Springer,1999,pp.223-238.

[8] T.ElGamal,"A Public Key Cryptosystem and a signature scheme based on discrete logarithms",IEEE Transactions on Information Theory,1985,pp.469-472

[9] Pascal Paillier,"Public-key cryptosystems based on composite degree residuosity classes",In 18th Annual Eurocrypt conference (EUROCRYPT99),Prague,Czech Republic,Vol.1592,1999.

[10] Boneh,E.Goh,K.Nissim,"Evalauting 2-DNF formulas on ciphertexts",In Theory of Cryptography Conference , TCC'05, Springer, 2005, pp.325-341.

About the Authors:

C.Veena is working as a Asst. Professor in CSE Dept. Holy mary Institute of Technology & Science. She has completed her MCA from S.V.University in 2002. She Completed M.Tech in CSE from JNTU Anantapur in 2013. She is having a total 08 years of teaching experience. She is pursuing her Ph.d (computer science,Reg no: PP.COMP.SCI.0612) in Rayalaseema University, Kurnool, Andhra Pradesh, under the guidance of Dr. M. Hanumanthappa, Professor & Chairman Dept of Computer Science& Applications, Bangalore University, Bangalore. Her research area of interest are Cloud Computing, Network security, Data Mining, Etc.

Dr. M. Hanumanthappa is working as a Professor & Chairman Dept of Computer Science& Applications, Bangalore University, Bangalore. He completed his MCA from Bangalore University in 1996. He received his M.Phil & Ph.d in Data Mining from Bangalore University in 2009. He is having total 18 years of teaching, Administration & Industry Experience. He adjudicated nearly 50 Ph.d, M.Phil (Computer science thesis of various Universities) and conducted 18 viva voce examinations for Ph.d, M.Phil candidates. He has total research publications:95, out of which international journals - 47, International conferences - 28, national conferences - 17, Monographs - 03. He is guiding 08 number of Ph.d students and Awarded 03 Ph.d. He received Dr.RadhaKrishna GIold Medal award by Global Economics progress and research association in 2012. His area of interest are Data Mining, Cloud computing, Network security