ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review of Security of Data Storage and Retrieval on Cloud using Homomorphic Encryption

Sudesh Sharma
M.TECH Student, Dept. of Computer Engg.
U.I.E.T, Kurukshetra University
Kurukshetra, India

Dr. Karambir
Assistant Professor: Dept. of Comp. Engg.
U.I.E.T, Kurukshetra University
Kurukshetra, India

Abstract: From the earlier few years and nowadays the cloud computing is an era of rapid progressive in terms of providing services and resources to the users. As with the increase in the industrial and business area the involvement of cloud computing also increased though it provides the services for data storage and avoid the cost expensive on software, but with the wide usage of cloud the security of data becomes an important issue for cloud adopters. The users store their data on cloud in encrypted form so that their data would be in safe hand, for this encryption/decryption techniques are in practice. In this survey we are reviewing homomorphic encryption (HE) which provides security in cloud and also ease the computation performed on encrypted data without decrypting it and also discuss some homomorphic schemes and algorithms mainly EcElgamel algorithm**.**

Keywords: cloud data security, homomorphic encryption, homomorphic algorithms, fully homomorphic encryption (FHE), partial HE, EcElgamel.

I. INTRODUCTION

Cloud computing can be defined as a form that enables on demand admittance to a shared collection of configurable computing resources. It is a growing technique which provides the services are known as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) in industries [1].

Some characteristics of cloud computing provided as [1]:

- On-demand self-service: A user can get resources, according to his/her necessity and without any other human interference.
- Broad network access: Computing and storage capabilities can be accessible from anywhere and by any way over the broad and easily accessible network.
- Resource pooling: A large amount of multitenant and location independent physical and virtual resources pooled which can be dynamically assigned [1]. Users don't have any control or knowledge about these resources (example: database, CPU, etc.).
- Rapid elasticity: The provisioning of the capabilities is so elastic and responsive that it provides a sense of infinite capacity. Scaling up and Scaling down of capabilities is very fast.
- Measured Service: though computing resources are lumped together and shared by several consumers the cloud frame is proficient to use proper mechanisms to assess the handling of these resources for each individual consumer by its metering capabilities.

A. Data Security on Cloud

To forbid the user's data from outside attackers is another major challenge faced by the users and to resolve this challenge Encryption is best way to make data storage on cloud secured, mainly encryption is of two types that is symmetric and asymmetric encryption. It is the technique for converting the plain text message or information in the coded form so that only legitimate user can access and read the plain message [3, 4].

- Symmetric encryption scheme: In this system encryption as well as decryption both can be performed with the single key (private key) [3, 4].
- Asymmetric encryption scheme: In relation with previous scheme, this scheme introduces a key pair one is to encrypt and another to decrypt. The encryption key is public, as the decryption key remains private [3, 4].

B. Homomorphic Encryption (HE)

It is method relied on asymmetric cryptography and is capable to perform operations on encrypted data without decrypting them, this functionality is major application of this method which makes it feasible to execute calculations on encoded confidential data by producing the exactly same result which when obtained by performing same operation on plain data . This method also helps to outsource the encrypted data on cloud [2, 3].

Different forms of homomorphic encryption

If from Enc (x) and Enc (y) it is possible to compute Enc (f (x, y)), where f can be: +, × and without using the private key then it is homomorphic encryption [5].

- Additive Homomorphic Encryption**:** it is additive, if Enc (x + y) = Enc (x) + Enc (y) where x and y are plaintext messages, + denotes the additive operation. This property is shown by Pailler[6] and Goldwasser-Micalli[7].
- Multiplicative Homomorphic Encryption: it is multiplicative, if Enc (x*y) = Enc (x) *Enc (y) where x and y are plaintext messages, *denotes the multiplicative operation. This property is shown by RSA [8] and ElGamel [9] cryptosystem.
- Fully Homomorphic Encryption (FHE): it is the encryption which satisfies both additive and multiplicative properties simultaneously and in this type of encryption more than once both operations can be performed on data [10].

- Somewhat Homomorphic Encryption (SHE): this method provides a limited operation on cipher texts with one operation at a time. In real world this type of encryption is used in many applications where it is known that how many times addition or multiplication is needed.

II. LITERATURE SURVEY

Craig Gentry [10] proposed the first FHE scheme, solving a central unfasten problem in cryptography. The construction of scheme was made the use of hard problems on ideal lattices and it was suggested that ideal lattices offer both additive and multiplicative homomorphism as considered necessary to estimate general circuits.

Craig Gentry [2] described a "fully homomorphic" encryption scheme that kept data private. According to this paper an arbitrator could perform complex processing of data without being capable to observe it, this helps to made cloud computing well-suited with privacy. This paper presented the above scheme [10] expensive. The scheme presented in this paper, while conceptually simpler, seems to be less efficient than the lattice-based scheme.

Zvika Brakerski and Vinod Vaikuntanathan [11] presented a FHE scheme which was based on the (standard) learning with errors (LWE) hypothesis. Applying identified results on LWE, the safety of the scheme was relied on the worst-case rigidity of "short vector problems" on random lattices. Presented construction was improved Firstly, by using re-linearization technique on partial HE based on LWE Secondly, by deviating from the "squashing paradigm" used during all earlier works, new dimension modulus reduction technique, which shortens the cipher texts and reduces the decryption complexity of the scheme, without introducing additional assumptions.

Deyan Chen and Hong Zhao [12] mainly focused on data safekeeping and confidentiality protection issues which was big problem faced in cloud computing at the enterprise level and across each phase of data life cycle. Future concerns was suggested, as movement of employees in organizations is high so to guarantee about no un-authorized access made to the organization's cloud resources by some employees who have resigned.

Maha Tebaa et al. [5] proposed that when operation required to be performed on distant server's data then it was necessary that the CSP had access to the original data and to obtain this data then it would decrypt them. To crack that trouble this paper employed a security method called HE, which perform the operations on encrypted data without decrypting that data hence, does not required for raw entries and thus increase confidentiality of data.

S.G sutar and G. A. Patil [4] proposed that Privacy management was a serious matter in cloud whenever the services accessed through un-trusted service provider or third party/inter-mediator. This paper presented a HE function on secret credentials secrecy of personal information sent by the cloud users to un-trusted service provider or arbitrator could be managed. Un-trusted service provider or arbitrator compared the personal information received from both, client and server in coded form. The Paillier cryptosystem [6] was used for privacy management.

Michael Brenner et al. [13] discussed an algebraically homomorphic scheme of limited multiplicative depth that could be used as an approach to build practical applications to facilitate operation on encrypted data. This paper discussed the properties of the SHE scheme and provided a proof of correctness and also gave a security investigation for different attack models and stated, in which conditions the scheme was secured.

Songzhu Mei et al. [14] projected Trust Enhanced Third Party Auditor (TETPA), a case for trusted and practical auditor, in Cloud environment. It used several methods, such as TPM (Traditional audit methods)-compatible and USB Key for Cloud users to enable remote attestation, so that cheating attacks could be avoided. With the TETPA, users could be protected from non-sense data losses.

Simon Fau et al. [15] proposed a first evaluation towards the practical use of (FHE) to perform true calculations, in terms of software engineering and performances. A model targeting any FHE scheme was presented also provided realization of Brakerski-Gentry-Vaikuntanathan (BGV) scheme which was one of the most promising FHE schemes with respect to practicality. It was tried to fill the bridging gap between various non-trivial algorithms and their practical, relatively seamless, execution on FHE schemes.

Bhabendu Kumar Mohanta and Debasis Gountia [16] analyzed the different security issues present and how to guarantee privacy while operation with the data encountered. To ensure privacy during computation some FHE was presented which allow the users to perform computation on encrypted data without using secret key of client. The main defect of this scheme was that after encryption the volume of the data became very large which would cause heavy burden for network and storage.

W. Wang et al. [17] overcome the performance bottleneck of the Gentry, Halevi FHE by introducing an array of algorithmic optimizations by presenting two optimizations: partial FFT where they speed up modular multiplications by introducing Strassen's FFT based multiplication algorithm and full FFT optimization where they gain additional speed by eliminating the greater part of FFT conversions via delayed modular reductions and by performing the bulk of the calculations directly in the FFT domain. But memory becomes bottleneck due to speed gain.

FENG Chao and XIN Yang [18] suggested some key issues of Gentry-style HE scheme regarding its original implementation and also called it as a slow key generation algorithm and proposed key generation algorithm by choosing eigen values of primary matrix that enables one to create a more practical partial HE Furthermore, security analysis of the approximate shortest vector problem (SVP) against lattice attacks was given.

G. jeeva Rathanam and M. R. sumalatha[19] designed a secured storage system in which data was stored on server by dynamic data operation with Partitioning Method and ensured better security and dynamic operation in the environment. To attain this approach Improved Adaptive Huffman Technique and Improved RSA Double Encryption Technique which enabled the data access in an efficient way were used. The system does a verification to avoid the loss of data and ensures security with storage integrity method. Professional distributed storage auditing mechanism was implemented to defeat the limitations in managing the data loss and provide security in service by enforcing error localization and easy detection of misbehaving server.

Darko Hrestak et al. [20] suggested several other FHE systems where each had its one advantages and drawbacks and also discussing the strengths and weaknesses of HE along with gave a brief description of several promising FHE systems. And in addition, gave a special consideration to the HE systems for cloud computing.

Kamal Kumar Chauhan et al. [21] concerned on many standard encryption method that were used to provide security to data in storage and transmission state, but in processing state when computing was done over data HE methods and their application in cloud to secure data would be used because it allows users to operate on encrypted data directly without decrypting it .In these methods, the problem faced was that the fully homomorphic and partial homomorphic methods were not feasible and not so easy to implement for cloud computing. Therefore the problem will lead to design efficient and feasible HE algorithms.

Ali Azougaghe et al. [22] mainly focused on some threats in cloud and presented a simple more generalized security holding architecture for inter-cloud data sharing. The security to data was provided by using algorithms (AES) Advanced Encryption Scheme [31] and Elgamel [9], these were used to provide double security to data so that only intended user could access their data. This paper also offered some solutions for protecting against DDOS attacks in cloud computing.

Ayantika Chatterjee and Indranil Sengupta [23] presented that there was extra overhead for processing of encrypted data due to repeated encryption-decryption therefore HE schemes were beneficial as they provided direct proscessing on encrypted cloud data. FHE provides a method of performing arbitrary operations directly [10]. Termination was a concerned issue while handling encrypted data so authors presented a method of handling execution by communication between server and client and discussed issues for translating variable definitions, instruction executions, handling of loops and terminating conditions when the algorithms hold encrypted data.

Ryan Hayward and chia- chu chiang [3] discussed about reduced adoption of cloud because of security of data and presented a realization of a processing dispatcher which took an iterative set of operations on FHE encrypted data and splits them among a numbers of processing engines. A private cloud was build to hold concurrent processing of HE in the cloud. A client-server model was created to estimate cloud computing of the Gentry's encryption algorithm along with developing a distributed algorithm to sustain analogous processing of the Gentry's algorithm for estimation on the cloud.

Yasmina Bensitel and Rahal Romadi [24] focused on cloud computing and its adoption in different domain, and described the role of HE technique for privacy preserving data sharing in the cloud. It might be either additive or multiplicative homomorphic Therefore, proposed a system that ensures secrecy of data by using partial HE algorithms (RSA [8] and Paillier [6]. Also gave some examples of some statistical functions used in real life for a medical domain, and which could be used over encrypted data and also gave details of their implementation (hybrid solution).

Gnanaprakasam T and Rajivkannan A [25] projected a new method i.e. dual encryption for data security in cloud. The privilege of the method was that the other external attackers cannot generate a valid signature or valid message authentication. Furthermore, the cloud server was not aware about the secret data of the corresponding owner and performance was evaluated using the encryption and decryption time. Authors proposed secure data in cloud system using RSA [8] and OECC (optimal elliptic curve cryptography) algorithm for encryption, and suggested that these algorithms would gave a good result when these compared to an existing encryption method using AES [31].

Prof. S.V.Phulari et al. [26] proposed an efficient data storage security using File Partitioning Technique in which files partitioned into number of partitions and these partitions either depends on file size or also on number of server of respective file. Files could be easily partitioned. Data could be stored in secure manner by using partitioning technique. Data stored in cloud computing was secured by using AES algorithm [31]. By using this users could be access stored data in flexible way and data would be stored in less cost. So that it also decrease space and time at the time of data storage.

Ms. Nikita N Chintawar et al. [27] suggested data security on cloud by creating digital signature and encryption with ECC (Elliptic Curve Cryptography) because it offered enhanced security and more efficient performance than the other public key cryptography techniques like RSA [8] which was in use. After comparing the RSA and ECC ciphers, the ECC had manifest to complex much less overheads compared to RSA. The ECC had numerous benefits because of its capacity to supply the same level of security using less key size. Overall, it was suggested ECC the better algorithm than others because in small processing devices ECC could be applied for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to other algorithms.

Manish M. Potey et al. [28] proposed storage proficient HE scheme using Elliptic Curve. This scheme was creates a cipher text 50-60 % smaller in size as compared to other HE schemes. Due to this data processing efficiency was improved as it provides the data security with the smaller key size with offering same security like RSA. The security of ECC ElGamal depends on the complexity of evaluating the elliptic curve logarithm problem.

Kamal Benzekki et al. [29] proposed a architecture of multiple distributed servers and multiple clouds to partition the data and to almost permit achieving FHE. The distributed architecture was presented for enabling the valuation of any function and processing encrypted data. It could bring lots of benefits to the HE application and making it more practical in the case of the security of data and applications.

Babitha.M.P and K.R Remesh Babu [30] presented a simple secure system for storage of data on cloud using 128 bit AES [31] algorithm and for authentication an SMS alert method was used which provide an alert SMS to the registered user's number if any other person tried to fetch his/her data file. A model was proposed in which data splitting is done on different server and then encrypt it individually by AES. This paper also compared AES, DES and RSA for execution time of data or to observe the increase in delay by increasing the file size.

III. CONCLUSIONS

In this survey, various security methods for cloud data storage are discussed with their drawbacks and advantages as cloud data security is a great task for cloud providers so different approaches shown are not sufficient today due to increase in the number of business as well as institutions. cloud data security provided using partial homomorphic method is best technique as it resolved so many problems of cloud provider and users regarding the safety of their data because this method provide computation over stored encrypted data on cloud. Homomorphic encryption algorithms used for data security are RSA, Pallier, Elgamel etc. which are not so much advantageous due to their larger key size and execution time. AES [30] is used widely for encryption but it has limitation that it is not homomorphic algorithm so another algorithm for better results and reduced computation time is EcElgamel because it uses elliptic curve which reduces the key size to a greater extent by providing same security. Data partition can be used among distributed servers to effectively encrypt the data without any greater load on a single server.

IV. REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing - v15," 21. Aug 2009.

[2] Craig Gentry, "Computing Arbitrary Functions of Encrypted Data", Communications of the ACM, VOL. 53, No. 3, pp.97-105, march 2010.

[3] Ryan Hayward and Chia-Chu Chiang, "Parallelizing fully homomorphic encryption for a cloud environment", Journal of Applied Research and Technology (available online at science direct), Vol. 13, pp. 245-252, August 2015.

[4] S.G Sutar and G. A. Patil, " Privacy Management in Cloud by making use of Homomorphic Functions", International Journal of Computer Applications, Vol. 37, No.2, pp.0975-8887, January 2012.

[5] Maha Tebaa, Saïd El Hajji, Abdellatif El Ghazi "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering, Vol.1, WCE 2012, July 4 - 6, 2012.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT, Vol. 1592, pp. 223–238, 1999.

[7] Julien Bringe and al. "An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication", Springer-Verlag, 2007.

[8]R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, 21(2):120-126, 1978. Computer Science, pp. 223-238, Springer, 1999.

[9] Taher ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, pp. 469-472, 1985.

[10] Craig Gentry, "Fully homomorphic encryption using ideal lattices", in Proceedings of the 41 Annual ACM Symposium on Theory of Computing, pp. 169–178, 2009.

[11] Zvika Brakerski and Vinod Vaikuntanathan, "Effcient Fully Homomorphic Encryption from (Standard) LWE", 52 Annual IEEE Symposium on Foundations of Computer Science from IEEE Computer Society, pp.97-106, 2011.

[12] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering From IEEE Computer Society, pp.647-651, 2012.

[13] M. Brenner, H. Perl, and M. Smith, "Practical applications of homomorphic encryption" ,in SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography, Rome, Italy, SECRYPT is part of ICETE - The International Joint Conference on e Business and Telecommunications, pp. 5–14, july 2012.

[14] S. Mei, C. Liu, C. Yong, W. Jiangjiang and W. Zhiying, "TETPA: A case for trusted third party auditor in Cloud environment", IEEE Conference Anthology, pp-1 – 4, 1-8 Jan. 2013.

[15]Simon Fau,Renaud Sirdey, Caroline Fontaine, Carlos Aguilar-Melchor and Guy Gogniat, "Towards practical program execution over fully homomorphic encryption schemes", IEEE Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp.284-290, 2013.

[16] Bhabendu Kumar Mohanta and Debasis Gountia, "Fully homomorphic encryption equating to cloud security: An approach" IOSR Journal of Computer Engineering (IOSRJCE), e-ISSN. (2278-0661), p- ISSN.(2278-8727), Vol. 9, No. 2, PP. 46-50, jan-feb 2013.

[17] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, "Exploring the feasibility of fully homomorphic encryption" , IEEE Transactions on Computers, vol. 99, pp. 1, 2013.

[18] FENG Chao and XIN Yang, "Fast key generation for Gentry-style homomorphic encryption", The Journal of China Universities of Posts and Telecommunications, Vol. 21, No. 6, pp. 37-44, December 2014.

[19] G.jeeva Rathanam and M.R. Sumalatha, "Dynamic Secure Storage System in Cloud Services", IEEE International Conference on Recent Trends in Information Technology.

[20] Darko Hrestak and Stjepan Picek, "Homomorphic Encryption in the Cloud", MIPRO, may 2014.

[21] Kamal Kumar Chauhan, Amit K.S Sanger, Ajai Verma, "Homomorphic Encryption for Data Security in Cloud Computing", IEEE International Conference on Information Technology, pp.206-209, 2015.

[22] Ali Azougaghe, Zaid Kartit, Mustapha Hedaboui, Mostafa Belkasmi, Mohamed El marraki, "An Efficient Algorithm for Data Security in Cloud Storage ", 15th International Conference on Intelligent Systems Design and Applications (ISDA), pp.421-427, 2015.

[23] Ayantika Chatterjee and Indranil Sengupta, "Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud", IEEE Transactions on Cloud Computing, pp. 1-14, September 2015.

[24] Yasmina Bensitel and Rahal Romadi, "Secure data storage in the cloud with homomorphic encryption ", 2nd International Conference on Cloud Computing and Applications, 24-26 may 2016.

[25] Gnanaprakasam T and Dr. Rajivkannan A, "Optimal ecc based dual encryption technique for data security in cloud", International Journal of Advanced Engineering Technology, e-ISSN(0976-3945), Vol.7,no.2,pp.1049-1055, April-June 2016.

[26] Prof. S.V.Phulari, Sneha Jamadade, Swati Mhetre, Pramila Gonde and Jyoti Birajdar, "Cloud Computing Security using Data Partitioning Technique", International Journal of Engineering Science andComputing(IJESC),ISSN(2321-3361),Vol.6,No.4,pp.4595-4597,April 2016.

[27] Ms. Nikita N Chintawar, Ms. Sonali J Gajare, Ms. Shruti V Fatak, Ms. Sayali S Shinde and Prof. Gauri Virkar, "Enhancing Cloud Data Security Using Elliptical Curve Cryptography", International Journal of Advanced Research in Computer and Communication Engineering(IJARCE), ISSN (Online) (2278-1021) ISSN(Print)(2319-5940), Vol.5, No.3, pp.94-97,march 2016.

[28] Manish M. Potey, Dr. C. A. Dhote and Deepak H.Sharma, "Efficient Homomorphic Encryption using ECC-ElGamal Scheme for Cloud Data", 3rd International Conference on Electrical, Electronics, Engineering Trends, Communication, Optimization and Sciences (EEECOS),pp.39-43,2016.

[29] Kamal Benzekki, Abdeslam El Fergougui, Abdelbaki El Belrhiti El Alaoui, "A Secure Cloud Computing Architecture

Using Homomorphic Encryption", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7, No. 2, pp.293-298, 2016.

[30] Babitha.M.P and K.R Remesh Babu, "Secure Cloud Storage Using AES Encryption", IEEE International Conference on Automatic Control and Dynamic Optimization Techniques, pp.859-864, 2016.

[31] J. Daemen & V. Rijmen, " The design of Rijndael: AES-the advanced encryption standard", Springer Science & Business Media, 2013.