COMPARATIVE ANALYSIS OF HOMOMORPHIC ENCRYPTION IN CLOUD COMPUTING

Sumitha.J,

M.Phil. Research Scholar,Department of Computer Science,Karpagam Academy of Higher Education,

Dr. S.Manju Priya,

Associate Professor,Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore

ABSTRACT

Cloud computing is known as developing technology called as "computing". It offers the resources through the platform and infrastructure. The cloud computing offers their main resources through the service of internet. Cloud applications use giant knowledge center and effective servers that host internet applications and services. The service areas are said to be unit delivered which are associate to be used over the net and the unit is obtained by the cloud client on an as-needed or pay-per-use business model.

KEYWORDS: Cloud Computing, Homomorphic Encryption, RSA, Elgamal, Paillier.

1. INTRODCUTION

In today's world scenario the use of web and new technologies for business and users are already a part of a standard of living. Any data is offered any place in the world at any time. But that wasn't doable few years past. Today it has arisen plenty of prospects of access to public and personal data like web speed access or the preparation of positive that permit the affiliation to the Internet from virtually every place. There are different variety of virtualization in cloud computing [6].The NIST has four cloud models [9]. In such way, Cloud Computing has many simulations tools (E.g.: CloudSim, etc..,) are readily available to do the experiments and to test the system quality [11]. The speedy development of the web and therefore the emergence of cloud computing have enabled a unique trend of buying and intense Information Technology (IT) services [5].

1.1 SECURITY IN CLOUD COMPUTING ENVIRONMENT

Security in cloud computing is called as major concern. Knowledge in cloud ought to be held in encrypted method. To limit shopper from accessing the shared knowledge directly, proxy and brokerage services can be used. Security is the combination of confidentiality, the interference of the unauthorized method of revealing the knowledge, integrity, unauthorized modification, deletion of knowledge, and unauthorized withholding of knowledge. The provider of cloud should make the user aware about all issues [3].The organization of the cloud computing with respect to the aspects of data security are: integrity, Confidentiality, availability, Privacy are shown in the fig 1.1.

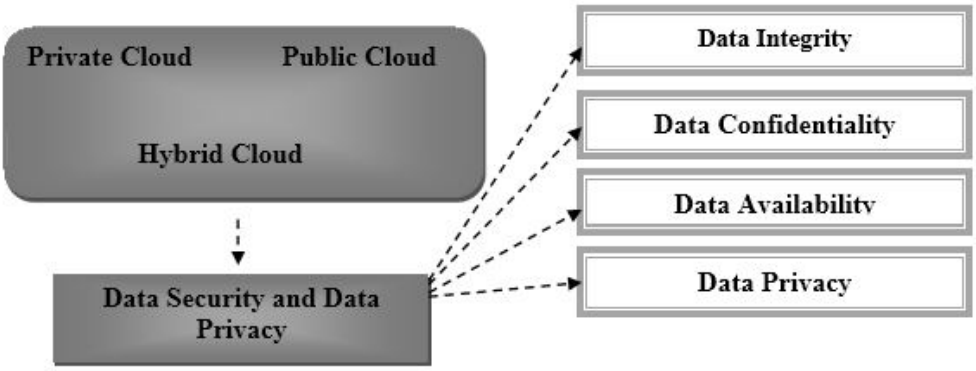

Fig 1.1. Organization of Cloud Security and Privacy

1.2 DATA SECURITY IN CLOUD COMPUTING

Mostly, the safety problems or the issues that arises in Cloud Computing are the outcome of users/enterprises with lack of management on the physical infrastructure. The Security Issues in cloud computing are illustrated in the fig 1.2.

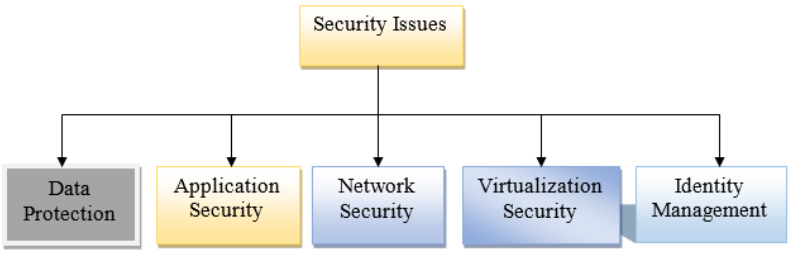

Fig 1.2. Security Threats in Cloud Computing

2. LITERATURE SURVEY

D.Chandravathi and Dr.P.V.Lakshmi [2] guarantees the security of the proposed system and provides the security to the data with the technique of using the Hill Cipher cryptography in Homomorphic Encryption of Additive property. Further, it can be improved by the existing using some of the parameters.

Ruchita Patel, Veena Kulkarni [8] by using the K-means of a method the user data is splitted with two kinds of host and keys are sent over the cloud to perform the Paillier Homomorphic Encryption to prevent from the attacker. This provides scope for the key to avoid the intermediate of an intruder to the user data which is been distributed.

Yasmina BENISTEL and Rahal ROMADI et. al., [10] in their paper, discussion of Homomorphic Encryption (HE) is made and analysed the confidentiality of the data in the cloud by using Partial Homomorphic Encryption (PHE) Algorithms. They have shown that the Fully Homomorphic Encryption (FHE) will not provide a better solution. Instead, the Somewhat Homomorphic Encryption (SHE) or a Partial Homomorphic Encryption (PHE) gives better result in a medical domain using the Homomorphic Encryption (PHE).

Chandhiny G, Dr. Vairamuthu S [1] in their paper, they have proposed Paillier method for providing the privacy of preserving the financial data by using the partial homomorphic encryption properties among their cloud data, which is been used to avoid the higher amount of computational complexity in fully homomorphic encryption (FHE).

3. HOMOMORPHIC ENCRYPTION

Homomorphic encoding could perform operations on encrypted information while not knowing the private key, through computations to be meted out on cipher-text and procure the encrypted result which is been decrypted provides the results of operations performed on the plaintext of Homomorphic encryption.

4. TYPES OF HOMOMORPHIC ENCRYPTION

There are two types of homomorphic Encryption they are namely: Partial Homomorphic Encryption (PHE) and Fully Homomorphic Encryption (FHE) and Somewhat Homomorphic Encryption (SHE) [7].

4.1 Somewhat Homomorphic Encryption

FHE (Fully Homomorphic Encryption) schemes while not "refreshing" the noise also can use as partial HE schemes. These schemes sometimes support an outsized variety of additives and restricted levels of multiplications. HE (Homomorphic Encryption) schemes with this property are typically mentioned as Somewhat Homomorphic encoding Schemes (SWHE).

4.2 Fully Homomorphic Encryption

The Fully Homomorphic Encryption allows multiple types of operations to perform on the encrypted data. It performs Addition and Multiplicative property [4].

4.3 Partial Homomorphic Encryption

Partial homomorphic cryptography is the most significant form of homomorphic technique, it performs the computation on a number of mathematical operations and has high potency for sensible applications like the Paillier which will perform evaluations in milliseconds level. It permits only one operation to perform on the data.

5. COMPARISON OF PERFORMANCE ANALYSIS

The Table 5.1 represents the four different sizes of key and the corresponding Encryption time taken by RSA, Elgamal and Paillier Algorithm by using their respective Homomorphic encryption property operations.

Table 5.1 Encryption time and Decryption Time process (ms)

Type of Scheme / Key Size (Bit)	Encryption Process				Decryption Process			
	256	512	1024	2048	256	512	1024	2048
RSA Algorithm	4	5	43	67	20	22	95	567
Elgamal Algorithm	18	40	156	1213	30	70	309	786
Paillier Algorithm	32	74	391	2520	39	90	589	4381

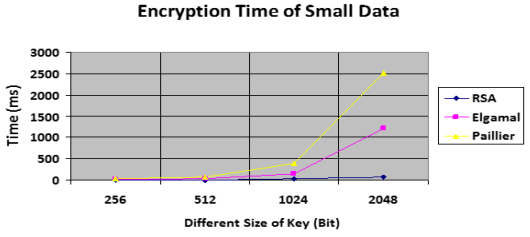

Fig 5.1 Encryption Time Representation

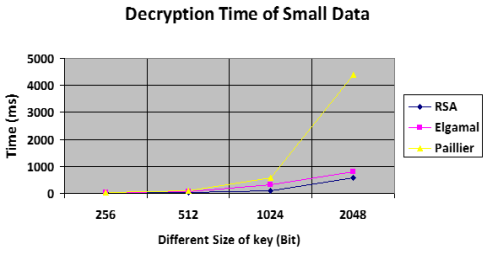

Fig 5.2 Decryption Time Representation

After the successful Execution of the encryption and decryption process in cloud, the comparison is made between the original data and the decrypted data with various key sizes. As a comparative and analytical study of the above given results, RSA is faster than Elgamal and Paillier algorithms, but its security is lower than the other cryptosystem's. In RSA we get the same cipher when we execute the same plaintext for many times.

Table 5.2 Encryption time (ms) of Different Data Size

Type of Algorithm & Scheme / Key Size (Bit)	Encryption Process			
	32B	1KB	10KB	100KB
RSA Algorithm	1	9	67	558
Elgamal Algorithm	43	1213	11847	109040
Paillier Algorithm	79	2520	22131	243235

Table 5.3 Decryption time (ms) of Different Data Size

Type of Algorithm / Data Size used (Bit)	Decryption Process			
	32B	1KB	10KB	100KB
RSA Algorithm	25	567	5598	56912
Elgamal Algorithm	19	786	6423	67532
Paillier Algorithm	12	4381	42129	416205

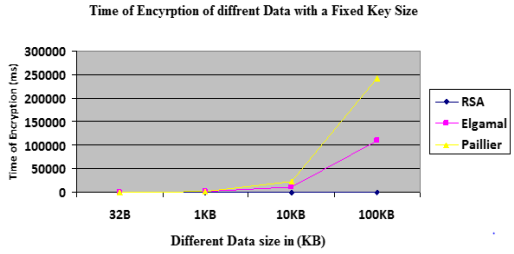

Fig 5.3 Encryption Time Representation

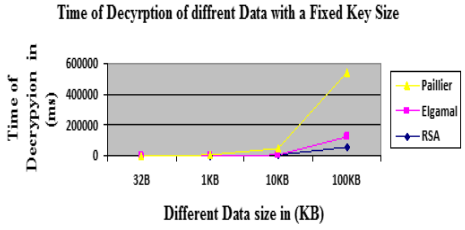

Fig 5.4 Decryption Time Representation

But, when in terms of contrary it means that the cryptosystem of algorithms such as Elgamal and Paillier use random or different cipher text for the given Plain text. RSA algorithm is faster but the other algorithms like Elgamal and Paillier are the most efficient to use for the security purpose of data in the cloud environment.

CONCLUSION:

In this paper, the comparison of homomorphic encryption has been done. From the above results, RSA is said to be faster when the Paillier and Elgamal algorithms are considered to be the most efficient when it comes in terms of security. Encryption plays very important role when it comes in terms of security. From the simulation result, we evaluated that RSA algorithm is much better than Paillier and Elgamal algorithm. The Elgamal and Paillier are called as probalistic algorithm but, it is less secure than the previous cryptography systems. In future, the research can be concentrated on optimizing or concerning, the tests of homomorphic encryption algorithms by storing their encrypted data and can be able to perform both the operations such as addition and multiplication of data in cloud.

References:

1) Chandhiny G, Dr. Vairamuthu S," ***Securing Financial Database Using Partial Homomorphic Encryption",*** International Journal of Pure and Applied Mathematics, Volume 119, Issue No. 7, 2018.
2) D.Chandravathi, Dr.P.V.Lakshmi," ***Homomorphic Encryption Scheme Using Hill Cipher For Cloud Data Security",*** International Journal of Advanced Information Science and Technology, Vol.5, No.9, September 2016.
3) Daniya Rao , Deepak Painuli, et,al.," ***Homomorphic Hybrid Encryption for Cloud Computing",*** International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 5, May 2016.
4) Dr.A.Padmapriya, P.Subhasri ***"Cloud Computing: Security Challenges & Encryption Practices",*** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.

5) K.Govinda, V.Gurunathaprasad, H.SathishKumar,***"Third Party Auditing For Secure Data Storage In Cloud Computing Through Digital Signature Using RSA",*** International Journal of Advanced Scientific and Technical Research, volume 4,Issue 2,August 2012.

6) Maha Tebaa,Said EL HAJII,***"secure cloud computing through Homomorphic encryption",*** International Journal Of Advancements in Computing technology, Volume-5, Issue-16, Dec.-2013.

7) N. Vamshinath, K. Ruth Ramya, Sai Krishna et, al., "***Homomorphic Encryption for Cluster in Cloud",*** International Journal of Security and Its Applications Vol. 9, No. 5 (2015).

8) Ruchita Patil,Veena Kulkarni,***"Hybrid Cryptosystem Approach For Secure Communication",*** International Journal Of Computer Science and Engineering,pp21-24.

9) Vineet Kumar Singh,Maitreyee Dutta, ***"Secure Cloud Network Using Partial Homomorphic Encryption",*** International Journal of Advanced Research in Computer Science ,volume 5,No 4,May-June 2014.

10) Yasmina BENSITEL, Rahal ROMADI,***"Secure Data Storage In The Cloud With Homomorphic Encryption",*** Journal of Theoretical and Applied Information Technology, Vol.82, No.2, December 2015.

11) Sumitha.J, Dr. S.Manju Priya, "***International Journal of Computer & Mathematical Sciences",*** International Journal of Computer & Mathematical Sciences, Volume 7, Issue 3**,** March 2018.