ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

A Review on Partially Homomorphic Encryption Scheme used in Cloud Computing

Nivedita W. Wasankar[1], A.V. Deorankar[2]

M. Tech. Scholar, Department of Computer Science and Engineering, Government College of Engineering, Amravati, MH, India[1]

Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering, Amravati, MH, India[2]

ABSTRACT: Homomorphic encryption is the encryption scheme which means the operations on the encrypted data. Homomorphic encryption is useful that allows the operations on the cipher text, which can provide the same results after calculations as the working directly on the raw data. As cloud computing provides different services,homomorphic encryption techniques can be used to achieve security. In this paper, We presented the partially homomorphic encryption techniques.

KEYWORDS: :Cloud Computing, Homomorphic encryption, cipher text, partially homomorphic encryption.

I. INTRODUCTION

Homomorphic encryption is a form of encryption that allows for some computations to be performed on the ciphertext without decrypting the ciphertext. The result of the operations is returned as an encrypted result, which when decrypted is the same as if some operation was performed on the plaintext. There are many form of partially homomorphic cryptosystems that allow for some specific operations to be performed (namely addition and multiplication). PHE allows only one type of operation with an unlimited number of times (i.e.,no bound on the number of usages). In other words, PHE schemes can only be used for particular applications, whose algorithms include only addition or multiplication operation. PHE schemes are deployed in some applications like e-voting or Private Information Retrieval (PIR). In the section II, various partially homomorphic encryption schemes are described. for example, RSA, Paillier, and ElGamal. The additive and multiplicative properties of the homomorphic encryption are described.

II. LITERATURE SERVEY

There are several useful PHE examples in the literature. Each has improved the PHE in some way. However, in this section, we primarily focus on major PHE schemes that are the basis for many other PHE schemes.

1. RSA: In 1978 Ronald Rivest, Leonard Adleman and Michael Dertouzos [1] suggested for the first time the concept of homomorphic encryption. RSA is an early example of PHE and introduced by Rivest, Shamir, and Adleman [Rivestetal.1978b] shortly after the invention of public key cryptography by DiffieHelman [Diffie and Hellman 1976]. RSA is the first feasible achievement of the public key cryptosystem. Moreover, the homomorphic property of RSA was shown by Rivest, Adleman, and Dertouzous [Rivest et al. 1978a] [6] just after the seminal work of RSA. Indeed, the first attested use of the term "privacy homomorphism" is introduced in [Rivestetal.1978a]. The security of the RSA cryptosystem is based on the hardness of factoring problem of the product of two large prime numbers [Montgomery 1994].RSA is only homomorphic over multiplication. Hence, it does not allow the homomorphic addition of ciphertexts.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

2. Goldwasser–Micali: The Goldwasser–Micali (GM) cryptosystem [2] is an asymmetric key encryption algorithm developed by ShaffGoldwasser and Silvio Micali in 1982. GM proposed the first probabilistic public key encryption scheme which is additive Homomorphic encryption, but it can encrypt only a single bit. GM is provably secure under standard cryptographic assumptions. Encryption is performed using a probabilistic algorithm, a given plaintext may produce very different cipher texts each time it is encrypted. This has significant advantages, as it prevents an adversary from recognizing intercepted messages by comparing them to a dictionary of known cipher texts. The GM cryptosystem is based on the hardness of quadratic residuosity problem [Kaliski 2005]. GM is homomorphic over only addition for binary numbers.

3. El-Gamal: It was described by TaherElGamal in 1984[3]. In cryptography, the ElGamal encryption System is an asymmetric encryption algorithm for public key cryptography which is based on the DiffieHelman exchange. ElGamal encryption can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem in group related to computing discrete logarithms. It is mostly used in hybrid encryption systems to encrypt the secret key of a symmetric encryption system. ElGamal encryption is used in the free GNU privacy Guard software, recent versions of PGP, and other cryptosystems. It allows the homomorphic multiplication of ciphertexts.

4. Benaloh: The Benaloh Cryptosystem [4]is an extension of the Goldwassermicali cryptosystem(GM) created in 1994 by Josh (Cohen) Benaloh. The main improvement of the Benaloh Cryptosystem over GM is that longer blocks of data can be encrypted at once, whereas in GM each bit is encrypted individually. Benaloh's proposal was based on the higher residuosity problem. Higher residuosity problem (x^n) [Zheng et al.] is the generalization of quadratic residuosity problems (x^2) that is used for the GM cryptosystem. Homomorphic property of Benaloh shows that any multiplication operation on encrypted data corresponds to the addition on plaintext. As the encryption of the addition of the messages can directly be calculated from encrypted messages E(m1) and E(m2), the Benaloh cryptosystem is additively homomorphic.It performs unlimited number of additions but only one multiplication.

5. Paillier: The Paillier cryptosystem, named after and invented by pascalpaillier in 1999[5], is a probabilistic asymmetric algorithm for public key cryptography. The paillier is based on composite residuosity problem [Jager 2012]. Composite residuosity problem is very similar to quadratic and higher residuosity problems that are used in GM and Benaloh cryptosystems. The scheme is an additive homomorphic cryptosystem.

6. **Naccache-Stern scheme:** The Naccache–Stern cryptosystem [8,9,13]is a homomorphic public key encryption whose security rests on the higher residuosity problem. The Naccache–Stern cryptosystem was discovered by David Naccache and Jacques Stern in 1998. Naccache-Stern scheme is a generalization of Benaloh cryptosystem to increase its computational efficiency. The encryption step is precisely the same as in Benaloh's scheme. However, decryption is different. Similar to the Benaloh's cryptosystem, this scheme is also an additive homomorphic cryptosystem

7. **Okamoto-Uchiyama scheme:** Okamoto-Uchiyama (OU) [Okamoto and Uchiyama 1998] proposed a new PHE scheme to improve the computational performance by changing the set, where the encryptions of previous HE schemes work[8,9,13]. The domain of the scheme is the same as the previous public key encryption schemes, Z^*_n, however, Okamoto-Uchiyama sets $n = p^2q$. To improve the performance of the earlier schemes on homomorphic encryption, Okamoto and Uchiyama changed the base group G, p and q being two large prime numbers as usual. One of the biggest advantages of this scheme is that its security is equivalent to the factorization of n. However, a chosen-ciphertext attack has been proposed on this scheme that can break the factorization problem. This scheme is an additive homomorphic cryptosystem. This has somewhat limited is applicability.

8. **Damgard-Jurik scheme:** Damgard-Jurik (DJ)[DamgårdandJurik2001] introduced another PHE scheme as a generalization of Paillier[8,9,13]. These three cryptosystems preserve the homomorphic property while improving the original homomorphic schemes. Damgard and Jurik propose a generalization of Paillier's scheme. Scheme can be used

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

in a number of applications. They also show that the semantic security of this scheme is equivalent to that of Paillier's scheme. This scheme is an additive homomorphic cryptosystem just like paillier's scheme.

9. **Galbraith scheme:** Galbraith [Galbraith2002] introduced a more natural generalization of Paillier's cryptosystem [8,13]. This is an adaptation of the existing homomorphic encryption schemes in the context of elliptic curves. Most important advantage of this scheme is that the cost of encryption and decryption can be decreased. Similar to the paillier's, this scheme is also an additive homomorphic cryptosystem

10. **Kawachi scheme:**Kawachi [Kawachi et al. 2007] suggested an additively homomorphic encryption scheme over a large cyclic group, which is based on the hardness of underlying lattice problems [8,13]. They named the homomorphic property of their proposed scheme as pseudo homomorphic. Pseudo homomorphism is an algebraic property and still allows homomorphic operations on ciphertext, however, the decryption of the homomorphically operated ciphertext works with a small decryption error. This scheme is an additive homomorphic cryptosystem.

III. CONCLUSION

This paper presents the basic concept of the homomorphic encryption and the presents partiallyhomomorphic encryption techniques as per the properties of the homomorphic encryption; Paillier can be used for preserving the additive property of homomorphic encryption while ElGamal and RSA can be used for multiplicative property. This paper can be useful for those who are wishing to carry out research in the direction of the homomorphic encryption. This survey can be helpful to know which and how various schemes are being used for applying homomorphic encryption for privacy preservation.

REFERENCES

1. Rivest, R., Shamir, A. and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21, 2 (1978), 120-126.
2. Goldwasser, S. and Micali, S. Probabilistic encryption. Journal of Computer and System Sciences 28, 2 (1984), 270-299.
3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology, Proceedings of CRYPTO '84. G. Blakley and D. Chaum (Eds.). Springer, Berlin Heidelberg, 1985, 1018.
4. Boneh, D. The decision Diffie-Hellman problem. In Algorithmic Number Theory, Proceedings of the Third International Symposium (ANTS-III) (Portland, June 21-25). J.Buhler (Ed.). Springer, Berlin Heidelberg, 1998, 4863.
5. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Eurocrypt, 1999.
6. Rivest, R., Adleman, L. and Dertouzos, M. On data banks and privacy homomorphisms. In Foundations of Secure Computation 4, 11 (1978), 169-180.
7. Boneh, D., Goh, E.-J. and Nissim, K. Evaluating 2-DNF formulas on ciphertexts. In Theory of Cryptography, Proceedings of the Second Theory of Cryptography Conference (TCC) (Cambridge, February 10-12). J. Kilian (Ed.). Springer, Berlin Heidelberg, 2005, 325-341.
8. Abbas Acar, HidayetAksu, A. SelcukUluagac, and Mauro Conti, 2016. A survey on homomorphic encryption schemes: theory and implementation. ACM Comput. Surv. V, N, Article A (January 2017), 35 pages.
9. S. Ramachandram, R.Sridevi, P. Srivani "A Survey Report On Partially Homomorphic Encryption Techniques In Cloud Computing" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 12, December – 2013.
10. Gentry, C. A fully homomorphic encryption scheme. Doctoral Dissertation, Stanford University, 2009.
11. Gentry, C., Sahai, A. and Waters, B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In Advances in Cryptology, Proceedings of CRYPTO '13. R. Canetti and J. Garay (Eds.). Springer, Berlin Heidelberg, 2013, 75-92.
12. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. In Proceedings of the thirty seventh annual ACM symposium on Theory of computing (STOC '05). ACM, New York, NY, USA, 2005, 84-93.
13. http://en.wikipedia.org