Achieving Fully Homomorphic Encryption in Security -A Survey

Aditi Soral

M. Tech Scholar, Department of Computer Science and Engineering,
Gurukul Institute of Technology, Kota, Rajasthan, India

Abstract— Many conventional cryptographic systems have homomorphic properties, yet there was no need of homomorphisms and little attention was paid to it. The ability to process encrypted data led to a renewed interest in Homomorphisms and a new cryptographic primitive, Fully Homomorphic Encryption (FHE) emerged. With time, question arose as to whether FHE is possible or not which has now modified as whether FHE is applicable or not. This paper provides a brief survey focusing on the development of HE to FHE and discussing all relevant research works in this direction in one section. The second section discusses the applications of FHE. The last section describes briefly some of the research works aiming at Searching/Sorting through FHE.

Keywords—*Information Security, Homomorphic Encryption, Fully Homomorphic Encryption, Sorting, Searching.*

I. INTRODUCTION

In recent years, Cloud Computing has emerged as an efficient service based shared platform where information is shared to and fro the Cloud Service Provider (CSP) and the Client very frequently. Due to the Cloud being public to all users and the plenty of information, also referred to as Big Data, being kept on a shared platform, security of the information is at risk. The need for security in Cloud Computing environment and Big Data residing in it has been emphasized by [1,2]. Plentiful security schemes have been proposed till date and one of the most frequently used schemes among them is Cryptography. Cryptography aims at encrypting the data and decrypting it back when needed. The encrypted test cannot be understood by the other users except the authorized ones. The only problem was the inability to process the encrypted text thereby maintaining confidentiality with usability. This led to the emergence of a whole new cryptographic primitive, Homomorphic Encryption (HE). The need for HE arose only recently and the research works headed in this direction at a very fast pace. Some partially homomorphic schemes are discussed in [3, 4, 5]. However, whether Fully Homomorphic Encryption could be achieved or not remained a question, the answer to which was given by Gentry in 2009[6]. FHE has its own shortcomings, and developments in overcoming the same and in extending FHE to all applications became an ongoing research area. One of the major shortcomings FHE possesses is the impracticality of the scheme in executing SQL operations over a cloud database due to high computational costs as discussed in [7]. This paper provides an overview of the research works proposed in the direction of FHE. Section II discusses the various FHE schemes proposed till data. Section III emphasizes on the various applications where FHE has proved its usability. However, query processing in FHE still remains an unresolved issue and very little work is done in this direction. Section IV discusses the few developments aiming at searching and sorting through FHE.

II. ACHIEVING FHE

The utility of constructing a fully homomorphic scheme was recognized long before. The first problem in this direction was proposed by Rivest et al [5], a convincing solution to which was developed more than 30 years later. During this period, the best result achieved was the Boneh-Goh-Nissim cryptosystem [8] in which evaluation of an unlimited number of addition operations was supported but was limited to at most one multiplication. The various FHE schemes proposed since then are discussed below, arranged chronologically.

A. Gentry(2009)

The first plausible construction in this direction was the work of Gentry [6] who used lattice-based cryptography and supported both addition and multiplication on ciphertexts, making it possible to construct circuits for the purpose of performing arbitrary computations. The public key was used to encrypt the decrypted circuit and on the growing noise in the ciphertext beyond an acceptable level, a new ciphertext was obtained by passing the ciphertext through the encrypted decryption circuit (called refreshing procedure). This property of the cipher was called bootstrappability.

B. Aldar C.F Chan (2009)

Chan [9] aimed to work on privacy homomorphism which allows operating on encrypted data and hence proposes two additive homomorphic schemes-Iterated Hill Cipher (IHC) and Modified Rivest Scheme (MRS). The two proposed schemes allow security against cipher-text only attacks. Plus different

representations of the same data in the encrypted domain are possible.

C. Smart and Vercauteren (2010)

Smart and Vercauteren [10] followed the work of Gentry [6] and likewise, developed a simplified and specialized version of the lattice based scheme of Gentry. The designed fully homomorphic scheme from a somewhat homomorphic scheme had significant improvements to Gentry's scheme like relatively small key and ciphertext size and smaller message expansion. Also, it allowed FHE over any field of characteristic two and uses elementary theory of algebraic number fields, thereby not requiring lattices for the understanding of encryption and decryption processes.

D. DGHV (2010)

van Dijk, Gentry, Halevi and Vaikuntanathan [11] in their proposal start by developing a somewhat homomorphic scheme with the use of only elementary modular arithmetic and then convert it into fully homomorphic encryption scheme using Gentry's method [6], the difference between the two methods is using simple addition multiplication over the integers instead of using ideal lattices over a polynomial ring. The use of simple addition multiplication operations makes the resultant algorithm conceptually simpler.

E. GH (2011)

Gentry and Halevi [12] present a new technique of achieving FHE. They propose a FHE scheme as a hybrid of SWHE and Multiplicative Homomorphic Encryption (MHE), purpose of which is to eliminate the squashing step of decryption circuit of the Gentry's SWHE scheme [13] which raises a Sparse Subset Sum Problem (SSSP) but still relying on bootstrapping. The main purpose of their proposal is to express the decryption function of the SWHE scheme of Gentry as a depth-3 arithmetic circuit of a particular form.

F. GHS (2011)

Gentry, Halevi and Smart [14] pointed out that the need for homomorphically evaluating the reduction of one integer modulo another is the main bottleneck of Gentry's FHE scheme [6], done typically by emulation of a binary modular reduction circuit using bit operations on binary representation of integers. The bottleneck was sufficiently reduced by working with modulus very close to a power of two. Their scheme was simpler and faster as compared to that of Gentry's and also reduced the size of the public key in some cases.

G. GHPS (2012)

Gentry, Halevi, Peikert and Smart [15] extended the work of Brakerski, Gentry and Vaikuntanathan [16] known as the BGV scheme of Fully Homomorphic Encryption over polynomial rings in the context of bootstrapping because implementation of such ring switching is non-trivial, the reason being reliability on the ring algebraic structure for their homomorphic properties. Their proposal is able to work on any cyclotomic ring and is useful in the context of bootstrapping and also in reducing the computational overhead achieved in BGV [16] due to the use of rings of very large dimension. For the reduction in computational overhead, authors switched to small ring ciphertexts.

H. Xiao et al (2012)

Xiao et al [17] proposed a non-circuit based symmetric key homomorphic encryption scheme which is a faster and a more secure variant of the Gentry's scheme [6]. The non-circuit based approach is more efficient as it does not require additional circuit computation overhead. The authors propose that instead of using one master key for retrieval of data from a server, as is done in existing homomorphic schemes, different user keys can be achieved from that one master encryption key. Also, they propose a protocol using these different user keys to provide a correct and secure communication between the server and the users.

I. Coron et al (2013)

The work of DGHV [11] over the integers was extended by Coron et al [18] for the purpose of batching FHE to a scheme supporting encryption and homomorphic processing of a vector of plain text bits as a single ciphertext. The resultant scheme was based on various techniques of [6, 11, 19, 20, 21] as it extends DGHV [11], supports the same batching capability of [20, 21] and has efficiency equal to that of [22]

J. GSW (2013)

The authors [23] present a conceptually simpler FHE scheme, based on learning with errors (LWE) problem, simpler because it builds FHE scheme using the approximate eigenvector method, instead of complicated multiplication and re-linearization steps of previously related schemes. The homomorphic addition and multiplication of their proposed scheme are just matrix additions and multiplications for most part of the scheme, the result of which is an easier and asymptotically faster. It also eliminates the need of an evaluation key as the evaluator is able to perform homomorphic operations without any knowledge of the user's public key except for some basic parameters, thereby constructing the first identity-based FHE scheme. Compilation of the work by Gorbunov et al [24] into an attribute-based FHE is also done, permitting homomorphic processing of the data encrypted under the same index.

K. Emura et al (2013)

Emura et al [25] aimed at controlling that who can perform the homomorphic operations; when and where. Because of the malleability property of

homomorphic encryption that anyone can perform the operations "freely", it becomes difficult to achieve adaptive chosen ciphertext (CCA) and homomorphic property simultaneously. The authors found a plausible solution to the problem by proposing a keyed- homomorphic public-key encryption (KH-PKE) which introduces a secret key to control who is allowed to perform the homomorphic operation. KH-PKE schemes are constructed by further introducing a new concept of homomorphic transitional universal hash family.

L. Kim et al [2015]

Kim et al [26] proposed a fully homomorphic scheme which generalizes the DGHV [11] scheme and modifies the third proposal of RSA [27] on the Chinese Remainder theorem and ring homomorphism. The proposed scheme is secure against the chosen plaintext attacks under the decisional approximate GCD assumption and the sparse subset sum assumption when the message space is restricted to Z_2^k. Also it has a relatively less overhead as compared to the overhead of the DGHV [11] scheme.

III. Applications Of FHE

Below are discussed some of the relevant research works applying FHE in different applications.

A. Damgard et al (2006)

Authors [28] propose an approach aiming at compilation of a class of Σ-protocols (3-move public-coin protocols) into non-interactive zero-knowledge arguments. Their proposal is based on homomorphic encryption and does not use random oracles. For the verifier, the only requirement is setting up of a private/public key pair. Their method applies to all known discrete-log based Σ-protocols. As for the applications point of view, their proposal obtains a non-interactive threshold RSA without random oracles and non-interactive zero-knowledge for NP with increased efficiency as compared to previous proposed methods in this direction.

B. Brenner et al (2011)

Authors [29] aimed at security of the data on cloud and propose to compute a secret program on an untrusted resource using FHE by designing a software implementation of the same. The scheme is capable of solving problems of encrypted storage access with encrypted addresses and encrypted branching and comprises of the runtime environment for an encrypted program and an assembler to generate the encrypted machine code.

C. Gahi et al (2011)

Authors [30] propose the first secure database system based on a FHE scheme with circuits for the implementation of SQL statements over encrypted data. A prototype of a database system for storing and processing data in encrypted form is built. Execution of SQL statements is done without any knowledge of the position of records extracted/ affected in the database. Performance analysis of the proposed scheme is done to measure the time a query on the database takes to execute and is found large due to impracticality of the existing homomorphic encryption schemes.

D. Wei and Reiter (2012)

Authors [31] propose practical methods allowing a client (the third-party) to evaluate a deterministic finite automaton (DFA) on an encrypted file stored at a server (the cloud), once authorized to do so by the file owner. The proposal aims to outsource the data to any third party along with limiting the use of that data by that particular third party. Their proposed protocols successfully protect the privacy of the DFA and the file contents from a malicious server and the privacy of the file contents (except for the result of the evaluation) from an honest-but-curious client (and, heuristically, from a malicious client.

E. GHS (2012)

Gentry, Halevi and Smart [22] implemented leveled homomorphic encryption (without bootstrapping) for evaluation of AES-128 circuit in three different ways developing AES- specific implementations and generic tools for FHE evaluation. The tools include variant of the BV scheme [32] and extension of BGV [16] scheme. The results of the implementations form the crux of their paper.

F. Bonneh et al (2012)

Boneh, Segev and Waters [33] insisted on targeted malleability; aiming to control the number of homomorphic computations one can perform on encrypted data. For this, they propose a generalized version of the work of Dolev, Dwork and Naor [34] in the direction of non-malleability. Their proposed scheme targets only a specific number of allowable functions. The construction part is done using standard cryptographic tools and on- succinct non-interactive arguments, both providing different efficiencies and are preferred depending on the underlying building blocks.

G. Gahi et al (2012)

A Location-Based Service (LBS) based on FHE can process encrypted inputs for retrieving encrypted location-related information which can further be decrypted only by the user who requested the data. Still, the encountered processing time and the upper limit imposed on the allowed number of operations are major unsolved challenges. This problem is addressed by Gahi et al [35] who built a fully secure FHE scheme allowing users to benefit from location-based services not compromising the data confidentiality and integrity. Their proposed scheme consisted of search circuits allowing an executor (i.e. LBS server) for receiving encrypted inputs/requests followed by performing a blind search for retrieval of encrypted

records matching the selection criterion. A querier can send the user's position and the service type he/she is looking for, in encrypted form, to a server and then the server would respond to the request without any knowledge of the contents of the request and the retrieved records. A prototype further improving the practicality of the proposed scheme was also proposed.

H. Gennaro and Wilch (2013)

The authors [36] propose and instantiate Fully HMACs and the concept of short tag for authentication of the result of the computations. The fully homomorphic message authenticator proposed is a symmetric-key variant of fully homomorphic signatures, defined by Boneh and Freeman [37]. Anybody is able to perform arbitrary computations over authenticated data; the only difference now will be of the short tag. The short tag makes it possible for the user to verify that the produced result is the correct and authenticated output of the given computation. Verification is done with the user's private key.

I. Wang et al (2013)

Authors [38] worked on the performance bottleneck of the Gentry Halevi FHE [12] and introduced an array of algorithmic optimizations employing aggressive pre-computation strategy; first is partial FFT to speed up modular multiplications by introducing Strassen's FFT based multiplication algorithm, and second is full FFT optimization to gain additional speed by eliminating the majority of FFT conversions via delayed modular reductions and by performing the bulk of the computations directly in the FFT domain.

J. Yukun et al (2013)

Authors [39] propose a novel secure metering data collection scheme to check tampering of (Smart Meters) SM data in protecting users' privacy premise. Assuming that the SM data includes two types, one is the power consumption value from the last slot to the current slot and the other is the SM reading in the current slot where the consumption value is result of the difference between SM reading in the current slot and that in the last slot, authors use HE to see whether the comparison of both the types gives equal results or not. This comparison makes the Energy Suppliers (ES) aware whether tampering of data has taken place or not. Their proposed scheme is efficient enough even if links between ES, TTP (Trusted Third Party) and SM are not reliable all the time and works even if SM data is correct in the current slot but tampered in the last slot. Comparisons with message digest and digital signature are also provided.

K. Gauraha et al (2013)

Authors [40] propose a secure FHE scheme that fulfills I/O confidentiality, duplicitous pliability and competence. Such a duplicitous pliability project can be hustled in the overall mechanism of FHE with close-to-zero additional overhead. The results show the practicality of the scheme. The steps of the scheme include devising robust algorithms for achieving numerical stability, exploring the dense matrix, sparse matrix structure of problem for further efficiency improvement, reading alignment in the form of sequence of se servers, Achieving desired encryption through the Stochastic chain process.

L. Mani et al (2013)

Mani, Shah and Gunda in 2013 [41] addressed the issue of impracticality of the Gentry's FHE scheme for query processing on an encrypted database. As a solution, the authors propose a data model representing relational tables and intermediate results during query processing; a computational model for the purpose of processing queries by the service provider on the encrypted data; algorithm for related operators matching our data and computational models and lastly, techniques for transferring back the results of the queries to the client side.

M. Gupta et al (2013, 2014, 2015)

Authors in [42,43] emphasized on the need of symmetric FHE schemes because certain applications inherently need secret keys and proposed Fully Homomorphic schemes with symmetric keys based on matrix operations. The time complexity has been claimed to be linear in the security parameter λ. No refresh procedure has been included as there is no noise accumulation. Also, a protocol of hierarchical division of keys is proposed which makes it possible to provide partial access to encrypted data in a multiuser environment. In [44] a fully homomorphic scheme with symmetric keys, over integers is proposed based on linear algebra. There is no requirement of evaluation key in this scheme, making it suitable for outsourcing computations over encrypted data and private information retrieval**.**

N. Joo and Yun (2014)

The authors in [45] work on achieving Homomorphic Authenticated Encryption (HAE) in a twofold way; first by defining security notions in HAE with comparisons between each followed by creating a HAE scheme which is somewhat homomorphic for arithmetic circuits. The proposed scheme is secure against ciphertext attacks both for privacy and authenticity and is based on the error-free approximate GCD assumption.

O. Yuan and Yu (2014)

When talking about collaboration of multi parties by conducting joint Back-Propagation neural network learning on the union of their respective data sets, an open problem exists due to lacks of a solution that allows two or more parties, each with an arbitrarily partitioned data set, to collaboratively conduct the learning. Authors [46] address this open problem by utilizing the power of cloud computing and proposing a FHE scheme, allowing each party to encrypt his/her private data locally followed by uploading the

ciphertexts into the cloud. The cloud then executes most of the operations pertaining to the learning algorithms over ciphertexts without knowing the original private data. The computation and communication costs for each party are minimal with no dependence on the number of participants because the expensive operations are safely loaded to the cloud.

P. Vijay and Sharma (2014)

Authors [47] propose a symmetric FHE scheme based on the DGHV scheme [11]. FHE is extended for Verifiable Delegation of Computation and Input Verifiability and two protocols have been designed for the same. The ciphertexts accumulate noise after a certain number of computations, therefore a refresh scheme is proposed.

IV. Searching/ Sorting through FHE

A. Han et al (2012)

Authors [48] propose a new system for searching on encrypted data which combined ABE (Attribute based Encryption) and FHE, enabling anyone even without private-key of the encrypted data to search the data. Application and Implementation of FHE on outsourcing of computation is also done.

B. Wang et al (2012)

Authors [49] analyze the usage of fully homomorphic encryption on query processing and show that FHE schemes supporting addition, multiplication, AND and XOR operations on ciphertexts are well able to carry out complex aggregations, joins, range or selection queries on the server side and return the answers to the same in a result buffer. In cases, where answer sizes to queries are not known, no guarantee is possible about whether all matching answers will be correctly constructed from the result buffer or not. If not, answers can be constructed using overwhelming probabilities.

C. Guan et al (2013)

Authors [50] start their proposal by first proving that a homomorphic encryption with a function to detect zero, detect equality, compare the value or detect overflow on ciphertexts is not secure if there is no restriction to limit the times of operating these functions. But with some restrictions, a homomorphic encryption scheme can still detect zero with the key-owner decrypting the ciphertext and announcing the result if all people are allowed to detect zero on ciphertexts. If on the other hand, only few people are allowed for the same when key-owner agrees, symmetric homomorphic encryption scheme with proposed new version of ring learn with error assumption is done.

V. Conclusions

Information Security with usability forms the basis of HE. Since the beginning of research headed at cryptography and its primitives, HE was around it. But the need for HE is more recent, therefore, the developments in the past few years have been major. The next problem to be addressed in HE was building FHE schemes. Started by Gentry, the FHE schemes proposed focus on making FHE efficient in terms of cost and query processing. This paper surveys the development of HE to FHE and the recent research works headed in the direction of FHE related to query processing in FHE. Also, it discusses the work done in proving effectiveness of the scheme in various applications.

References

[1] S.Kokila and T. Princess Raichel, Software as a Service, a Detailed Study on Challenges and Security Threats, *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, Vol. 2, Issue 12, pp. 9-14, 2015.

[2] K.Iswarya, Security Issues Associated With Big Data in Cloud Computing , *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, Vol. 1, Issue 8, pp. 1-8, 2014.

[3] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, Vol. 21, Issue 2, pp.120–126, 1978.

[4] T. Elgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions On Information Theory*, Vol. IT-31, No. 4, 1985.

[5] Paillier, Public-key cryptosystems based on composite degree residuosity classes, *Proceedings of EUROCRYPT-99*, Springer, pp. 223–238, 1999.

[6] C. Gentry, Fully homomorphic encryption using ideal lattices, *Proceedings of the 41st ACM Symposium on Theory of Computing*, STOC 2009, pages 169-178. ACM, 2009.

[7] K. Sravani and D. Praveen Kumar, Data Confidentiality, performance and cost evaluation of public cloud databases through adaptive encryption scheme, *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, Vol. 2, Issue 6, pp. 18-22, 2015.

[8] D. Boneh, E.-J. Goh, and K. Nissim, Evaluating 2-DNF formulas on ciphertexts, TCC *2005*, 2005.

[9] A.C.F Chan, Symmetric-Key Homomorphic Encryption for Encrypted Data Processing, *IEEE*, 2009.

[10] N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes, *Public Key Cryptography – PKC 2010*, Berlin, Heidelberg, New York, 2010.

[11] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers, *Proceedings of Eurocrypt-10, Lecture Notes in Computer Science, vol 6110*, Springer, pp 24-43, 2010.

[12] C. Gentry and S. Halevi. Implementing Gentry's fully homomorphic encryption scheme, *EURO-CRYPT 2011*, Springer, K. Paterson (Ed.), 2011.

[13] C. Gentry and S. Halevi, Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits, *Cryptology ePrint Archive: Report 2011/279*, 2011

[14] C. Gentry, S. Halevi and N. P. Smart, Better bootstrapping in fully homomorphic encryption, *Cryptology ePrint Archive, Report 2011/680*, 2011.

[15] C. Gentry, S.Halevi, C.Peikert and N. P. Smart, Ring Switching in BGV-Style Homomorphic Encryption, *Proceedings of the 8th International Conference, SCN 2012*, pp 19-37, 2012.

[16] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, Fully homomorphic encryption without bootstrapping, *Cryptology ePrint Archive, Report 2011/277*, 2011.

[17] L.Xiao, O. Bastani and I-L.Yen, An Efficient Homomorphic Encryption Protocol for Multi-User Systems, University of Texas at Dallas, 2012.

[18] J.S. Coron and T. Lepoint and M. Tibouchi, Batch Fully Homomorphic Encryption over the Integers, *Cryptology ePrint Archive: Report 2013/036*

[19] N. P. Smart, F. Vercauteren, Fully homomorphic SIMD operations, *Designs, Codes and Cryptography*, Volume 71, Issue 1, pp 57-81, 2014

[20] Z. Brakerski and V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard)LWE, *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science , FOCS'11*, pages 97-106. IEEE Computer Society, 2011.

[21] Z. Brakerski and V. Vaikuntanathan, Fully homomorphic encryption from Ring-LWE and security for key dependent messages, Phillip Rogaway, editor, *Advances in Cryptology, CRYPTO 2011 , volume 6841 of Lecture Notes in Computer Science* , pages 505-524, Springer, 2011.

[22] C. Gentry, S. Halevi, and N. P. Smart, Homomorphic evaluation of the AES circuit, Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 , volume 7417 of LectureNotes in Computer Science* , pages 850-867, Springer, 2012.

[23] C. Gentry, A. Sahai and B. Waters, Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, *Advances in Cryptography-CRYPTO 2013, Volume 8042 of the series Lecture Notes in Computer Science*, pp 75-92

[24] S. Gorbunov, V. Vaikuntanathan, and H. Wee, Attribute-based encryption for circuits, *STOC*, pages 545-554, 2013.

[25] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda and S. Yamada, Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption, *Proceedings of the 16th International Conference on Practice and Theory in Public-Key Cryptography*, Nara, Japan, pgs 32-50, doi-10.1007/978-3-642-36362-7_3, 2013.

[26] J. H.Cheon, J. Kim ,M. S. Lee and A. Yun, CRT-based fully homomorphic encryption over the integers, *Information Sciences*, Volume 310, Pages 149–162, 2015

[27] W. Diffie, M. Hellman, ,New directions in cryptography, *IEEE Transactions on Information Theory*, Vol.22, Issue 6, pp. 644–654, 1976

[28] I. Damgard, N.Fazio and A. Nicolosi, Non-interactive Zero-Knowledge from Homomorphic Encryption, *Proceedings of the Third Theory of Cryptography Conference, TCC 2006, New York, Volume 3876 of the series Lecture Notes in Computer Science*, pp 41-59, 2006.

[29] M. Brenner, J. Wiebelitz, G. von Voigt and M. Smith, Secret Program Execution in the Cloud Applying Homomorphic Encryption, *Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011*), Korea, 2011

[30] Y.Gahi, M. Guennoun and K. El-Khatib, A Secure Database System using Homomorphic Encryption Schemes, *Proceedings of the Third International Conference on Advances in Databases, Knowledge, and Data Applications, DBKDA 2011*, 2011.

[31] L. Wei and M. K. Reiter, Third-Party Private DFA Evaluation on Encrypted Files in the Cloud, *Proceedings of the 17th European Symposium on Research in Computer Security, Pisa, Italy, Volume 7459 of the series Lecture Notes in Computer Science*, pp 523-540, 2012

[32] Z. Brakerski and V. Vaikuntanathan, Fully homomorphic encryption from ring-LWE and security for key dependent messages, *Advances in Cryptology–CRYPTO 2011*, Springer Berlin Heidelberg, 505-524, 2011.

[33] D. Boneh, G. Segev and B. Waters, Targetted Malleability-Homomorphic Encryption for restricted computations, *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12*, Pages 350-366, ACM New York, USA, , 2012.

[34] D. Dolev, C. Dwork, and M. Naor, Non-malleable cryptography, *SIAM Journal on Computing* , Volume 30, Issue 2, pp:391–437, 2000.

[35] Y. Gahi, M. Guennoun, Z. Guennoun and K. El-Khatib, Privacy Preserving Scheme for Location-Based Services, *Journal of Information Security*, Volume 3, 105-112, 2012.

[36] R. Gennaro and D. Wichs, Fully homomorphic message authenticators, ASI-*ACRYPT 2013*, 2013.

[37] D. Boneh and D. M. Freeman, Homomorphic signatures for polynomial functions, K. G. Paterson, editor, *EUROCRYPT 2011, volume 6632 of LNCS*, pages 149-168. Springer, May 2011.

[38] W. Wang, Y. Hu, L. Chen, X. Huanga and B. Sunar, Exploring the Feasibility of Fully Homomorphic Encryption, *IEEE Transactions on Computers*, Volume 64, Issue 3, doi-10.1109/TC.2013.154, 2013.

[39] N. Yukun, T. Xiaobin, C. Shi, W. Haifeng, Yukai And B. Zhiyong, A Security Privacy Protection Scheme for Data Collection of Smart Meters Based on Homomorphic Encryption, *EuroCon 2013*, Croatia, 2013

[40] N. Gauraha, D. Mishra and P. Trivedi, Data Security in Distributed System using Fully Homomorphic Encryption and Linear, *Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT)*, pgs- 423-425, 2013.

[41] M. Mani, K. Shah, M. Gunda, Enabling Secure Database as a Service using Fully Homomorphic Encryption: Challenges and Opportunities, published in arXiv:1302.2654, 2013.

[42] C.P. Gupta and Iti Sharma, A Fully Homomorphic Encryption scheme with Symmetric Keys with Application to Private Data Processing in Clouds, *Proceedings of the Fourth International Conference on Network of the Future (NoF'13)*, Pohang, Korea, Oct 2013.

[43] Iti Sharma, C.P. Gupta, ,Making Data in Cloud Secure and Usable: Fully Homomorphic Encryption with Symmetric keys, *International Journal of Communication Networks and Distributed Systems*, Inderscience. 2015 Vol. 14 No. 4 pp 379-399, 2015.

[44] N. Aggarwal, C.P. Gupta, Iti Sharma, Fully Homomorphic Symmetric Scheme without Bootstrapping, *Proceedings of International Conference on Cloud Computing and Internet of Things (CCIOT)*, pp 14-17, 2014.

[45] C. Joo and A. Yun, Homomorphic Authenticated Encryption Secure against Chosen-Ciphertext Attack, *Advances in Cryptology – ASIACRYPT 2014*, Vol 8874 of the Lecture Notes in Computer Science, pp 173-192, 2014.

[46] Jiawei Yuan and Shucheng Yu, Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing, *IEEE Transactions On Parallel And Distributed Systems*, Vol. 25, No. 1, pgs 212-221, 2014.

[47] A. Vijay and V. K. Sharma, Verifiable Delegation of Computation through Fully Homomorphic Encryption, *International Journal of Computer Applications*, Volume 97, Issue 15, pp:35-40, July 2014.

[48] Jing-Li, Han Ming Yang, Cai-Ling Wang and Shan-Shan Xu, The Implementation and Application of Fully Homomorphic Encryption Scheme, *Proceedings of the 2012 Second International Conference on Instrumentation & Measurement, Computer, Communication and Control*, 2012

[49] S. Wang, D. Agrawal, and A. El Abbadi, Is Homomorphic Encryption the Holy Grail for Database Queries on Encrypted Data?, Technical Report, Department of Computer Science, UCSB, 2012

[50] D. J. Guan, Chen-Yu Tsai and E. S. Zhuang, Detect Zero by Using Symmetric Homomorphic Encryption, *Proceedings of the 2013 Eighth Asia Joint Conference on Information Security*, 2013.and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.