International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Privacy Preserving Outsourced Calculations With Symmetric Fully Homomorphic Encryption

C.N.Umadevi, N.P.Gopalan

***Abstract*: Cloud computing is a new paradigm which provides cloud storage service to manage, maintain and back up private data remotely. For privacy concerns the data is kept encrypted and made available to users on demand through cloud service provider over the internet. The legacy encryption techniques rely on sharing of keys, so service providers and end users of the cloud have exclusive rights on the data thus the secrecy may loss. Homomorphic Encryption is a significant encryption technique which allows users to perform limited arithmetic on the enciphered data without loss of privacy and security. This paper addresses a new simple and non-bootstrappable Fully Homomorphic Encryption Scheme based on Q_P^n matrices as symmetric keys with access control.**

***Keywords*: Access Policy, Fibonacci P-Number, Fully Homomorphic Encryption, Smith Normal Form, Semantic Secure.**

I. INTRODUCTION

Homomorphism is a map preserving mathematical structure and in the field of cryptography homomorphism can be enforced as an encryption technique which allows an arbitrator to perform certain operations on the ciphers without any insight of encryption algorithm and keys used. The word homomorphism was found in the context [1] and it has propelled the researchers to design such systems. The Homomorphic Encryption (HE) schemes are categorized into the following types based on the number of operations allowed over the cipher:

- Partially Homomorphic Encryption (PHE)
- Somewhat Homomorphic Encryption (SWHE)
- Fully Homomorphic Encryption (FHE)

In an open untrusted network the data can be kept secure and confidential using Homomorphic Encryption and the encrypted data can be involved in some computations. Let M is the secret message, C is the Cipher obtained by the encryption function Encrypt (M) and Decrypt(C) repossess M then by FHE,

$$G(M) = \text{Decrypt}(G(C))$$

Where, G is an arithmetic function.

Cloud computing paradigm provides its services to its users through cognate devices as pay-per-use at any time but data security and privacy are its prominent dilemma. By stipulating FHE schemes to bestow security and some access control scheme to prevent the cloud users to access everything, this problem can be fixed. This paper addresses a symmetric FHE scheme based on Q_P^n matrices with access control in which access control policies are asserted in eXtensible Access Control Markup Language (XACML).

A. Literature Survey

The Fully Homomorphic Encryption systems:

The aboriginal FHE scheme was introduced in 2009 [2] and several variations of this scheme was found in [3]-[10] with lattice based techniques in backdrop. They are all PHE schemes in initial and later bootstrapped to FHE schemes thus made them to be complex and impractical. A new FHE scheme based on integers [11] swamped the above said intricacy. Later many mutated integer and Linear Algebra based schemes [12] - [17] are introduced.

Access Control:

Access control is a process of authorization and authentication of shared resources with selective restriction over it. The request to access a resource is either granted or denied based on access control policies. The work found in [18]-[20] proposes many access policy structures. An XML based access control policy frame work is Extensible Access Control Markup Language (XACML), is a general purpose, flexible, powerful language with separate communication for request and response and supports different platforms and languages for dynamic and complex systems. The access control policies are written and can be embedded to the attributes which needs to be controlled from access. The following table layouts the test attributes that can be expressed in access policy.

Table.I Test Policy attributes and their descriptions

S.No.	Attribute Description	Test policy Attributes
1	A unique ID for each access	Access ID
2	Role or Name of the accessor	Subject
3	Name of the resource	Object
4	Access rights	Action
5	The IP address of the preferred machine	IP Address
6	The maximum access count	Max.Access count
7	The time elapses to access	Time
8	The date elapses to access	Duration
9	To restrict access based on location	Location

Manuscript published on 30 August 2019.
*Correspondence Author(s)
C.N.Umadevi, Research and Development Centre, Bharathiar University, Coimbatore, Tamilnadu, India,
N.P.Gopalan, Department of Computer Applications, National Institute of Technology, Trichy, Tamilnadu,, India,

B. Our contribution

The present paper addresses a new FHE technique with Q_P^n matrices as symmetric keys and the homomorphic behavior is assured by Smith Normal Form (SNF). The symmetric key of this system exhibits a size of O (1) and the cipher text size is also fixed regardless of the size of secret message. The access control technique addressed in this paper is a CP-ABE scheme in which access control policies are written in XACML. Thus the proposed system preserves the secrecy, privacy of the secret data and allows the cloud end user to perform calculations on the encrypted data without decryption. The access control system provides a controlled access over the encrypted data thus any access which satisfies the access policy can only gain access on encrypted data. Thus the proposed system imparts an encrypted controlled access over the ciphers stored in enigmatic networks.

II. PRELIMINARIES

All the computations involved in this scheme are based on integers in a ring Z_N to operate in ring $M_4(Z_N)$, where N is a composite number which need not be prime and it is a product of 2m odd mutual prime numbers p_i and q_i such that 1<=i<=m. The plain text space is transformed into a matrix M_4 (Z_N) before encryption. The system also involves two arbitrary integers n_1, $n_2 \in Z_N$, and let P=3, where P is a Fibonacci P-number. The n_1 and n_2 are used to generate the n_1^{th} and n_2^{nd} Fibonacci number, they are used to construct Q_P^{n1} and Q_P^{n2} matrices and are the symmetric keys of this system having the properties of invertible, uni modular and square matrices.

Smith Normal Form

Smith Normal Form (SNF) can be used to solve polynomials of invariant coefficients, linear programming involving integers, Diophantine equations and so on.

Definition 1

A matrix $D \in M_N (Z_N)$ is an invertible matrix if and only if the determinant of D is not equal to 0 and GCD (determinant of D, N) =1.

Definition 2

Let $R_{m\times n}$ is a set of all m×n integer matrices, the matrices α, β of $R_{m\times n}$ are said to be in Smith Normal Form if and only if β=S α T where, S and T are unimodular, invertible matrices such that $S \in R_{m\times m}$ and $Q \in R_{n\times n}$.

Definition 3

If β = S α T is in Smith Normal Form then α and β are said to be equal matrices

(β ~ α) and $\alpha = S^{-1} \beta T^{-1}$ also holds in $R_{m\times n}$ where S^{-1} and T^{-1} are the inverses of S and T.

Transformation of integer to M_4 (Z_N)

Any secret integer $T \in Z_N$ is converted into a diagonal matrix M_4 and the following steps shows how this coding is performed:

i. r is any arbitrary integer such that $r \in Z_N$.
ii. Using the values of r and T construct the linear congruence $x \equiv x_i \pmod{f_i}$, $y \equiv y_i \pmod{f_i}$ and $z \equiv z_i \pmod{f_i}$.
iii. Solve the above linear congruence equations using Chinese Remainder Theorem and construct a diagonal matrix D (T, x, y, z).

The r value makes our system IND-CPA. The selection of r is dependent on N but when these values thrives it do not influence the encryption and decryption scheme. For the same plain text T and N with different r value different ciphers can be generated.

III. SYMMETRIC FULLY HOMOMORPHIC ENCRYPTION AND DECRYPTION

The encryption and decryption technique involves the following algorithms and are subject to modulo N operations:

1. Key-Generation (n1, n2)

Step 1: Select any two large integers (n1, n2) mod N and let P=3.

Step2: Find the $n1^{th}$ and $n2^{nd}$ Fibonacci numbers and generate Q_P^{n1} and Q_P^{n2} matrices and they are the symmetric key pairs.

2. Encrypt (D(T,x,y,z), Q_P^{n1} , Q_P^{n2})

The encryption process is simply the matrix multiplication of the symmetric keys and the plan text diagonal matrix D.

Cipher C= (Q_P^{n1}. D (T, x, y, z). Q_P^{n2}) mod N

3. Decrypt(C, $(Q_P^{n1})^{-1}$, $(Q_P^{n2})^{-1}$)

Compute the inverses of the symmetric key pairs and the resultant of the simple matrix multiplication is M.

T= $(M)_{1,1}$ =Decrypt ($(Q_P^{n1})^{-1}$. C. $(Q_P^{n2})^{-1}$) mod N

Performing fully homomorphic computations over the ciphers:

Let the ciphers CP1 and CP2 of the plain text integer T1 and T2 respectively then the FHE system provides the following computations:

Decrypt [(CP1+CP2) mod N] = T1+ T2
Decrypt [(CP1- CP2) mod N] =T1- T2
Decrypt [(CP1×CP2) mod N] = T1× T2

IV. SYSTEM ARCHITECTURE

The system architecture is given in Fig. 1 and our system incorporates the following entities to render encrypted data processing without loss of privacy and confidentiality of outsourced data.

1. **Cloud Data Owner (CDO):** The CDO outsources their private data to cloud, and security and confidentiality is retained by fully homomorphic encryption and the access is controlled using XACML policies stored in Attribute Server (AS).
2. **Cloud Users (CU):** Cloud Users are the data processing entities. The access of a CU is controlled by the access policies written in XACML that are stored in the Attribute Server. Each CU is controlled through different test policy attributes against the ciphers that they access. In addition to a unique Access ID, Object, Subject and Action, a CU can be controlled over Time, IP address, their location, maximum access count or date of access.

3. **Cloud Server (CS):** The fully homomorphically encrypted data are stored in the CS which works in harmony with the AS. The symmetric keys used for encryption are kept secret by the CDO and are often refreshed. The CS and AS are fully controlled by the CDO.
4. **Cloud Service Provider (CSP):** The CSP acts as an interface between the Cloud and the CU. The CU registers with the CSP whose user credentials are verified on each logon and on successful logon they are directed to the CS where their access credentials are verified by the AS for each access. Thus the whole encrypted data outsourcing and access control aspects are hidden from the CSP and CU.

Thus our system provides a strong security and access control over the outsourced data.

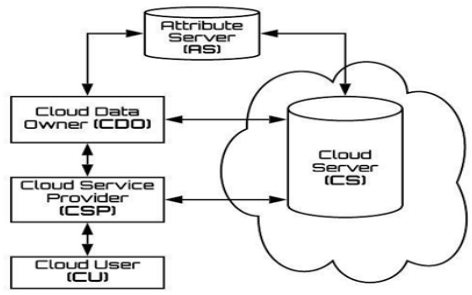

Fig.1. System Architecture

V. SECURITY AND ANALYSIS

The outsourcing and computations over the ciphers of a data stored in a private cloud can be accredited by the FHE schemes and it possesses the following characteristics:

- IND-CPA
- Data and computations are privacy preserving
- Compact

An encryption scheme in which two different encryptions of the same secret data is not same is said to be semantic secure or IND-CPA. The transformation of the secret integer μ to a matrix M_4 (Z_N) is based on the arbitrary integer r. The same symmetric key pair and μ with different r value the encryption algorithm produces different ciphers. Thus our scheme is IND-CPA. The CU is allowed to access and perform operations on the encrypted data based on access policies. Since our scheme is IND-CPA the processing entity CU cannot speculate the plain text from the known cipher text, thus making our system and computations over the cipher as privacy preserving one.

The symmetric FHE scheme discussed in this paper do not unfolds the size of the ciphers when operations are performed over it. The plain text integer, ciphers and result of computations over the ciphers all are 4×4 matrices in the message space of N. The size of the ciphers is independent of the upshot of the evaluation function thus our system is compact.

The encryption and decryption algorithms are executed in MATLAB having the secret integer 257 with different r and N values and the following table shows the cipher, execution time for encryption and decryption algorithms. Thus our scheme is IND-CPA with different r and N values but same plain text.

Table. II Execution time of Encryption and Decryption Algorithms

SECRET DATA	r	CIPHER	N	ENCRYPTION TIME	DECRYPTION TIME
257	292	980	1155	0.00056	0.00062
257	1046	1085	3003	0.00063	0.00065
257	37962	44308	55913	0.00063	0.00078

The following Fig.2 shows the variations in the sizes of r, N and cipher for the secret integer 257.

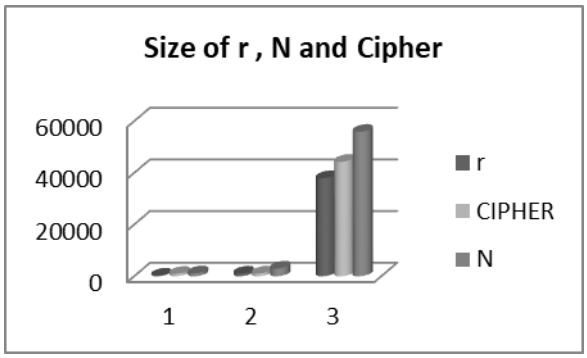

Fig.2. Comparing the sizes of r, N and ciphers

Comparison with other schemes:

The present scheme is compared with the literatures ([5], [11] and [12]) on various parameters and it is tabulated below:

Table. III comparison of schemes with our scheme

Parameters	[5]	[11]	[12]	Our scheme
Cipher size	$O(\lambda.d^2)$	$O(\lambda^{10})$	$O(\lambda)$	O(1)
Message Space	R_P	{0,1}	N/Z_N	N/Z_N
Technique used	LWE	Integers	Linear Algebra	Matrices
Public key size	$O(\lambda^2)$	$O(\lambda^2)$	NA	NA
Secret key	$O(\lambda^{10})$	$O(\lambda^{10})$	$O(\lambda)$	O(1)
Bootstrapping	Not needed	yes	Not needed but uses refresh key of size O(log λ)	Not needed
Type of Homomorphic Encryption	SWHE	FHE	FHE	FHE

VI. CONCLUSION

This paper introduces a new Symmetric Fully Homomorphic Encryption scheme. It is simple, noise free, IND-CPA secure, needs no bootstrapping with a message space Z_N and the plain text integer is encoded into a matrix M_4 (Z_N) using CRT. The access policy and the cipher are controlled by the Cloud Data Owner and are hidden from the external world. All the computations over the cipher are in the domain of commutative algebraic matrices.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The access policy is expressed using XACML which makes the scheme light weight. Thus this scheme finds its applications even in dark networks to secure private secret data.

REFERENCES

1. R.Rivest, A.Shamir and L.Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, 21(2), pp. 120-126.
2. Gentry, A Fully Homomorphic Encryption Scheme, Dissertation, https://crypto.stanford.edu/Craig/Craig-thesis.
3. Pierre-Alain Fouque, Benjamin Hadjibeyli and Paul Kirchner, "Homomorphic Evaluation of Lattice-Based Symmetric Encryption Schemes", https://eprint.iacr.org/2019/653.pdf.
4. Gentry, Craig. (2009). Fully Homomorphic Encryption Using Ideal Lattices. Proceedings of the Annual ACM Symposium on Theory of Computing. 9. 169-178. 10.1145/1536414.1536440.
5. T. Plantard, W. Susilo and Z. Zhang, "Fully Homomorphic Encryption Using Hidden Ideal Lattice", IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2127-2137, Dec. 2013.
6. Gu, Chunsheng. (2011). Fully Homomorphic Encryption, Approximate Lattice Problem and LWE. IACR Cryptology ePrint Archive. 2011. 114. 10.11591/closer.v2i1.1339.
7. Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba. Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics. 1st Cross Domain Conference and Workshop on Availability, Reliability, and Security in Information Systems (CD-ARES), Sep 2013, Regensburg, Germany. pp.55-74.
8. K. Hariss, M. Chamoun and A. E. Samhat, "On DGHV and BGV fully homomorphic encryption schemes," 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, 2017, pp. 1-9.
9. T. Shen, F. Wang, K. Chen, K. Wang and B. Li, "Efficient Leveled (Multi) Identity-Based Fully Homomorphic Encryption Schemes," in IEEE Access, vol. 7, pp. 79299-79310, 2019.
10. W. Weili, H. Bin and Z. Xiufeng, "Identity-based leveled fully homomorphic encryption over ideal lattices," 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), Beijing, 2017, pp. 377-381.
11. M. Van Dijk, C. Gentry, S. Halevi and V.Vaikuntanathan, Fully homomorphic encryption over the integers, Proceedings of EUROCRYPT-2010, Lecture Notes in Computer Science, vol. 6110, Springer, pp.24-43.
12. Martins, Paulo & Sousa, Leonel & Mariano, Artur. (2017). A Survey on Fully Homomorphic Encryption: An Engineering Perspective. ACM Computing Surveys. 50. 1-33. 10.1145/3124441.
13. Iti Sharma, A Symmetric FHE scheme based on Linear Algebra, International Journal of Computer Science and Engineering Technology, Vol.05, pp.558-562.
14. Beunardeau, Marc & Connolly, Ais & Géraud, Rémi & Naccache, David. (2016). Fully Homomorphic Encryption: Computations with a Blindfold. IEEE Security & Privacy. 14. 63-67. 10.1109/MSP.2016.8.
15. J. Coron, T.Lepoint and M.Tibouchi, Batch fully homomorphic encryption over the integers, https://eprint.iacr.org/2013/36.pdf
16. L. Cardoso dos Santos, G. Rodrigues Bilar and F. Dacêncio Pereira, "Implementation of the fully homomorphic encryption scheme over integers with shorter keys," 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, 2015, pp. 1-5.
17. J. Ye and M. Shieh, "Low-Complexity VLSI Design of Large Integer Multipliers for Fully Homomorphic Encryption," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 9, pp. 1727-1736, Sept. 2018.
18. Ding, Yong & Han, Bo & Wang, Huiyong & Li, Xiumin. (2018). Ciphertext retrieval via attribute-based FHE in cloud computing. Soft Computing. 22. 10.1007
19. Ahmed El-Yahyaoui, and Mohamed Daifr Ech-Cherif El Kettani, "About Fully Homomorphic Encryption Improvement Techniques," International Journal of Embedded and Real-Time Communication Systems, vol. 10, no. 3, pp. 1–20, 2019.
20. Clear, Michael, Hughes, Arthur, Tewari and Hitesh. (2013). Homomorphic Encryption with Access Policies: Characterization and New Constructions. 0.1007/978-3-642-38553-7_4.

AUTHORS PROFILE

C.N.Umadevi, received B.Sc., Computer Science from Madras University, Tamilnadu, India in 1998. Then received M.Sc., and M.Phil., degrees from Bharathidasan University, Tamilnadu, India in 2001 and 2004 respectively. Now working as a research scholar of Bharathiar University, Tamilnadu, India. Attended and submitted papers in more than five international conferences organized by IEEE, ACM and Scopus.

Dr. N. P. Gopalan, received MSc. in Mathematics from Madras University in the year 1978 and received PhD in Applied Mathematics from IISc. Bangalore, in 1983 and joined ISRO as Scientist B and worked in classified Projects for 6 months. Joined NIT and is serving it for the past 33 years. Wrote 5 text books published from Prentice Hall India and has 60 international and more than 100 conference papers. He is a reviewer for IEEE and Elsevier journals. Supervised and completed 14 PhD students in various areas. Awarded the Eminent Engineer from Institution of Engineers, India, in February 2016. Has a Patent for wireless underwater Robot design.