IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

Comparative Analysis of Tensor Based Light Weight FHE

Vinay Kumar Devara[1], Dr. Anshul Mishra[2], Dr. D. Ramesh [3]
Research Scholar Department of Computer Science[1]
Research Supervisor Department of Computer Science and Engineering[2]
NIILM University, Kaithal, Haryana, India[1,2]
Research Co-Supervisor Department of Computer Science[3]
Kakatiya University, Warangal-TG, India[3]

Abstract: *The Homomorphic Encryption technique does a computational operation on unoriginal data. There are a few reasons for the inconvenience of the existing structure. One of the reasons is the inherent slow blueprint because of a bootstrapping procedure or cap her text refreshing algorithm, complex circuit examination because of bit w_i seen crypton, large message expansion, and public key. In this research, the FHE based symmetric key is used. Here the proposed framework was analyzed with the various security level, and it provides semantic security. Later, the novelty of the proposed framework was proved with an experimental analysis and comparative analysis. In the future, crypt analysis would be analyzed on FHE based symmetric key.*

Keywords: Cloud Computing, Homomorphic Encryption technique.

I. INTRODUCTION

Nowadays, most people store and maintain their sensitive data over the cloud server. Increasing storage and transmission of data over the cloud increases the vulnerability of data. For this purpose, a standard encryption mechanism was used to ensure authenticity, integrity, and confidentiality. Homomorphic encryption plays a key role in cloud computing.

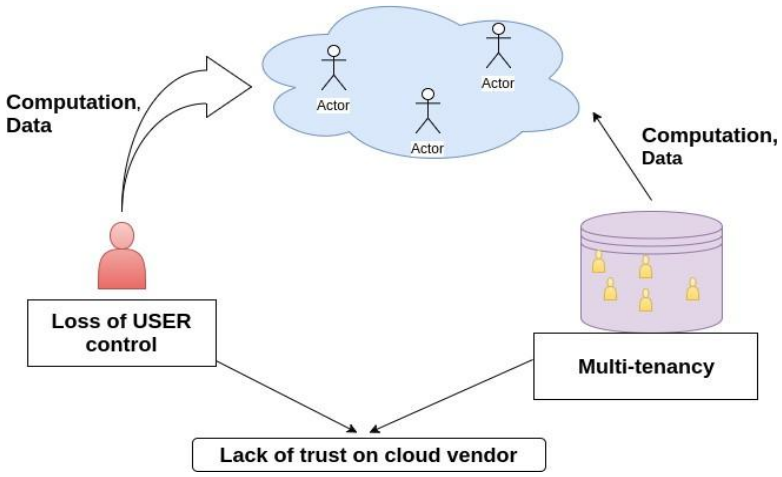

Figure 1: Security Concerns in Cloud Computing

Figure1 represents the limit to cloud computing on the cloud vendor side. In homomorphic encryption, the cipher text is forwarded to the cloud, computation is performed directly on ciphertext, and the computation output will be in ciphertext form.

The computations result is decrypted to obtain the respected play in text. If the structure of supports numerous multiplication and addition operations, and examining arithmetic encrypted data circuits, it's referred to as FHE. The client can trust in the CSP for the transfer of data. Few security issues in cloud computing are data is transferred by the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

client to the third party over a common cloud server. If small security vulnerability occurs in any technology like memory management, load balancing factor, transaction management, resources, virtualization scenario, network structure, database, etc might pull down the entire system. Figure 1 illustrates security concerns.

Gentry [1] introduced 3 steps procedure for a secure FHE scheme using ideal lattices. Smart et al. [2] constructed the first attempt to implement the Gentry created an FHE structure which has small-sized ciphertext and key. Later Dijk et al. [3] introduced the FHE structure which utilizes simple integer arithmetic. Xiao et al. [6] create demon-circuit dependent symmetric key HE structure. Liang

[10] made asymmetric and symmetric QHE (Quantum Fully Homomorphic Encryption) and also created four symmetric QHE structures and distributed key issuing with the use of secret sharing facilitates functioning quantum operators. Chen et al. [11] introduced an FHE structure depending on LWE (Learning With Error) phenomenon for effective key size. Hemal Atha et al. [12] presented an FHE structure depending on the ring for secure data over cloud computing. Sharma [13] utilized symmetric key FHE structure to work with bits of plain text to convert them to an integer using linear algebra. Filho et al. [14] introduced a compression technique to reduce and optimize the size of the public key using a Genetic algorithm.

Nagasawa [15] used FHE with a public key without bootstrapping depending on Diffie-Hellman and discrete algorithms based on the octonion ring.

Today, there is necessary for creating a HE structure, which is feasible and practical. HE facilitates users to do computation directly on ciphertext and analysis the computational procedures done by a third party. Homomorphic property is used to convert problems from one form of the algebraic system model to another form of the algebraic system model. Then the issue is resolved in the transform algebraic system and the computational result is efficiently translated back. Hence, the cryptosystem using the homomorphic property is most popular.

II. TENSOR BASED LIGHT WEIGHT FHE SCHEMES

Here the researcher describes the proposed FHE system based on symmetric key and it optimizes the previous work using a tensor- based technique. Sub-modules of tensor based FHE are

Key generation: Here client or key distribution or generation center executes keygen () to generate a secret key that is used for result decryption and issue parameter encryption purposes.

Encryption procedure: The client can perform encryption on private data using a secret key and stores it in the cloud. Homomorphic computational are done within the cloud over encrypted data.

Decryption procedure: From the cloud, the client receives a computed result and further decrypts it with the same secret key.

Key Refresh procedure: Here, periodical refreshment of the key is done to maintain backward and forward secrecy.

Optimization procedure: Here, the best element selection is done based on a set of existing alternatives. To acquire the best value for objective function for a given domain.

III. ANALYSIS OF TENSOR BASED LIGHT WEIGHT FHE SCHEME

Analysis and observations of the proposed structure are given below:

Correct ness of Decryption step

It's noticed that, Dec procedure (D, R,K,K^T) $\Rightarrow$ $K\times D\times K^T$

The property of the or thoronol matrixes K. $K^T=K^T.K=I$ or $K^{-1}=K^T$

So Dec_ procedure (D, R, K, KT) $\Rightarrow K\times K^T$ xc $(N,a_1,a_2,a_3)\times K\times K^T$

$\Rightarrow I$ xc$(N, a_1,a_2,a_3)\times I$

$\Rightarrow$c(N, a_1, a_2, a_3)

$\Rightarrow$ [N11]

$\Rightarrow$ N

SECURITY ANALYSIS

In the 2nd procedure, N plaintext is encrypted with the K key. Suppose if the cipher text is a passive or active adversary, one can understand plain data with out knowledge of key information. In large space Z_r, the enemy will do brute force

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

attacks, so the search must be done in 2^r possibilities, an exponential procedure. During the polynomial time, determination and guessing of attack are not possible. In procedure 4, key refreshment is performed; this is done periodically based on the timestamp. So the proposed procedure is more secure to area son able extent.

Computational Complexity Improvement

In the proposed system, the procedure of Williams [9] was utilized for the computation of matrix multiplication in the encryption and decryption steps. This technique enhances the bound-on matrix multiplication exponent<*2.3727* and increases the overall speed-up of the proposed prototype.

IV. PERFORMANCE EVALUATION OF TENSOR BASED LIGHT WEIGHT FHE

Experimental Analysis of Tensor Based Light weight FHE

The proposed framework is simulated on a virtual cloud server. For implementation, a cloud server is used provided by Microsoft AZURE on Android Studio 3.0.1 SDK is also used to simulate the FHE model based on the client-cloud server. For the development of the backend interface, Judkin 9.0.1 is utilized. The machine utilized for simulation has a specification of window 10, size of RAM is 16 GB RAM, GeForce GTX 1080 GPU supported by NVIDIA on Intel i7 Octa-core machine. Received results are illustrated in table 1.

Table 1: Performance Evaluation of Tensor Based Light weight FHE

Client Data size	Key size (Bits)	Enc () (in seconds)	Upload () (in econds)	Dec () (in seconds)
500KB	16	2.1	2.1	2.5
1MB	32	2.7	2.5	2.8
2MB	32	3.1	3.3	3.3
50MB	64	6.1	6.5	6.1
200 MB	64	9.5	9.0	9.1
500 MB	128	19.1	19.3	19.1

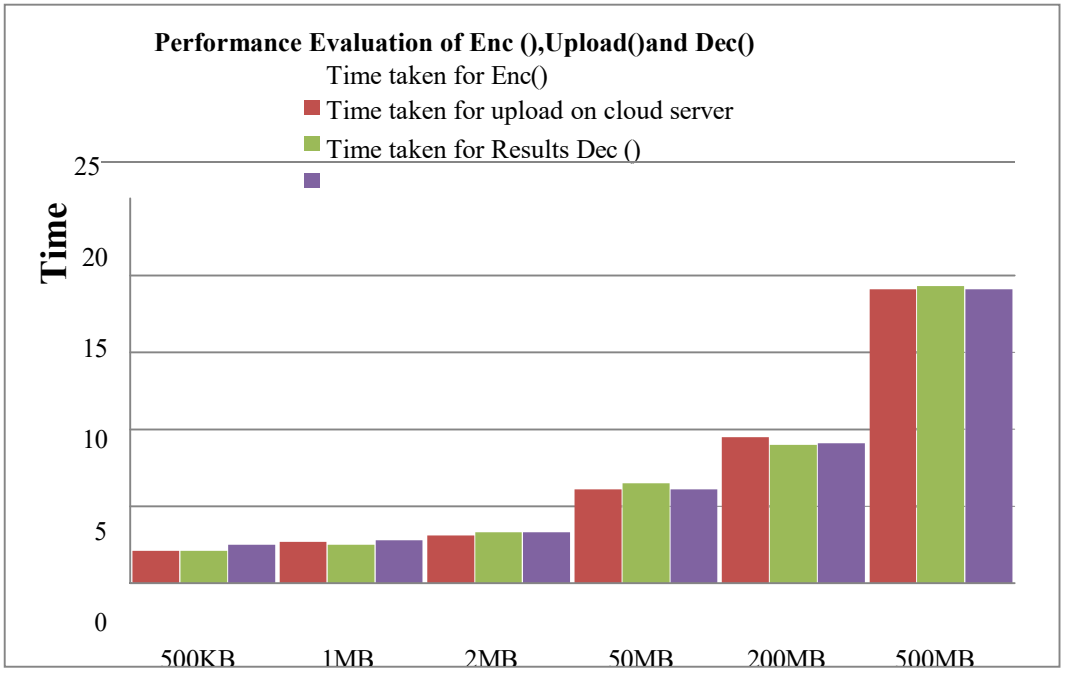

Figure 2: Performance Evaluation of Enc (), Upload () and Dec () Functions Comparative Analysis of Tensor Based Lightweight FHE

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

In table 1, the proposed framework is tested with different client's key parameter, private data size, etc. private data of the client can be of any form like a video file, pdf file, text, image, integer, etc. time taken for private data encryption, upload on a cloud server, download and decryption on the client-side is calculated. Computational operation is done on the transform parameter within the cloud. The overall execution time is illustrated in figure 2 from the experiment analysis the client data size is from 500KB to 500 MB, the encryption time for 500 MB data size is 17 seconds more than the 500 KB client data size, for decryption 500 MB data size is 17.2 seconds higher than the 500KB data size and decryption operation takes 17.6 seconds more time in when compared to 500MB with 500KB data size. Based on the analysis reveals that when data size is increased, the computational time is also increased.

In this section, the proposed structure is compared with the existing structure on various parameters. The worst-case time complexity of 2×2 matrix in the sequential procedure, the exponent complexity bound is $\simeq 3$, comparatively, acquires a lesser exponent of complexity bound which is2.3727 when adopted optimization procedure in a secure FHE cloud. Hence, gained ≅1.26 speed-up approximately. Obtained the comparatively lesser exponent of complexity bound i.e.- 2.3727Speed up (S)=tnp/tp, where tnp=time taken by non-pipeline, tp=time taken by pipeline, S=3/2.37=1.26adopted optimization procedure in secure cloud FHE. Therefore, gained approximately=1.26 as speed-up. The speed up(S) exponent is a representation is shown in figure 3. The time complexity of n×n matrix multiplication from sequential to optimized exponent is shown in table 2

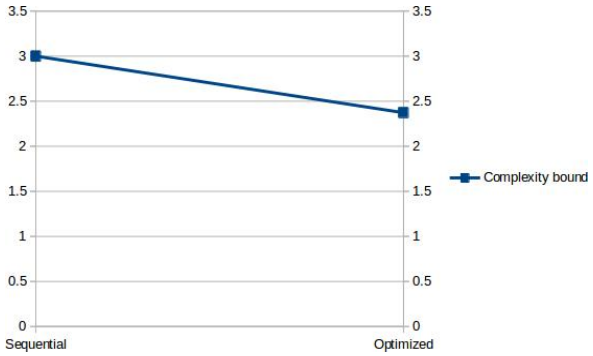

Figure 3: Optimized Time Complexation Matrix Multiplication

Table 2: Time Complexity of n×n Matrix Multiplication

Sl. No	Algorithm	Complexity
1	The run time of the divide and conquer matrix Multiplication (naive method)	$O(n^3)$
2	Strassen's algorithm (1969)	$O(n^{2.807})$
3	Coppersmith–Winograd algorithm (1990)	$O(n^{2.376})$
4	Optimized CW-like logrithms (V.V. Williams)2012	$O(n^{2.373})$

The Master Theorem: Let $a \geq 1$ and $b > 1$ be constants, let f(n) be a asymptotically positive function, and let T(n) be a function over the positive numbers defined by the recurrence $T(n) = aT(n/b) + f(n)$. If $f(n) = \Theta(nd)$, where $d \geq 0$, then

Case-1: $T(n) = \Theta(n^{\log_b a})$ if $^{\log_b a} > d$,

Case -2: $T(n) = \Theta(n^{\log_b a} \log n)$ if $^{\log_b a} = d$,

Case -3: $T(n) = \Theta(nd)$ if $^{\log_b a} < d$.

Key Generation

Key Gen (): Recurrence relation for key size is 128 bits and iterations in the homomorphic circuit are represented with 78 bits. the proposed scheme obtains less by 0.43 of the computational complexity results when compared with existing significant schemes are depicted in figure 4

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

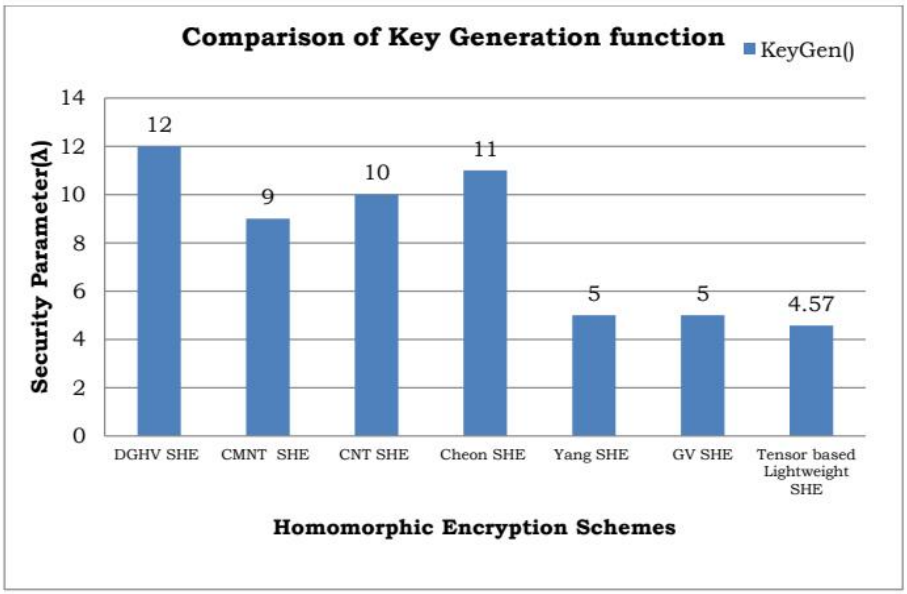

Figure 4: Comparison of Key Generation Function

Encryption

Enc(): Recurrence relation for key size is 64 bits and iterations in the Homomorphic circuit are represented with 128 bits. The recurrence relation for performing the encryption process is Compare the 4.33 with f(λ) i.e 5 satisfy case-3, then time complexity will be $T(\lambda)=O(\lambda^5)$. Figure 5 shows the performance evaluation of the encryption process of the proposed method and compared it with the significant latest methods. From the analysis, the encryption function obtains less by 1 of computational complexity with the existing schemes.

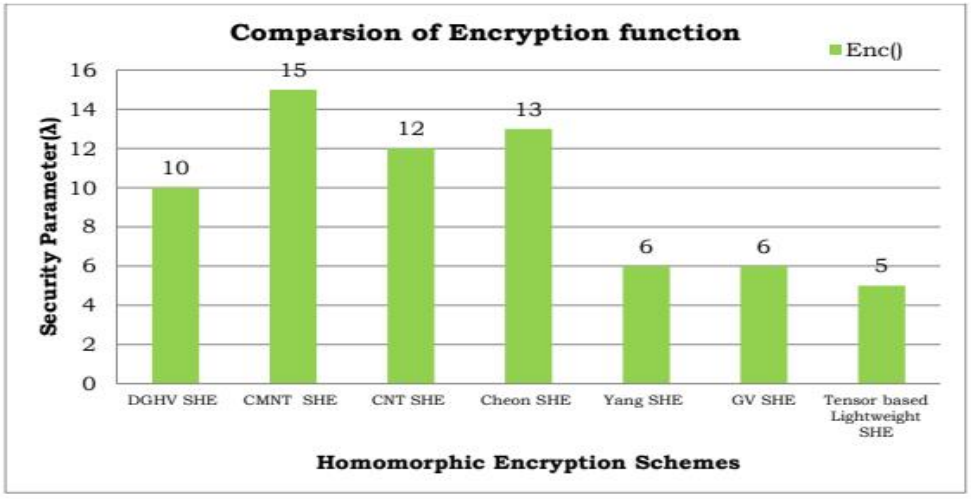

Figure 5: Comparison of the Encryption Function

Decryption

Dec (): Recurrence relation for key size is 64 bits and iterations in the homomorphic circuit are represented with 128 bits. The experiment results obtained by the decryption process and comparative analysis are depicted in figure 6 The decryption function reduces the security parameter by 0.17 when compared with the existing scheme.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

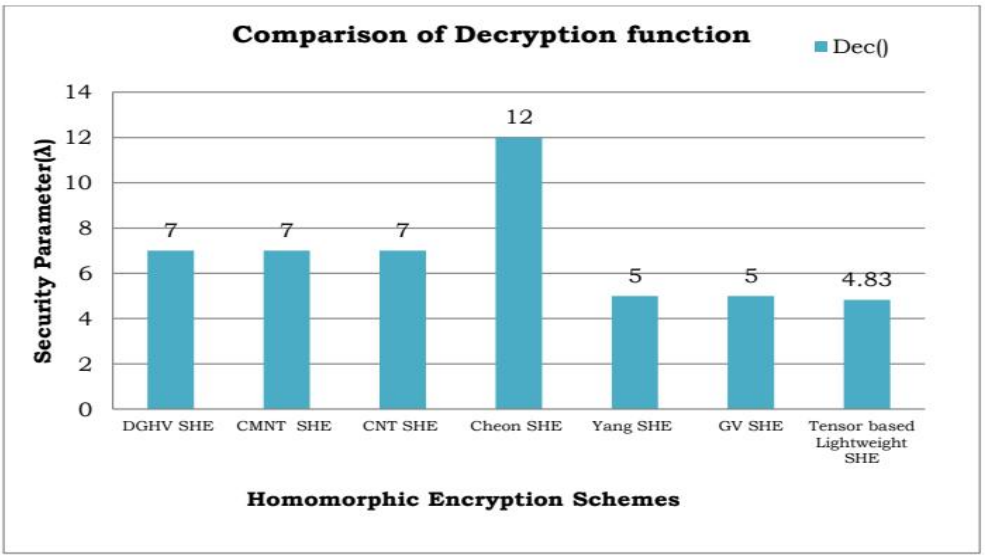

Figure 6: Comparison of the Decryption Function

Massage Expansion

Recurrence relation for evaluation of time complexity of message expansion is represented Figure 7 depicts the results obtained by the proposed scheme and shown a similar performance with the existing schemes.

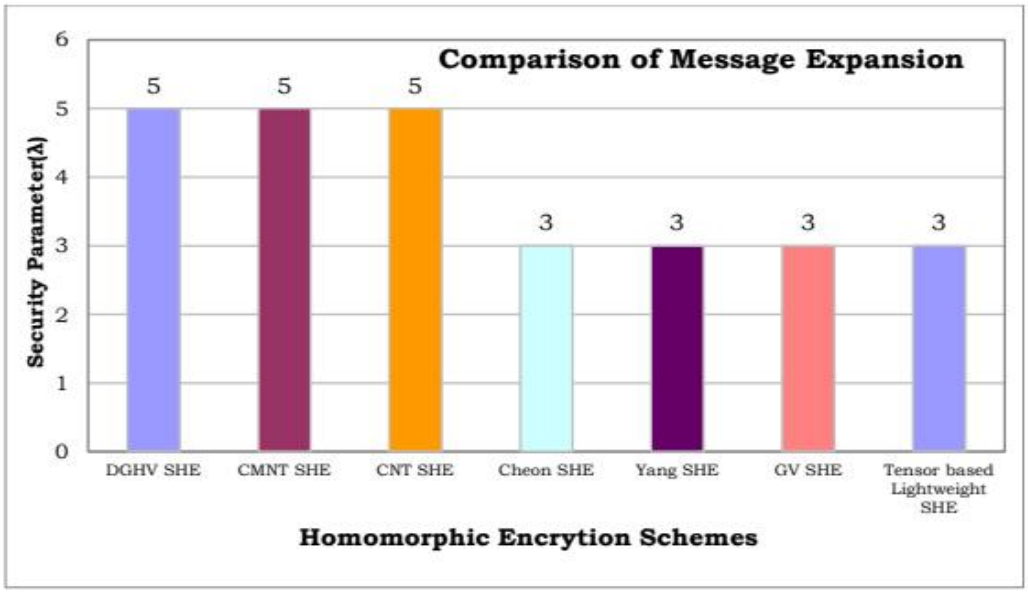

Figure 7: Comparison of Message Expansion Function

Homomorphic Additive Function

The result obtained by the homomorphic addition property applied to the proposed scheme and performance of the additive property is 0.47 less than the recent existing significant method are represented in figure 8

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

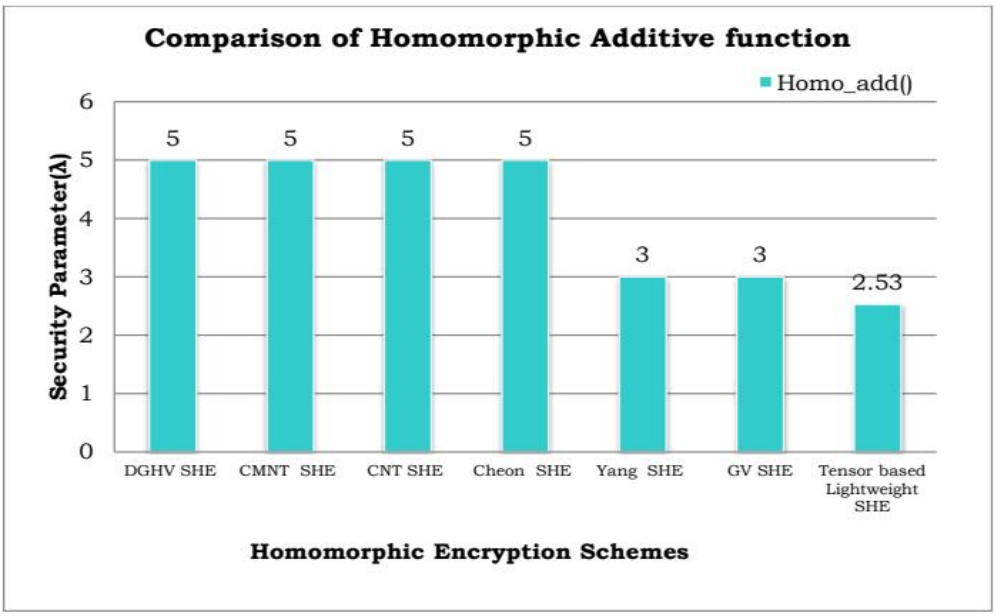

Figure 8: Comparison of Homomorphic Additive Function

Homomorphic Multiplicative Function

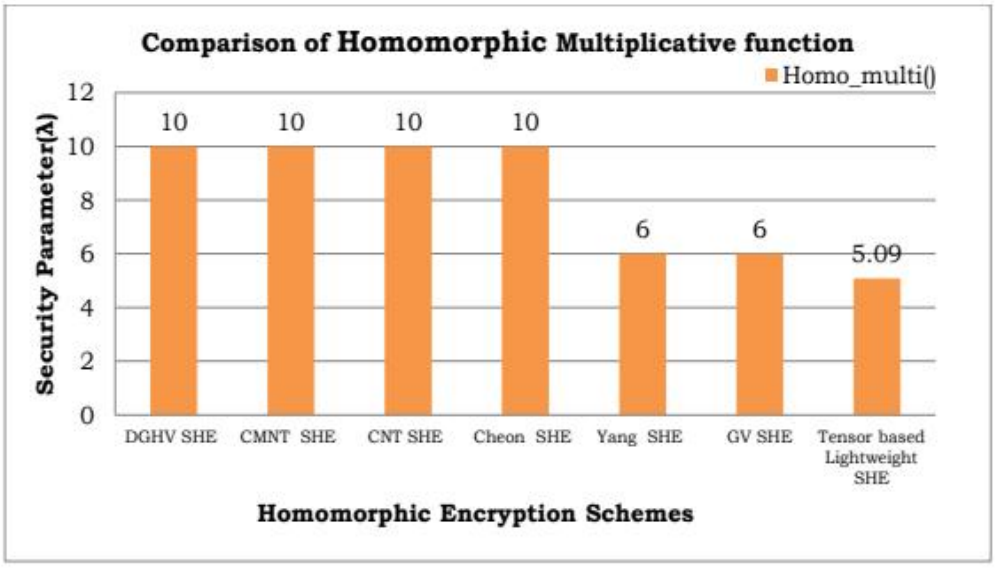

Figure 4.9: Comparison of Homomorphic Multiplicative Function

performance evaluation of the multiplication homomorphic encryption scheme of proposed work with existing schemes is taken less by 0.91 of the security parameter (λ) as shown in figure 9. The overall comparative summary of tensor scheme is shown table 3

Table 3: Comparative Summary

Comparison factor	Dijkstra.[3]	Coronet al. [4]	Coronet al. [7]	Cheo net al. [16]	Yang et al. [8]	Ramaiah Tal.[5]	Proposed
Scheme Name/ Time complexity	DGHV FHE scheme	CMNT FHE scheme	CNT FHE	Batch FHE	Anew SHE scheme	GV scheme	Tensor based lightweight the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

Size (Pub key)	$O(\lambda^{10})$	$O(\lambda^{7})$	$O(\lambda^{5})$	$O(\lambda^{7})$	$O(\lambda^{3})$	$O(\lambda^{3})$	-
key Generation	$O(\lambda^{12})$	$O(\lambda^{9})$	$O(\lambda^{10})$	$O(\lambda^{11})$	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{4.5})$
Encryption	$O(\lambda^{10})$	$O(\lambda^{15})$	$O(\lambda^{12})$	$O(\lambda^{13})$	$O(\lambda^{6})$	$O(\lambda^{6})$	$O(\lambda^{5})$
Decryption	$O(\lambda^{7})$	$O(\lambda^{7})$	$O(\lambda^{7})$	$O(\lambda^{12})$	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{4.8})$
Message Expansion	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{3})$	$O(\lambda^{3})$	$O(\lambda^{3})$	$O(\lambda^{3})$
Homomorphic addition	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{5})$	$O(\lambda^{3})$	$O(\lambda^{3})$	$O(\lambda^{2.5})$
Homomorphic multiplication	$O(\lambda^{10})$	$O(\lambda^{10})$	$O(\lambda^{10})$	$O(\lambda^{10})$	$O(\lambda^{6})$	$O(\lambda^{6})$	$O(\lambda^{5})$

V. CONCLUSION

The symmetric key based lightweight FHE algorithm with the steps of key generation, encryption procedure, decryption procedure, key refreshing procedure and uses tensor-based optimization to reduce the computational cost. Then the proposed method is validated by reduced time complexity in terms of key generation, encryption, evaluation, and decryption steps. Finally, the proposed method of efficient performance measures is proved with security analysis.

REFERENCES

[1]. C. Gentry, "Fully homomorphic encryption using ideal lattices" in Proceedings of the forty-first annual ACM symposium on Theory of Computing, pp.169-178, 2009.

[2]. N. P. Smart and F. Veratrin, "Fully homomorphic encryption with relatively small key and ciphertext sizes" in International Workshop on Public Key Cryptography, Springer pp. 420-443, 2010.

[3]. M. Van Dijk, C. Gentry, S. Halevi, and V. Vicentine than, "Fully homomorphic encryption over the integers" in Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 24-43, 2010.

[4]. J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully homomorphic encryption over the integers with shorter public keys" in Annual Cryptology Conference, pp. 487-504,2011.

[5]. Y. G. Ramaiah and G. V. Kumari "Efficient public key homomorphic encryption over integer plaintexts" in International Conference on Information Security and Intelligent Control, pp. 123-128,2012.

[6]. L. Xiao, O. Bastani, and I.-L. Yen, "An Efficient Homomorphic Encryption Protocol for Multi-User Systems" The International Association for Cryptologic Research Cryptology, pp. 193-209, 2012.

[7]. J.-S. Coron, D. Naccache, and M. Tibouchi, "Public key compression and modulus switching for fully homomorphic encryption over the integers" in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 446-464,2012.

[8]. H. Yang, Q. Xia, X. Wang and D. Tang, "A New Somewhat Homomorphic Encryption Scheme over Integers" IEEE International Conference on Computer Distributed Control and Intelligent Environmental Monitoring, pp. 61-64, 2012.

[9]. V. Vassilevska Williams, "Multiplying matrices faster than Coppersmith Winograd" in proceedings of ACM Symposium Theory Computation (STOC), pp. 887-898, 2012.

[10]. M. Liang, "Symmetric quantum fully homomorphic encryption with perfect security" Quantum information processing, vol. 12, no.12, pp. 3675-3687, 2013.

[11]. . Chen, J. Wang, hang, and X. Song, "A fully homomorphic encryption scheme with better key size" China Communications, vol. 11, pp. 82-92, 2014.

[12]. S. Hemalatha and D. R. Manickachezian, "Performance of ring- based fully homomorphic encryption for securing data in cloud computing" International Journal of Advanced Research in Computer and Communication Engineering, vol.3, no.11, pp. 8496-8500, 2014.

[13]. Sharma, "A symmetric FHE scheme based on Linear Algebra" International Journal of Computer Science & Engineering Technology, vol. 5, no.5, pp. 558-562, 2014.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

[14]. J. Gavinho Filho, G. P. Silva, and C. Miceli, "A public key compression method for Fully Homomorphic Encryption using Genetic Algorithms" 1th International Conference on Information Fusion (FUSION), pp. 1991-1998, 2016.

[15]. M. Yagisawa, "Fully Homomorphic Public-key Encryption Based on Discrete Logarithm Problem" International Association for Cryptologic Research Cryptology, pp. 54, 2016.

[16]. M. Tebaa and S. E. Hajji, "Secure cloud computing through homomorphic encryption" International Journal of Advancements in Computing Technology, vol.5, no.16, 2013