A Hybrid Improved Zhou and Wornell's Inspired Fully Homomorphic Encryption Scheme for Securing Big Data Computation in Cloud Environment

Nithiavathy R (✉ nithiavathy.r@skct.edu.in)

Sri Krishna College of Technology <https://orcid.org/0000-0002-0988-0177>

Vanitha K

Madanapalle Institute of Technology and Science

Manimaran A

Madanapalle Institute of Technology and Science

Ilampiray P

Sri Krishna College of Technology

Alaguvathana P

Sri Krishna College of Technology

Research Article

Keywords: Big data, Cloud environment, Encryption

Posted Date: April 16th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-356001/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

A Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption Scheme for Securing Big Data Computation in Cloud Environment

AUTHOR 1 & CORRESPONDING AUTHOR:

Dr. R.Nithiavathy
Assistant Professor,
Department of Computer Science & Engineering,
Sri Krishna College of Technology, Kovaipudur, Coimbatore, Tamilnadu, India
nithiavathy.r@skct.edu.in
Mobile: 8220537319

AUTHOR 2:

Dr. K.Vanitha
Assistant Professor,
Department of Computer Science & Engineering,
Madanapalle Institute of Technology & Science,
kvanithacse@gmail.com
Mobile: 8940087949

AUTHOR 3:

Dr.A.Manimaran
Assistant Professor
Computer Applications,
Madanapalle Institute of Technology & Science,
drmanimaranca@gmail.com
Mobile: 9940956729

AUTHOR 4:

P.Ilampiray,
Assistant Professor,
Department of Information Technology,
Sri Krishna College of Technology, Kovaipudur, Coimbatore, Tamilnadu, India
ilampiray.p@skct.edu.in
Mobile: 8778712186

AUTHOR 5:

P.Alaguvathana
Assistant Professor,
Department of Information Technology,
Sri Krishna College of Technology, Kovaipudur, Coimbatore, Tamilnadu, India
alaguvathana.p@skct.edu.in
Mobile: 9626343506

A Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption Scheme for Securing Big Data Computation in Cloud Environment

R.Nithiavathy^{1*}, K.Vanitha², A.Manimaran³, P.Ilampiray⁴, P.Alaguvathana⁵

¹Assistant Professor, Department of Computer Science & Engineering,
Sri Krishna College of Technology, Coimbatore, Tamilnadu, India
nithiavathy.r@skct.edu.in

²Assistant Professor, Department of Computer Science & Engineering,
Department of Computer Science & Engineering,
Madanapalle institute of technology & science,
kvanithacse@gmail.com

³Assistant Professor, Department of Computer Science & Engineering,
Madanapalle institute of technology & science,
drmanimaranca@gmail.com

⁴ Assistant Professor, Department of Information Technology,
Sri Krishna College of Technology, Coimbatore, Tamilnadu, India
ilampiray.p@skct.edu.in

⁵Assistant Professor, Department of Information Technology,
Sri Krishna College of Technology, Coimbatore, Tamilnadu, India
alaguvathana.p@skct.edu.in

Abstract: The process of performing smart computations in the big data and cloud computing environment is considered to be highly essential in spite of its complexity and cost. The method of Fully Homomorphic encryption is considered to be the effective approach that provides the option of working with the encrypted form of sensitive data in order to preserve high confidentiality that concentrates on deriving benefits from cloud computing capabilities. In this paper, a Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption (HIZWFHE) Scheme is proposed for securing big data computation, when they are outsourced to cloud service. This HIZWFHE scheme is potent in encrypting integer vectors that permit the computation of big data represented in the contextual polynomial form in the encrypted form with a bounded degree of limits. This HIZWFHE scheme is determined to be highly applicable and suitable and applicable in cloud big data computation in which the learning process of low dimensional representations is of high concern.

Keywords: Big data, Cloud environment, Encryption

1. Introduction

The cloud computing is considered as a successful computing model with a considerable number of merits facilitated to the providers and clients [1]. This cloud computing possesses a dramatic advantage of delegating the complex big data computations by deriving the benefits of optimal technologies that provides maximum computation power under lowest expensive [2]. This cost merits facilitated by the cloud computing is determined as the major statements that provides the justification behind the utilization of it in a diversified number of industries [3]. However, the emergence of security issues under the process of managing the computation of data is considered as the major challenge [4]. In the recent decade, a number of research works were contributed to secure the data stored in the cloud [6-7]. However, the fully homomorphic encryption schemes are considered to be vital in ensuring maximum security without the knowledge of data and computation function [8]. Most of the fully homomorphic encryption schemes are considered are affected by a vulnerability in the secret key [9]. Further, the noise free-based fully homomorphic encryption schemes are considered to be highly suitable and applicable to superior cloud data computation with reduced time [10].

In this paper, a Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption (HIZWFHE) Scheme is proposed for facilitating superior security under big data computation. This proposed HIZWFHE scheme is also potent in encrypting integer vectors that permit the computation of big data that are represented in the bit vector form with the threshold degree of limits. The secrecy degree of the proposed HIZWFHE scheme is investigated for identifying its potential in securing big data computations in the cloud environment. The experimental investigations of the proposed HIZWFHE scheme was also conducted using time incurred in single operations (seconds), the time incurred per operations for a single bit of encrypted data (seconds), percentage increase in data retrieval, percentage increase in response time, percentage increase in Unmask performance time and percentage decrease in the memory consumption rate under a varying number of dimensions.

2 Related Work

In this section, the most recent approaches of the fully homomorphic encryption schemes are presented with the merits and limitations

Initially, Kim et al. [11] has presented hybrid data mining based approach for identifying DDoS attacks and to mitigate it by various means. This method comprises of two different modules automated selection module and classification module. The hybridization of data mining capability is due to crucial data flow in the DDoS attack detection. The gathering and utilization of the data flow is performed based on the Netflow. Scherrer et al. [12] in 2014 recommended a method in order to extract features of the DDoS attack and based on the features how the detection and mitigation of DDoS. This Polly Cracker-based FHE is integrated with the merits of Polly Cracker for attaining superior performance in computation with a reduction in time. This Polly Cracker-based FHE is determined to secret in nature. But, the memory consumptions of this Polly Cracker-based FHE is comparatively low compared to the Gentrys' Scheme proposed for Homomorphic encryption. Further, Lee et al.[13] in 2008 implemented a method which acts as aproactive measure for DDoS attacks. This proactive protocol has been proposed based on the distributed architecture and also based on selecting various variable related to the attack occurring features. Cluster based mechanism has been presented for mitigating DDoS attacks. Nguyen and Choi [14] in 2016 have presented a method which aids in identification of DDoS attacks based on the network conditional parameters. With reference to the key features the key variable are chosen and based on the k -nearest neighbor method the network conditions and performance are classified. The unmask performance time of this Non-Deterministic FHE scheme was determined to be maximum to a degree of 93% with reduced overhead in computations.

Tsai and Lin [15] introduced a method for mitigating DDoS which is referred as Triangle Area Based Nearest Approach. The accuracy of this approach is evaluated based on the false negative and false positive rate. Bhange et al.[16] illustrated a novel methodology to mitigate DDoS attack and its influence in the network performance. The distributed network traffic is analyzed based on the parameters of the network. This analysis is performed in order to identify the difference in the anomaly traffic and normal traffic. Tan et al. in 2014 [17] recommended more comfortable and efficient approach for detecting and isolation of DDoS attack in the networking

environment. This novel detection scheme is based on the MCA in order to protect from DDoS attacks. This modified Gentry's scheme utilized 0.47 seconds of computation time for the user and 0.1 seconds for the server. But, the memory consumption rate of this modified Gentry's scheme is only half, leaving the remaining memory cycles idle during the process of data computations in the clouds.

Luo et al. [18] has developed a mathematical model based estimation for the mitigation of DDoS attacks for the networking environment. This method results in an efficient and effective way of detecting and mitigating DDoS attacks. This Ghostshell-based FHE is effective in the process of SIMD operations exploitation with a single time chosen MAC identifier. This Ghostshell-based FHE incorporated the multiplication depth of 2 with the benefits of Hamming distance that supports 2400 bit of data. The unmask performance time, memory consumptions of this RN-FHE was also estimated to be 23% lower than the DORACS-FHE scheme. In addition, a FHE that focuses on the provision of security against Adaptive Chosen Ciphertext Attack (CCA) was proposed for handling the issues that are the most common in cloud storage, cloud computation, electronic voting and multi-party computation [19]. This FHE scheme included the property of residual classes by imposing the composite degree of modular arithmetic with determined superior security. This proposed DORACS-FHE improves the unmask performance time, memory consumptions and time consumptions with increased scalability of data used for computations. However, the data retrieval rate is determined is comparatively 19% lower than the existing approaches of the literature.

3 Proposed Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption (HIZWFHE) Scheme

The Hybrid Improved Zhou and Wornell's inspired Fully Homomorphic Encryption (HIZWFHE) Scheme for facilitating efficient security over the big data computations is proposed for permitting the possible computations over the encrypted data. This HIZWFHE Scheme aids in sustaining the function secrecy in big data computations of cloud environment by encrypting the data and the computation function, which enables the cloud to compute the function without the knowledge of data and computation function. This method of computing the function without the knowledge of data and computation function is contradictory to the existing Gentry-based

Homomorphic Encryption schemes. The Gentry-based Homomorphic Encryption schemes always necessitate the computation function to be made available in the unencrypted form over the clouds, since the computing requirements need to be transformed into a circuit.

Initially, this proposed HIZWFHE Scheme computes a ciphertext vector $C_V \in Z^n$ from the plaintext vector and a secret key $(P_{V(x)} \in Z^m, S_{K(x)} \in Z^{m \times n})$ by satisfying the condition presented in Equation (1)

$$S_{K(x)} * C_V = wP_{V(x)} + e \quad (1)$$

Where e and w represents the error term and a large integer that possess elements that are smaller than $\frac{w}{2}$.

In this proposed HIZWFHE Scheme, the size of the secret key is considered to be very small compared to the utilized large integer $(S_{K(x)} \in Z^{m \times n}) \ll w$. This consideration is determined to be vital in maintaining the error terms as small as possible in order to apply possible operations in the encrypted field. The decryption of the ciphertext vector is determined in a straightforward manner with the knowledge of the secret key $S_{K(x)} \in Z^{m \times n}$ based on Equation (2)

$$P_{V(x)} = \text{Ceil}\left(\frac{S_{V(x)}}{w}\right) \quad (2)$$

Further, the vital concept that is used for performing the most significant operations in the encrypted field is the key switching mechanism. The process of key switching process aid in choosing a new secret key $S^C_{K(x)} \in Z^{m \times n}$ and its associated ciphertext $C^C_V \in Z^n$ with the knowledge of $S_{K(x)} \in Z^{m \times n}$ and $C_V \in Z^n$ respectively. This process of key switching aids in generating the ciphertext of the form represented in Equation (3)

$$wJP_{V(x)} = wP_{V(x)} \quad (3)$$

In this context, wJ is the secret key and plain text $P_{V(x)} \in Z^m$ with the zero error term. Then, the process of key switching is employed on wJ to determine the new secret key $S^C_{K(x)} \in Z^{m \times n}$ and its associated ciphertext $C^C_v \in Z^n$.

3.2 Key switching mechanisms of the proposed HIZWFHE Scheme

In this key switching process, the original secret key and ciphertext pairs are transformed into a modified secret key and ciphertext pairs with the initially considered secret key still used for the process of encrypting the original plaintext [19]. This process of key switching is efficient for simplifying the implementation and investigation of the operations that are feasible in the cloud environment. Suppose, the plaintext $P_{V(x)} \in Z^m$ is now encrypted into a ciphertext $C_v \in Z^n$ with the secret key $S_{K(x)} \in Z^{m \times n}$, then the new ciphertext $C^C_v \in Z^n$ is determined using the modified secret key $S^C_{K(x)} \in Z^{m \times n}$ based on Equation (4).

$$S^C_{K(x)} * C^c_{V(x)} = S_{K(x)} * C_{V(x)} \quad (4)$$

This process of key switching is partitioned into two steps which converts the original ciphertext and secret key into an intermediate form in the first step. Further, the switching process of bit representation is facilitated for determined the required secret key in the second key. Furthermore, the magnitude of $|C^*_{V(x)}| := \text{Maximum}\{|C_{V(x)}|\}$ is assigned to the value of 1, through the enforcement of bit representation. This assignment in the magnitude of the new ciphertext eliminates the issue of increasing values of the error term e^c in order to preserve the correctness of the degree.

Step 1: Select a value r such that $|C_{V(x)}| < 2^r$. Then, the original cipher text $C_V \in Z^n$ can be represented in its bit form $b_{R(i)} = [b_{R(i)(r-1)}, \dots, b_{R(i)(1)}, b_{R(i)(0)}]^T$ with the condition $b_{R(i)(k)} \in \{-1, 0, 1\}$ derived based on Equation (5)

$$C_{V(x)}^* = [b_{R(1)}^T, b_{R(2)}^T, \dots, b_{R(n)}^T] \quad (5)$$

Further, a matrix representing $S_{K(x)}^* \in Z^{mxn}$ is constructed by modifying each element of $S_{K(x)} \in Z^{mxn}$ derived from the original secret key, which is represented in a vector highlighted in Equation (6)

$$A_{ij} = [2^{r-1} S_{V(x-ij)}, \dots, 2 S_{V(x-ij)}, S_{V(x-ij)}] \quad (6)$$

For instance, if the vector $C_{V(x)} - [1, -3]$ is represented as $C_{V(x)}^* = [0, 0, 1, 0, -1, -1]$ under $r = 3$. Then,

the value of $S_{K(x)}^* \in Z^{mxn}$ can be computed based on a secret key $\begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix}$ as $S_{V(x)}^* = \begin{bmatrix} 4 & 2 & 1 & 8 & 4 & 2 \\ 20 & 10 & 5 & 16 & 8 & 4 \end{bmatrix}$

by preserving the condition $S_{K(x)}^C * C_{V(x)}^c = S_{K(x)} * C_{V(x)}$.

Step 2: In this step, the process of converting the bit representation of the original $S_{K(x)} \in Z^{mxn}$ is transformed into a new secret key-cipher text pair. Then, a new key switch matrix pair is constructed by satisfying the condition specified in Equation (7)

$$S_{V(x)}^c * K_{SM} = S_{V(x)}^* + E \quad (7)$$

3.3 Weighted inner products of the proposed HIZWFHE Scheme

In this step, the process of weighted inner product is determined by considering this operation as the product of matrix-vector. If $V(M)$ be the vector form of the matrix M , then the

columns of matrix M is concatenated with the matrix that posses that same order of the matrix M by using Equation (8)

$$P_{V(x)}^T = V(M)^T * V(P_{V(x)} * P_{V(x)}^T) \quad (8)$$

This process of weighted inner product aids in improving the dimensions of the ciphertext from order n to order n^2 . However, the dimensions are brought down to a manageable level by the utilization of the key switching process used before this step.

3.4 Polynomial generations of the proposed HIZWFHE Scheme

Finally, the arbitrary polynomials can be produced after the incorporation of three primitive operations that corresponds to addition, linear transformation and weighted inner product. The weighted inner product operation [20] is considered as the key component during the process of synthesizing polynomials in order to employ a slight enhancement for inheriting its inhomogeneous degree. In this context, the plaintext vector $P_{V(x)} = [P_{V(1)}, P_{V(2)}, \dots, P_{V(n)}]^T$ can be extended to a modified plaintext vector $P_{V(x)}^c = [1, P_{V(1)}, P_{V(2)}, \dots, P_{V(n)}]^T$ derived based on Equation (9)

$$C_{V(x)}^c = [w, C_{V(x)}^T]^T \quad (9)$$

Under the secret key $S_{K(x)}^c = \begin{bmatrix} 1 & 0 \\ 0 & S_{K(x)} \end{bmatrix}.$

Then, the method of the inner product is applied for calculating the polynomial of degree 2 based on Equation (10)

$$POLY_{DEG}^{ENCR} = (P_{V(x)}^C)^T * G * (P_{V(x)}^c) \quad (10)$$

Where G is the appropriately chosen for working with the maximum lowest enhancement in the existing data. For instance, the second order polynomial $f(P_{V(x)}) = x_2^2 + 4x_1x_1 - 3x_1 + x_2 + 4$ can be represented as the weighted inner product of $POLY_{DEG}^{ENCR} = (P_{V(x)}^C)^T * G * (P_{V(x)}^c)$ for

$$H = \begin{bmatrix} 4 & -3 & 1 \\ 0 & 0 & 4 \\ 0 & 0 & 1 \end{bmatrix}$$

estimating the value of $P_{V(x)}^c = [1, x_1, x_2]$ and $P_{V(x)}^C = [1, x_1, x_2]$. In addition, the polynomial of order b can be calculated by the cloud by parallelizing its operations over n variables by considering the complexity of $O(\log b * n^3)$. Moreover, the core overhead in the proposed HIZWFHE Scheme is mainly derived from the computation of key switch matrices on the client side for every individual inner product that are proportional to the polynomial degree. Further, the key switch matrices for each secret key need to be calculated systematically in the proposed HIZWFHE Scheme, such that the cloud possesses the significant in operating with the similar kind of matrices over different vectors. Hence, the overhead incurred on the client side is tolerable, if similar type of polynomials is estimated over diversified values. Furthermore, the employment of weighted inner product operations introduces a great increase in the error term, which need to

possess magnitude of order less than $\frac{w}{2}$ in order to achieve the process of successful decryption. This proposed HIZWFHE Scheme prevents the enforcement of diversified operations on the big data stored over the cloud, since they do not incorporate an error resetting operation during the process of fully homomorphic encryption scheme. Hence, it is evident that the proposed HIZWFHE Scheme is capable of composing arbitrary polynomials only through the defined operations of addition, linear transformation and weighted inner product. In addition, the value of w is considered to be sufficiently large depending on the employed weighted inner product operation counts used for the enforcement of the proposed HIZWFHE Scheme.

4 Secrecy Investigation of the proposed HIZWFHE Scheme.

In this section, secrecy inherent to the estimation of computation function of the cloud data (the function which is sent to the clouds by the collaborating clients) is investigated, since it is considered as the indispensable characteristics of the homomorphic encryption approach. In this context, the enforcement of encryption over the computation function ‘ $\mathcal{G}$ ’ is represented as a key switch matrix K_{SM} . This key switch matrix K_{SM} is considered as the data, which is sent to the cloud by the interacting clients. At this juncture, the matrix K_{SM} must be capable enough for hiding any significant information associated weighed inner product coefficient or the linear transformation coefficient. Hence, the secrecy of the proposed HIZWFHE Scheme depends on the potential in handling the issue of Learning with errors. This proposed HIZWFHE Scheme is considered to more secret and hard, if it is possible to estimate the equation $S_{V(x)}^c * K_{SM} = S_{V(x)}^* + E$ under $K_{SM} \in Z^{n_c \times nr}$ with the knowledge of K_{SM} and $S_{V(x)}^*$ respectively.

If suppose, the elements in the matrices are considered from the set of value Z , then the elements of Z_p for some prime number $p \gg \max\{|S_{K(x)}^c|, |K_{SM}|, |S_{K(x)}^*|, |E|\}$ can be defined. Thus the consideration of special case under the condition $S_{V(x)}^c = (s_{V(x)}^c)^T$ is a n-dimensional row vector with $E = e$ and $S_{V(x)}^c = S_{V(x)}^*$. Thus, the equation $S_{V(x)}^c * K_{SM} = S_{V(x)}^* + E$ can be translated into Equation (11)

$$(s_{V(x)}^*)^T * k_{sm(i)} = s_{V(x)}^* + e \quad (11)$$

Hence, it is accessible to ‘n’ samples of $(k_{sm(i)}, s_{V(x)}^*)$ in the modified secret key derived through Equation (12)

$$s_{V(x)}^* = ((s_{V(x)}^C)^T * k_{sm(i)}) - e_{(i)} \quad (12)$$

Thus, the issue of Learning with errors is made hard since solving Equations (11) and (12) are equivalently hard. It is highly difficult to recover the new secret key $s_{V(x)}^*$ based on the estimated key switch matrix K_{SM} . Hence, the malicious adversaries that intercept the communication with the cloud and the cloud itself cannot recover the secret key, plaintext, G and H corresponding to the weighted inner products and linear transformation processes. Therefore, the proposed HIZWFHE Scheme is determined to be highly secret.

5 Experimental Results and Discussion

In this section, the proposed HIZWFHE Scheme is investigated with the existing GENTRY-FHE [20], SMART-VEC [19] and BATCH-DGHV[18] fully homomorphic encryption schemes considered for facilitating superior security in big data computations in the clouds. The performance of the proposed HIZWFHE Scheme is compared with the benchmarked schemes by the enforcement of $n \times n$ linear transformation process that gets converted into a n -dimensional vector. In this investigation process, a single key switch matrix is employed to all the ciphertext vectors. Hence, this investigation of the proposed HIZWFHE Scheme considers an equivalent time, which is required for generating key switch matrix using linear transformation and employing it to 50 numbers of ciphertext vectors. Hence, the initial overhead over the 50 numbers of ciphertext vector operations are considered to determine the predominance of the proposed HIZWFHE Scheme is investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV.

In the first fold of investigation of the proposed HIZWFHE Scheme is investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using time incurred in single operations(seconds) by varying the number of dimensions. Figure 1 and 2 highlights the predominance of the proposed HIZWFHE Scheme investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using time incurred in single operations (seconds) by varying

the number of dimensions. The time incurred per operations under a varying number of dimensions with encrypted data of the proposed HIZWFHE Scheme was determined to be 12%, 16% and 18% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches. Likewise, the time incurred per operations under a varying number of dimensions with unencrypted data of the proposed HIZWFHE Scheme was determined to be 11%, 14% and 16% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches.

Figure 1: Performance of the proposed HIZWFHE Scheme under linear transformation of encrypted data

Figure 2: Performance of the proposed HIZWFHE Scheme under linear transformation of encrypted data

In the second fold of investigation of the proposed HIZWFHE Scheme is investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using time incurred per operations for a single bit of encrypted data (seconds) by varying the number of dimensions. Figure 3 and 4 exemplars the predominance of the proposed HIZWFHE Scheme investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using time incurred per operations per single bit of encrypted data (seconds) by varying the number of dimensions. The time incurred per operations per single bit of encrypted data under a varying number of dimensions with encrypted data of the proposed HIZWFHE Scheme was determined to be reduced by 14%, 19% and 21% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches. Likewise, the time incurred per operations for a single bit of encrypted data (seconds) under a varying number of dimensions with unencrypted data of the proposed HIZWFHE Scheme was determined to be greatly minimized by 13%, 15% and 18% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches.

Figure 3: Performance of the proposed HIZWFHE Scheme under time incurred per operations per single bit of encrypted data

Figure 4: Performance of the proposed HIZWFHE Scheme under time incurred per operations per single bit of unencrypted data

In the third fold of investigation of the proposed HIZWFHE Scheme is investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using the percentage increase in data retrieval, percentage increase in response time, percentage increase in Unmask performance time and percentage decrease in memory consumption rate by varying the number of dimensions. Figure 5 and 6 depicts the performance of the proposed HIZWFHE Scheme investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using data retrieval and Query time by varying the number of dimensions. The percentage increase in data retrieval of the proposed HIZWFHE Scheme under varying number of dimensions was determined to be enhanced by 8%, 10% and 13% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches. Likewise, the response time of the proposed HIZWFHE Scheme under a varying number of dimensions is confirmed to be highly improved by 10%, 13% and 15% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches.

Figure 5: Performance of the proposed HIZWFHE Scheme- percentage increase in data retrieval

Figure 6: Performance of the proposed HIZWFHE Scheme- percentage increase in response time

Figure 7: Performance of the proposed HIZWFHE Scheme- percentage increase in Unmask performance time

Figure 8: Performance of the proposed HIZWFHE Scheme- percentage decrease in memory consumption rate

Finally, Figure 7 and 8 depict the performance of the proposed HIZWFHE Scheme investigated with the existing GENTRY-FHE, SMART-VEC and BATCH-DGHV using the percentage increase at the Unmask performance time and percentage decrease in the memory consumption rate by varying the number of dimensions. The percentage increase in Unmask performance time of the proposed HIZWFHE Scheme under varying number of dimensions was determined to be enhanced by 10%, 13% and 16% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches. Similarly, the percentage decrease in the memory consumption rate of the proposed HIZWFHE Scheme under a varying number of dimensions is confirmed to be highly minimized by 11%, 14% and 17% superior to the baseline GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches considered for investigation.

6. Conclusion

This paper has portrayed the significance of the proposed HIZWFHE Scheme as a successful fully homomorphic encryption that is suitable for facilitating maximum secrecy in the big data computations of the cloud storage. The proposed HIZWFHE Scheme was determined to potent in handling the issue of learning with errors, which leads to maximum secrecy degree under big data computations. The proposed HIZWFHE Scheme used the merits of key switching process, linear transformation operation and polynomial generation for securing the data storage in clouds without the knowledge of the data and computation function used by the cloud. The simulation results of the proposed HIZWFHE Scheme evaluated under time incurred in single operations(seconds) by varying the number of dimensions is determined to be minimized on an average by 15% and 17% compared to the GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches considered for investigation. The proposed HIZWFHE Scheme evaluated under time incurred per operations for a single bit of encrypted data (seconds) by varying the number of dimensions is proving to be highly minimized on an average by 13% and 15% compared to the GENTRY-FHE, SMART-VEC and BATCH-DGHV approaches. As a plan of future work., it is decided to propose a Octonion algebra inspired Fully Homomorphic Encryption Scheme for securing big data computation on the cloud storage.

Funding This research work has not received any funding from any organization.

Data Availability Statement The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declaration

Conflicts of interest The authors declare that there is no conflict of interest.

References

1. Yi, X., Paulet, R., & Bertino, E. (2014). Fully Homomorphic Encryption. *Homomorphic Encryption and Applications*, 1(1), 47-66.
2. Zhou, H., & Wornell, G. (2014). Efficient homomorphic encryption on integer vectors and its applications. *2014 Information Theory and Applications Workshop (ITA)*, 1(2), 67-73.

3. Goyal, V., Movva, R., & Kunadharaju, A. (2017). A Secure Cloud Computing based Framework for Big Data Information management of smart Grids. *IJARCCCE*, 6(6), 47-52.
4. Zhang, Z., Plantard, T., & Susilo, W. (2012). Reaction Attack on Outsourced Computing with Fully Homomorphic Encryption Schemes. *Information Security and Cryptology - ICISC 2011*, 1(2), 419-436.
5. Ramaiah, Y. G., & Kumari, G. V. (2012). Efficient public key Homomorphic Encryption over integer plaintexts. *2012 International Conference on Information Security and Intelligent Control*, 1(1), 34-45.
6. Yang, H., Xia, Q., Wang, X., & Tang, D. (2012). A New Somewhat Homomorphic Encryption Scheme over Integers. *2012 International Conference on Computer Distributed Control and Intelligent Environmental Monitoring*, 2(1), 45-56.
7. Yong, D., Zheng, W., & Xinguo, L. (2013). A Novel Somewhat Homomorphic Encryption over Integers. *2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, 2(1), 56-67.
8. Zhang, Z., Plantard, T., & Susilo, W. (2012). On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers. *Information Security Practice and Experience*, 1(2), 353-368.
9. Plantard, T., Susilo, W., & Zhang, Z. (2013). Fully Homomorphic Encryption Using Hidden Ideal Lattice. *IEEE Transactions on Information Forensics and Security*, 8(12), 2127-2137.
10. Yi, X., Kaosar, M. G., Paulet, R., & Bertino, E. (2013). Single-Database Private Information Retrieval from Fully Homomorphic Encryption. *IEEE Transactions on Knowledge and Data Engineering*, 25(5), 1125-1134.
11. Li, Y., Gai, K., Qiu, L., Qiu, M., & Zhao, H. (2017). Intelligent cryptography approach for secure distributed big data storage in cloud computing. *Information Sciences*, 387(1), 103-115.
12. Chen, J. (2016). Cloud Storage Third-Party Data Security Scheme Based on Fully Homomorphic Encryption. *2016 International Conference on Network and Information Systems for Computers (ICNISC)*, 1(2), 34-46.

13. Ali, F. S., & Lu, S. (2016). Searchable Encryption with Conjunctive Field Free Keyword Search Scheme. 2016 International Conference on Network and Information Systems for Computers (ICNISC), 1(2), 78-87.
14. Ali, F. S., & Lu, S. F. (2016). Public Key Encryption With Conjunctive Field Free Keyword Search Scheme. International Journal of Computers & Technology, 15(14), 7423-7434.
15. Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., & Koshiba, T. (2014). Practical Packing Method in Somewhat Homomorphic Encryption. Data Privacy Management and Autonomous Spontaneous Security, 1(1), 34-50.
16. Lopez, J. M., Ruebsamen, T., & Westhoff, D. (2014). Privacy-friendly cloud audits with Somewhat Homomorphic and Searchable Encryption. 2014 14th International Conference on Innovations for Community Services (I4CS), 2(1), 65-76.
17. Yasuda, M., Yokoyama, K., Shimoyama, T., Kogure, J., & Koshiba, T. (2014). On the exact decryption range for Gentry–Halevi's implementation of fully homomorphic encryption. Journal of Mathematical Cryptology, 8(3), 89-97.
18. Coron, J., Lepoint, T., & Tibouchi, M. (2014). Scale-Invariant Fully Homomorphic Encryption over the Integers. Public-Key Cryptography – PKC 2014, 1(1), 311-328.
19. Xu, C., & Yang, S. (2018). An Improved Homomorphic Technique in Construction of Fully Homomorphic Encryption Scheme from LWE. Proceedings of the 2018 8th International Conference on Manufacturing Science and Engineering (ICMSE 2018), 1(1), 56-78.
20. Gentry, C., Groth, J., Ishai, Y., Peikert, C., Sahai, A., & Smith, A. (2014). Using Fully Homomorphic Hybrid Encryption to Minimize Non-interactive Zero-Knowledge Proofs. Journal of Cryptology, 28(4), 820-843.

Figures

Figure 1

Performance of the proposed HIZWFHE Scheme under linear transformation of encrypted data

Figure 2

Performance of the proposed HIZWFHE Scheme under linear transformation of encrypted data

Figure 3

Performance of the proposed HIZWFHE Scheme under time incurred per operations per single bit of encrypted data

Figure 4

Performance of the proposed HIZWFHE Scheme under time incurred per operations per single bit of unencrypted data

Figure 5

Performance of the proposed HIZWFHE Scheme- percentage increase in data retrieval

Figure 6

Performance of the proposed HIZWFHE Scheme- percentage increase in response time

Figure 7

Performance of the proposed HIZWFHE Scheme- percentage increase in Unmask performance time

Figure 8

Performance of the proposed HIZWFHE Scheme- percentage decrease in memory consumption rate