Research Article


S. Thanga Revathi, A. Gayathri, J. Kalaivani, Mary Subaja Christo, Danilo Pelusi, and M. Azees

1Department of Networking and Communications (School of Computing), SRM Institute of Science and Technology, Kattankulathur 603203, Chennai, India
2Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Chennai, India
3Faculty of Communication Sciences, University of Teramo, Via Balzarini, Teramo 64100, Italy
4Department of ECE, GMR Institute of Technology, Rajam, Andhra Pradesh 532127, India

Correspondence should be addressed to Mary Subaja Christo; marysubaja@gmail.com and M. Azees; azees.m@gmrit.edu.in

Received 22 October 2021; Revised 25 November 2021; Accepted 1 December 2021; Published 23 December 2021

Copyright © 2021 S. Thanga Revathi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The security of medical data in the cloud is the key consideration of cloud customers. While publishing the medical data, the cloud distributor may suffer from data leakages and attacks such that the data may leak. In order to resolve this, this article devises the developed Adaptive Fractional Brain Storm Integrated Whale Optimization Algorithm (AFBS_WOA), which is the hybridization of Adaptive Fractional Brain Storm Optimization (AFBSO) and Whale Optimization algorithm (WOA). The developed AFBS_WOA algorithm generates the key matrix coefficient for retrieving the perturbed database in order to preserve the privacy of healthcare data in the cloud. The developed AFBS-WOA scheme utilized the fitness function involving utility and privacy measures for calculating the secret key. Here, the privacy-preserved database is obtained by multiplying the input database with a key matrix based on developed AFBS-WOA using the Tracy–Singh product. For data retrieval, the secret key is shared with the service provider in order to retrieve the database, and then the data are accessed. Moreover, the experimental result demonstrates that the developed AFBS_WOA model attained the maximum utility and privacy measure of 0.1872 and 0.8755 using the Hungarian dataset.

1. Introduction

Healthcare involves various complex processes, such as treatment, diagnosis, prevention, and injury. Due to the advancement of technology, the healthcare industry has been introduced to reduce the services provided by hospitals. Nowadays, the healthcare industry is one of the tremendous emerging economies of the country. The healthcare industry performs various processes, such as medical data storage, medical data sharing, and providing medical advice to patients. Healthcare in a cloud environment is used to store the medical information of patients, including medical records, medical reports, scanning reports, and patient history. This information should be kept confidential and preserved in the cloud environment to maintain secrecy. The major challenge of healthcare in cloud computing is the privacy preservation of sensitive data. Since the healthcare model shares the sensitive information of patients with the service provider and third party through the cloud environment, this information may be hacked by the attackers [1]. Hence, various privacy preservation techniques have been introduced to conserve medical information. The important parameters considered for maintaining the security of medical information is privacy measure and utility measure. Privacy preservation is the process of conserving the sensitive information of an individual before publishing.
Some of the common privacy preservation techniques are perturbation approaches, generalization approaches, and synthetic data generators [2]. The perturbation approach produces some changes to input data, whereas the generalization approach replaces the original elements with less accurate elements, and synthetic data generators generate the synthetic data similar to the original data [3, 4]. Moreover, other protection methods employed to ensure the secrecy of information are data sanitization, blocking, cryptography, and anonymization. Data publishing with privacy conservation needs controlling the distribution while utilizing the personal details of a person. Data publishing involves two stages: data gathering and data publishing. In the initial phase, data is gathered from data owners through the data publisher, whereas the data publisher shares gathered information public or data recipient. In cloud storage, the stored information is offered by the Third-Party Auditor (TPA). Three service schemes, Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), are widely utilized for the computation and configuration of applications through Internet [2].

This article devises a novel optimization technique, namely, AFBS-WOA, to generate the retrievable data perturbation model in order to secure the data in the cloud. Here, the developed AFBS-WOA model is designed by incorporating AFBSO and WOA. Initially, the input database is combined with a secret key using the Tracy–Singh product, where the secret key is obtained by the developed AFBS-WOA scheme. The developed AFBS-WOA scheme utilized the fitness function, such as the utility and privacy measure for calculating the secret key. Moreover, the generated secret key is employed for the privacy-preserved healthcare data publishing in cloud computing.

1.1. Major Contribution of Developed AFBS-WOA Technique
The developed AFBS-WOA technique is devised to recognize the optimal key coefficient generation in order to preserve the privacy of healthcare data in the cloud. The algorithm utilizes the fitness function to calculate the secret key. The generated key will be used for the perturbation of the data in order to secure the patients’ data in the cloud. The stored data are retrieved at the required place after performing the retrieval process using the generated key.

The remaining section of this article is formed in the mentioned manner. Section 2 describes the literature survey based on privacy preservation in cloud computing; Section 3 describes the developed AFBS-WOA technique; Section 4 demonstrates the discussion of results; Section 5 provides the conclusion of this research.

2. Motivation
In the medical field, the medical records are conveyed to the research panel for deciding the kind, defect, severity, and effects of diseases. While publishing the information, the publishers do not leak any patients’ information with others for sustaining the data privacy. This motivates the researchers to do research in this domain.

2.1. Literature Survey. This section describes the literature survey of various existing techniques based on the privacy preservation of data in cloud computing.

Benifa and Mini [5] developed the Genetic Grey Wolf Optimization Algorithm (GGWO) to preserve the secrecy of information. Although the GGWO method obscures the sensitive information effectively, the information loss attained by this method was high. George and Sumathi [2] devised the Crow search-based Lion algorithm for generating the key matrix coefficient in order to preserve the information in the cloud. This method attained the maximum privacy measure and utility measure. However, the computational complexity of this method was high. Majeed [6] modeled the secure anonymization scheme for conserving the secrecy of medical information saved in the cloud. Although the privacy and utility attained by this method were high, this method has failed with a diverse environment. Yousra and Mazeena [7] developed the Privacy-Preserving Data Mining (PPDM) scheme for preserving the privacy of datasets. Although the processing speed of this method was high, the computation cost of this method was high.

Vijayakumar et al. [8, 9] proposed an alert system for helping patients with heart diseases during an emergency. The system sends a private and confidential message from the heart patient to the healthcare entities, including hospital, ambulance service, and personal doctor. The system has ensured a comparatively high level of security with low computational overhead and communication overhead. Zhou et al. [10, 11] have proposed an identity-based distributed decryption scheme for a personal health record sharing system. In this method, the data can be shared with multiple parties without reconstructing the decryption key. Moreover, it is proposed that it is secure against chosen ciphertext attack (CCA). The dynamic searchable symmetric encryption (DSSE) technique allows the user to search the dynamic information from the IIOHT system. Liu et al. [12] proposed a privacy-preserving DSSE scheme for IIOHT for the database with forward security. A secure index is developed based on the hash chain to overcome the file injection attack. Furthermore, the fine-grained operations are executed over the encrypted files, which return only the matched attribute instead of the whole file. This article also proposed a scheme to achieve attribute-based access control. Qian et al. [13] proposed a private set intersection scheme for fine-grained profile matching. The medical data are secured by reencryption techniques and the patient’s data are divided using multitag to perform the fine-grained operations. This proposed system has demonstrated that this scheme has improved efficiency by reducing the bilinear pairs.

Wang et al. [14] proposed a lightweight and reliable authentication protocol to handle the physical layer security problem and overcentralized server problem using cutting-edge blockchain technology and physically unclonable functions. In addition to this, a future extractor scheme was also proposed to handle the biometric information. The reliability of the system is proved using security evaluation methods, which illustrate that the authentication protocol
requires the least computational and communication cost. Wang et al. [15] proposed a system to address the common security weaknesses, such as the man-in-the-middle attack, key generation center, and denial-of-service attacks, by a novel pairing-free certificateless scheme. The system is based on the blockchain technique and smart contract to construct a reliable and efficient lightweight certificateless signature (CLS) scheme. The system is evaluated and proved to be reliable with less computational cost and communication cost.

2.2. Challenges. The challenges faced by the various privacy preservation techniques in cloud computing are listed as follows:

(i) The performance of the GGWO method can be enhanced by extending the technique with the group of optimization models using numerous datasets [1].

(ii) In [2], the security of the developed scheme is enhanced by including dyadic products; however, the performance of the dyadic product is not effective for all possibilities. Hence, the dyadic product can be replaced with some other advanced concepts for further improvements.

(iii) In [3], the selection of applicable trusted infrastructure, service provider, and algorithms is still inadequate to satisfy user confidentiality requirements.

(iv) The security method in [4] can be extended by including some effective sensitive attributes from the anonymous data in order to improve security.

3. Proposed AFBS-WOA for Privacy-Preserved Healthcare Data Publishing

This section describes the developed AFBS-WOA model for resolving the security issues in the cloud. Figure 1 shows the structural design of the privacy preservation scheme in the cloud using the developed AFBS-WOA. Here, the original database is multiplied with the optimal key matrix produced by the developed AFBS-WOA model using the Tracy–Singh product. The expression for Tracy–Singh product is signified as follows:

\[ T_{M\times N} = R_{M\times N} \times W_{OxP}, \]  

where the term \( W_{OxP} \) denotes the optimal key matrix acquired from AFBS-WOA, which is signified as follows:

\[ W_{OxP} = \begin{bmatrix} h_{11} & h_{12} & \ldots & h_{1q} \\ h_{21} & h_{22} & \ldots & h_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ h_{p1} & h_{p2} & \ldots & h_{pq} \end{bmatrix}, \]  

where \( h_{pq} \) specifies the optimal key matrix coefficient. The mathematical expression for the Tracy–Singh product among optimal key matrix with input data matrix is signified as follows:

\[ V_{SR\times UW} = (R_{uv} \circ W)_{uv} = \left( (R_{uv} \otimes W_{pq})_{pq} \right)_{uv}. \]

For the Tracy–Singh product, the product of the input partial matrix and the key coefficients are represented as follows:

\[ V_{SR\times UW} = \begin{bmatrix} R_{11} \circ W & R_{12} \circ W \\ R_{21} \circ W & R_{22} \circ W \end{bmatrix}. \]

Here, the terms \( R_{11}, R_{12}, R_{21}, \) and \( R_{22} \) indicate the matrix of input data and \( V_{SR\times UW} \) represents the matrix produced by the Tracy–Singh product. The obtained matrix size of the Tracy–Singh product is large, which is diminished to a size similar to that of the input database matrix for secure processing. Then, the mathematical notation for the reduced matrix is represented as follows:

\[ G_{M\times N} = \begin{bmatrix} G_1 & G_2 \\ G_3 & G_4 \end{bmatrix}, \]

where \( G_1, G_2, G_3, \) and \( G_4 \) denote the data matrix elements. Then, the secret key \( j_{1x1} = r_{11} \) is assessed from the reduced optimal key matrix, which is the primary element of the optimal key matrix. Moreover, the perturbed database \( R' \) is recognized by performing EX-OR operation for both reduced matrix \( G_{M\times N} \) and the secret key \( j_{1x1} \), and it is given in the following:

\[ R'_{M\times N} = G_{M\times N} \oplus j_{1x1}, \]

where \( G_{M\times N} \) depicts the reduced matrix.
3.2. Optimal Key Coefficient Generation Using Developed AFBS-WOA. This section describes the novel optimization method, namely, AFBS-WOA, for the optimal key coefficient generation. The developed AFBS-WOA algorithm is designed by integrating AFBSO [18] and WOA. The developed AFBS-WOA algorithm selects the key matrix coefficient without changing the characteristics of the original database. WOA is a metaheuristic method, which mimics the hunting activities of whales, and the AFBSO algorithm is designed based on the activities of the human brain. Although the searching behavior of WOA is high, the detection performance of this method is poor. Thus, the WOA algorithm does not attain the local optimum. In order to overcome this, the AFBS-WOA is developed, which improves the optimization issues. Thus, the developed AFBS-WOA algorithm selects the optimal key matrix coefficient. The processing steps for the developed AFBS-WOA algorithm are given as follows.

3.2.1. Initialization of Whale Population. The initialization function describes the size of the solution vector that relies on the size of the input matrix, which is demonstrated as follows:

\[ S = \{ S_u; 1 \leq u \leq O \}, \]  
\[ S_u \] represents the initial solution space and \( u \) represents the initialization of whales.

3.2.2. Fitness Measure. The fitness with maximum values of privacy and utility measure is considered as an optimal solution. The fitness function is used to predict the optimal solution. Here, the privacy measure is based on the modification degree and utility is based on the numerical characteristics, which are required to be preserved in order to attain the privacy-preserved database. The fitness function is described as follows:

\[ \text{Fitness} = \left( \frac{H + I}{2} \right), \]  
where \( H \) and \( I \) denote the privacy and utility, which are expressed as follows:

\[ H = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{R_{i,j} - R_{i,j}^*}{\text{Max}(R_{i,j}, R_{i,j}^*)}, \]  
\[ I = \frac{a + b}{2}, \]  
where \( R_{i,j}^* \) depicts the data elements of retrieved data, \( a \) depicts the mean, and \( b \) depicts the covariance. Moreover, the numerical aspects of the database rely on both mean and covariance acquired from the original and retrieved databases. The expression for mean and covariance is stated as follows:

\[ \text{Mean} a = 1 - \left[ \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{R_{i,j} - R_{i,j}^*}{\text{Max}(R_{i,j}, R_{i,j}^*)} \right], \]  
\[ \text{Covariance} b = 1 - \left[ \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} Q_{i,j} - \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} Q_{i,j}^* \right], \]  
where \( Q_{i,j} \) and \( Q_{i,j}^* \) defines the covariance of both original and retrieved database, correspondingly.

3.2.3. Solution Update Phase for Encircling Prey. In this phase, the solution update is done on the searching probability condition \( j < 0.5 \) and the value of \(|Y|\) is less than 1.
The distance measure is notified as $\bar{T}$, and its solution update is stated as follows:

$$\bar{T} = \left| \bar{U} \bar{S}' (f) - \bar{S} (f) \right|,$$

$$\bar{S} (f + 1) = \bar{S}' (f) - \bar{Y} \cdot \bar{T},$$  \hspace{1cm} (13)

where $\bar{Y}$ and $\bar{U}$ indicate two coefficients such that $\bar{Y}$ relies on two constraints, like $\bar{m}$ and $\bar{n}$. The value of $\bar{U}$ ranges between 0 and 1, whereas the value of $\bar{Y}$ differs between 2 and 0.

$$\bar{Y} = \bar{m} \cdot \bar{n} - \bar{m},$$

$$\bar{U} = 2 \cdot \bar{n}.$$  \hspace{1cm} (14)

### 3.2.4. Solution Update Phase for the Exploitation of WOA

After the solution update is done based on searching probability condition $j > 0.5$ and the value of $|Y|$ is fewer than 1, the exploitation process initiates, and it is stated as follows:

$$\bar{S}' (f + 1) = \bar{T} \cdot e^{bf} \cdot \cos (2\pi a) + \bar{S}' (f),$$

$$\bar{T}' = \left| \bar{S}' (f) - \bar{S} (f) \right|,$$  \hspace{1cm} (15)

where $b$ and $a$ specify the constant for search space, and the value of $\alpha$ differs between $[-1, 1]$.

### 3.2.5. Solution Update for the Exploration of WOA

When the condition of searching probability $j < 0.5$ and $|Y|$ is bigger than 1, then update solution becomes

$$\bar{S}' (f + 1) = \bar{S}'_{\text{rand}} - \bar{Y} \cdot \bar{T},$$

$$\bar{T}' = \left| \bar{U} \bar{S}'_{\text{rand}} - \bar{S}' \right|,$$  \hspace{1cm} (16)

where $\bar{S}'_{\text{rand}}$ states the random solution from optimization.

### 3.2.6. Solution Update Using AFBSO

The purpose of the AFBSO algorithm [18] is to select the optimal matrix coefficient. The optimal matrix coefficient is selected by updating the following equation:

$$S (f + 1) = \mu S (f) + \frac{1}{2} \mu S (f - 1) + \frac{1}{6} \mu (1 - \mu) S (f - 2)$$

$$+ \frac{1}{24} \mu (1 - \mu) (2 - \mu) S (f - 3) + \chi L (a, b),$$  \hspace{1cm} (17)

where $\mu = ((f_{\alpha} - f_{\min}) / (f_{\max} - f_{\min}))$, which represents the adaptive factor, $S (f)$ represents the idea chosen from the previous iteration, $S (f - 1)$ represents the idea chosen from $(f - 1)$th iteration, $S (f - 2)$ represents the idea chosen from $(f - 2)$th iteration, $S (f - 3)$ represents the idea chosen from $(f - 3)$th iteration, and $L (a, b)$ represents the Gaussian random value with mean $a$ and variance $b$.

$$\chi = d \log \left( \frac{L_{c_{\max}}/2 - L_{c}}{K} \right), \quad d = [0, 1],$$  \hspace{1cm} (18)

where $L_{c_{\max}}$ represents the maximum iteration and $L_{c}$ represents the correct iteration.

### 3.2.7. Reevaluation of Fitness Criterion

The solution acquired from the entire process is reevaluated using the fitness function, from which the maximum fitness value is considered an optimal solution.

### 3.2.8. Termination

At the final stage of iteration $Z$, a key matrix is obtained, which is considered as an optimal solution, and the obtained key matrix is employed to generate a retrievable perturbation database.

$$W_{\text{opt}} = S_{\text{optimized}}.$$  \hspace{1cm} (19)

### 3.3. Retrieval from Perturbed Database

For the retrieval phase, the perturbed database is EXORed with a secret key, which provides the reduced matrix $G_{M \times N}^{*}$. Furthermore, the reduced matrix $G_{M \times N}^{*}$ is partitioned using secret key $I$, such that the original database is retrieved at the receiver side.

$$G_{M \times N}^{*} = R_{M \times N}^{*} I_{1 \times 1},$$

$$R_{M \times N}^{*} = \frac{G_{M \times N}}{I_{1 \times 1}}.$$  \hspace{1cm} (20)

where $G_{M \times N}^{*}$ represents the retrievable reduced matrix and $R_{M \times N}^{*}$ shows the retrievable perturbation matrix. Table 1 describes the pseudocode of the developed AFBS-WOA for the retrievable data perturbation model.

### 3.4. Security Analysis

The developed AFBS-WOA model is developed for resolving the security issues in the data stored in the cloud. The original data are multiplied with the generated optimal key matrix before being stored in the cloud. An optimal key matrix is generated by the proposed AFBS-WOA model using the Tracy–Singh product. The generated matrix size is reduced to the size of the input for further processing. The stored data can be retrieved using an identified optimal key coefficient from the reduced matrix. This secret key shall be shared with the service providers for the data to be accessed. The following subsection discusses threats, security issues, challenges, and solutions for different kinds of attacks in the proposed system.

### 3.4.1. Password Guessing Attack

Password guessing attack is commonly known as Brute-Force Attack. The attacker tries to guess the password with certain combinations of the user credentials. To avoid this attack, the password should be set strongly. In our proposed system, the key to providing data security is generated separately for every data stored in the cloud. This makes it more secure against the Password Guessing Attack.
3.4.2. Data Breaches. Data breach refers to the leakage of data to the unauthorized user [19]. This attack can have a huge impact on the organization, including the leakage of sensitive data. It may occur due to problems in application designing, operational issues, or access by unauthorized users. In our proposed system, the data are stored in a perturbed format and can be retrieved only with the help of the unique secret key used for the perturbation. Thus, this system holds better for the data breach.

3.4.3. Man-in-the-Middle Attack. The man-in-the-middle attack is when an attacker positions himself between the two endpoints and alters the communication between the two parties. The proposed system perturbs the original data with an optimal key matrix $V_{SR}\, UW = (R_{uv} \oplus W_{pu})_{uv}$ before being storing in the cloud. Moreover, the data can be retrieved only using the secret key $G_{MN} = R_{MN} \oplus I_{1 \times 1}$, which is known only to the authorized persons. If the attacker is present between the cloud and the user, the attacker could not read the message as it is in the perturbed format and it can be retrieved only using the secret key.

4. Results and Discussion

This section describes the experimental outcomes recorded using the developed AFBS-WOA for privacy-conserved healthcare data publishing in cloud computing. Moreover, the simulation tool, database description, and comparative techniques are also described.

4.1. Experimental Setup. The experimentation of the developed AFBS-WOA-based privacy preservation model is implemented in Java with CloudSim tool, and the simulation requires PC, Intel I3 processor, 4 GB RAM with Windows 10 OS.

4.1.1. Database Description. The database utilized by the experimentation of the developed AFBS-WOA model is the heart disease dataset [20]. A total of three datasets are taken from the heart disease dataset, namely the Cleveland dataset, Hungarian dataset, and Switzerland dataset. The data size of the Cleveland dataset is 303 instances (rows) × 14 attributes (columns), Hungarian dataset is 294

---

**Table 1**: Algorithmic procedure of the developed AFBS-WOA for privacy-preserved healthcare data publishing.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Perturbed database retrieval using proposed AFBS-WOA</td>
</tr>
<tr>
<td>2.</td>
<td>Input: input database</td>
</tr>
<tr>
<td>3.</td>
<td>Output: perturbed data</td>
</tr>
<tr>
<td>4.</td>
<td>Parameters: Search agent $S$, highest iteration $Z$, optimized search agent $S^*$</td>
</tr>
<tr>
<td>5.</td>
<td>Initiate the algorithmic parameters</td>
</tr>
<tr>
<td>6.</td>
<td>For all element in database</td>
</tr>
<tr>
<td>7.</td>
<td>Calculate the secret key (apply AFBS-WOA)</td>
</tr>
<tr>
<td>8.</td>
<td>Calculate the Tracy Singh product based on input database as well as optimal key matrix</td>
</tr>
<tr>
<td>9.</td>
<td>Calculate secret key $J$ from optimal key matrix</td>
</tr>
<tr>
<td>10.</td>
<td>Perturbed database $R_{MN} = G_{MN} \otimes I_{1 \times 1}$</td>
</tr>
<tr>
<td>11.</td>
<td>End for</td>
</tr>
<tr>
<td>12.</td>
<td>End</td>
</tr>
<tr>
<td>//Developed AFBS-WOA algorithm</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Initiate</td>
</tr>
<tr>
<td>14.</td>
<td>Arbitrarily initialize whale population $S = {S_u; 1 \leq u \leq O}$</td>
</tr>
<tr>
<td>15.</td>
<td>Estimate the fitness measure using maximum privacy as well as utility</td>
</tr>
<tr>
<td>16.</td>
<td>While ($f &lt; Z$)</td>
</tr>
<tr>
<td>17.</td>
<td>For every $S$</td>
</tr>
<tr>
<td>18.</td>
<td>If ($j &lt; 0.5$)</td>
</tr>
<tr>
<td>19.</td>
<td>If ($</td>
</tr>
<tr>
<td>20.</td>
<td>$\overrightarrow{S} (f + 1) = S_j (f) - \overrightarrow{Y} \cdot \overrightarrow{I}$</td>
</tr>
<tr>
<td>21.</td>
<td>Else if ($</td>
</tr>
<tr>
<td>22.</td>
<td>$\overrightarrow{S} (f + 1) = \overrightarrow{S}_{rand} - \overrightarrow{Y} \cdot \overrightarrow{I}$</td>
</tr>
<tr>
<td>23.</td>
<td>End if</td>
</tr>
<tr>
<td>24.</td>
<td>Else if ($j &lt; 0.5$)</td>
</tr>
<tr>
<td>25.</td>
<td>If ($</td>
</tr>
<tr>
<td>26.</td>
<td>$\overrightarrow{S} (f + 1) = \overrightarrow{I} \cdot e^{</td>
</tr>
<tr>
<td>27.</td>
<td>Else if ($</td>
</tr>
<tr>
<td>28.</td>
<td>Update the solution using AFBSO</td>
</tr>
<tr>
<td>29.</td>
<td>End if</td>
</tr>
<tr>
<td>30.</td>
<td>Evaluate $Y$ if exceeds the search space</td>
</tr>
<tr>
<td>31.</td>
<td>Renew $S^*$ for optimal solution</td>
</tr>
<tr>
<td>32.</td>
<td>$f = f + 1$</td>
</tr>
<tr>
<td>33.</td>
<td>End while</td>
</tr>
<tr>
<td>34.</td>
<td>Return optimal solution $S^*$</td>
</tr>
<tr>
<td>35.</td>
<td>End</td>
</tr>
</tbody>
</table>
instances (rows) × 14 attributes (columns), and Switzerland data size is 123 instances (rows)×14 attributes (columns).

4.1.2. Metrics for Evaluation. The evaluation metrics employed for the developed AFBS-WOA algorithm are privacy and utility measures. The privacy measure depends on the modification degree, while the utility measure depends on the numerical characteristics; hence, the value of the privacy and the utility should be obtained as high as possible. The explanation for privacy and utility is already given in equations (10) and (11), correspondingly.

4.1.3. Techniques for Comparison. The performance improvement of the developed AFBS-WOA algorithm is calculated by comparing the recorded outcome with the outcome of existing techniques, such as Retrievable General Additive Strategy Database (RGADB) [21], Genetic Algorithm (GA) [22], WOA [23], and the genetic-WOA and BS-WOA.

4.2. Comparative Assessment of Developed AFBS-WOA. The performance improvement of the developed AFBS-WOA model is assessed by varying the percentage of data using three datasets, Cleveland dataset, Hungarian dataset, and Switzerland dataset, based on privacy and utility measures.

4.2.1. Comparative Assessment Based on the Cleveland Dataset. This section describes the assessment of the developed AFBS-WOA model based on evaluation metrics using the Cleveland dataset. Figure 2(a) describes the comparative assessment of the developed AFBS-WOA model by varying the percentage of data based on the privacy measure. When the percentage of data = 70, the privacy measure recorded by, the existing methods, RGADP is 0.1092, GA is 0.1099, WOA is 0.1122, Genetic-WOA is 0.1231, BS-WOA is 0.1484, whereas the privacy of the developed model measured is 0.1971. Figure 2(b) shows the comparative assessment of the developed model based on utility by changing the data percentage. For the data percentage = 80, the developed model recorded the utility measure of 0.8741, whereas the existing techniques, like RGADB, GA, WOA, Genetic-WOA, and BS-WOA, recorded the utility measure of 0.734, 0.7749, 0.7752, 0.7853, and 0.8751, correspondingly.

4.2.2. Comparative Assessment Based on the Hungarian Dataset. This section deliberates the comparative assessment of the developed AFBS-WOA model based on evaluation metrics using Hungarian dataset. Figure 3(a) shows the graphical outcome of existing comparative methods with the developed model based on privacy by changing the data. When the data percentage = 90, the developed model obtained the privacy of 0.1872, and the existing techniques, such as RGADB, GA, WOA, Genetic-WOA, and BS-WOA, measured the privacy values of 0.1055, 0.1076, 0.1077, 0.1527, and 0.1715, respectively. Figure 3(b) depicts the graphical representation of comparative results in terms of utility by adjusting the data percentage. When the data percentage = 80, then the utility measured by the developed AFBS-WOA model is 0.8751, RGADP is 0.7353, GA is 0.7749, WOA is 0.7752, Genetic-WOA is 0.7853, and BS-WOA is 0.8751.

4.2.3. Comparative Assessment Based on the Switzerland Dataset. This section described the comparative discussion of the developed AFBS-WOA model based on evaluation metrics using the Switzerland dataset. Figure 3(a) shows the comparative assessment of the developed model based on
privacy by changing the data percentage. For the data percentage $= 80$, the developed model recorded the privacy measure of 0.1836, whereas the existing techniques, like RGADB, GA, WOA, Genetic-WOA and BS-WOA, recorded the privacy measure of 0.1007, 0.1091, 0.1114, 0.1121, and 0.1462, correspondingly. Figure 4(b) describes the comparative assessment of the developed AFBS-WOA model by varying the percentage of data based on the utility measure. When the percentage of data $= 70$, the utility measure recorded by the existing models, like RGADP is 0.7235, GA is 0.7634, WOA is 0.7637, Genetic-WOA is 0.7731, and BS-WOA is 0.8628, whereas the developed model measured the utility of 0.8633.

4.3. Comparative Discussion. Table 2 describes the comparative discussion of the developed AFBS-WOA model for constructing the perturbation database. From the table, it is clearly declared that the developed model attained the maximum privacy of 0.1872 and maximum utility of 0.8755, correspondingly. The existing methods, like RGADB, GA, WOA, Genetic-WOA and BS-WOA, attained the privacy of 0.1055, 0.1076, 0.1077, 0.1527, and 0.1715 and the utility of 0.7355, 0.7753, 0.7755, 0.7853, and 0.8752. The comparative analysis clearly shows that the proposed AFBS-WOA achieves the maximum privacy and utility parameters compared with the other discussed existing methods. Medical data are shared all over the world for research purposes to enhance the healthy environment. Moreover, this proposed method can be applied in healthcare organizations to protect the medical data shared through the cloud. The patient’s data are stored and retrieved from the cloud in a secured way with more utility factor. The performance of the proposed system is implemented and compared using three different datasets with the fitness function.
The GGWO algorithm was proposed to enhance the security of the cloud data by employing the k-anonymization method to enhance the privacy policies of the stored data. The system evaluated has reduced fitness value with an increase in the number of iterations, which enhances the privacy of the system. Even though the system performs comparatively better than some of the other existing systems, the percentage of the information loss is comparatively high in this method. From the observations of our proposed system, we propose that it is likely to overcome the drawback of the GGWO with the maximum fitness value, privacy, and utility by enhancing the function using the proposed developed AFBS-WOA.

### 5. Conclusion

This article presents the developed AFBS-WOA model for generating the optimal key coefficient matrix. The developed AFBS-WOA method is formed by the combination of AFBSO and WOA methods in order to generate the optimal key coefficient matrix for privacy-preserved healthcare data publishing. The optimal key matrix selected by the developed AFBS-WOA method used utility and privacy measures for constructing the perturbation database in order to attain the privacy-conserved healthcare data publishing in cloud computing. Moreover, the secret key is shared with the service provider for retrieving the original perturbation database. The database from the data owner is multiplied with optimal key matrix produced by the developed AFBS-WOA model using the Tracy–Singh product to obtain the privacy-preserved healthcare database. The database retrieval is done by the key generated using the developed AFBS-WOA model. Moreover, the experimental result demonstrates that the developed AFBS-WOA model attained the maximum utility and privacy measure of 0.1872 and 0.8755 using the Hungarian dataset. In addition, the future enhancement of this research can be done by including some other effective optimization techniques for further improving the performance. In the future, the proposed method can be extended with more optimization algorithms on different datasets to enhance the GGWO system performance with various datasets.

### Data Availability

The data used to support the findings of this study are included within the article.

### Conflicts of Interest

The authors declare that they have no conflicts of interest.

### References


[14] W. Wang, C. Qiu, Z. Yin et al., ”Blockchain and PUF-based lightweight Authentication protocol for wireless medical

### Table 2: Comparative discussion.

<table>
<thead>
<tr>
<th>Database</th>
<th>Evaluation metrics</th>
<th>RGADP</th>
<th>GA</th>
<th>WOA</th>
<th>Genetic-WOA</th>
<th>BS-WOA</th>
<th>Developed AFBS-WOA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleveland</td>
<td>Privacy</td>
<td>0.1081</td>
<td>0.1093</td>
<td>0.1101</td>
<td>0.1375</td>
<td>0.1735</td>
<td>0.1781</td>
</tr>
<tr>
<td></td>
<td>Utility</td>
<td>0.7349</td>
<td>0.7746</td>
<td>0.7747</td>
<td>0.7849</td>
<td>0.8747</td>
<td>0.8749</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Privacy</td>
<td>0.1055</td>
<td>0.1076</td>
<td>0.1077</td>
<td>0.1527</td>
<td>0.1715</td>
<td>0.1872</td>
</tr>
<tr>
<td></td>
<td>Utility</td>
<td>0.7355</td>
<td>0.7753</td>
<td>0.7755</td>
<td>0.7853</td>
<td>0.8752</td>
<td>0.8752</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Privacy</td>
<td>0.1090</td>
<td>0.1107</td>
<td>0.1178</td>
<td>0.1480</td>
<td>0.1662</td>
<td>0.1691</td>
</tr>
<tr>
<td></td>
<td>Utility</td>
<td>0.7258</td>
<td>0.7650</td>
<td>0.7651</td>
<td>0.7750</td>
<td>0.8648</td>
<td>0.8657</td>
</tr>
</tbody>
</table>


