Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 20 No. 13 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijim.v20i13.62246

PAPER

A Bio-Inspired Privacy Preservation Framework for Interactive Mobile Healthcare Applications in Cloud Environments

Doddi Srilatha[1], Niroj Kumar Pani[2], Sejal Mishra[3], A. Sree Lakshmi[4], Jyoti Kanjalkar[5], Ketan Anand[6] (✉)

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, Hyderabad, India

[2]Department of Computer Science Engineering and Applications, Indira Gandhi Institute of Technology, Sarang, Odisha, India

[3]Dept. of CSE, Chandigarh University, Mohali, Punjab, India

[4]ICFAI Tech (Faculty of Science and Technology), ICFAI Foundation for Higher Education, Hyderabad, Telangana, India

[5]Vishwakarma Institute of Technology, Pune, Maharashtra, India

[6]School of Computing Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India

ketan.anand@sharda.ac.in

ABSTRACT

The rapid adoption of interactive mobile healthcare applications and cloud-enabled medical services has significantly increased the volume of sensitive patient information stored and exchanged across distributed cloud environments. Mobile health (mHealth) systems frequently rely on cloud-based repositories to support real-time accessibility, remote monitoring, and intelligent healthcare analytics. However, the involvement of third-party platforms and remote data processing introduces serious concerns related to privacy preservation and unauthorized disclosure of medical records. To address these challenges, this study proposes a bio-inspired optimization framework based on the Discrete Grey Wolf Optimizer (DGWO) for effective optimized key generation in healthcare data sanitization processes. The proposed approach integrates perturbation-based privacy preservation with optimized key management to enhance secure data sharing in mobile cloud healthcare environments while maintaining data utility for analytical tasks. The framework is evaluated using four benchmark healthcare datasets under multiple performance measures, including privacy preservation rate, information entropy, resistance against inference attacks, and data utility retention. Experimental results demonstrate that the proposed DGWO-based sanitization mechanism outperforms existing perturbation approaches in achieving a balanced trade-off between privacy and utility. The proposed model is particularly suitable for interactive mobile healthcare systems that require secure, efficient, and privacy-aware cloud data management.

KEYWORDS

data encryption, data restoration, data sanitization, Discrete Grey Wolf Optimizer (DGWO), cloud storage

Srilatha, D., Pani, N. K., Mishra, S., Lakshmi, A. S., Kanjalkar, J., Anand, K. (2026). A Bio-Inspired Privacy Preservation Framework for Interactive Mobile Healthcare Applications in Cloud Environments. *International Journal of Interactive Mobile Technologies (iJIM)*, 20(13), pp. 53–68. https://doi.org/10.3991/ijim.v20i13.62246

Article submitted 2026-03-07. Revision uploaded 2026-05-08. Final acceptance 2026-05-14.

1 INTRODUCTION

The rapid advancement of interactive mobile technologies and cloud computing has transformed the modern healthcare ecosystem by enabling real-time access, storage, and sharing of medical information through mobile devices and cloud-enabled services. In general, the collection of efficient sensitive data [1] accessibility is a key prerequisite for both health practitioners and pharmaceutical investigators for the goal of studying the features of illnesses. This is because the study of diseases is a study of characteristics. Recently, the proliferation of cloud computing services has made it possible for hospitals and healthcare centers to send their respective healthcare data to the cloud. The cloud provides ubiquitous data accessibility along with on-demand services that are of high quality at a cost that is acceptable. Furthermore, "Electronic Health Records" (EHRs) [2], [3] are a method that has gained widespread acceptance and has been used in a variety of healthcare or medical services for the purpose of enhancing the quality of patient care, which in turn is responsible for increasing the efficiency and effectiveness of healthcare supply [4], [5]. EHRs, in general, can serve the complex demands of patients by gathering information on their medical conditions and relationships. The information may be accessed by a multidisciplinary team of experts as well as other specialists from other fields. The prescriptions are presented in a manner that is both clear and organized, which helps to limit the number of medical mistakes that occur throughout the prescribing process. The use of electronic medical records makes it easier to provide requests and delegate tasks to different members of the team. Additionally, it encourages patients to take responsibility for their own medical treatment.

Along with all the benefits that medical cloud services provide, there are also certain security-related concerns that should be taken care of by individuals and governments alike. Because of the complicated or sensitive nature of medical data, as well as the social and legal implications for its exposure, the risk of privacy [6] or security risks grows when individual health care accounts are outsourced to the cloud. Encrypting healthcare data prior to sending it to the cloud is the standard way for preserving medical data [7]. This is done to protect the data from being accessed by unauthorized parties. The distribution of encrypted data, on the other hand, is not an efficient method since it has constraints in terms of substantial performance and maintenance concerns. Anonymization of data [8], [9] is the next step in the process of data sanitation, with the goal of protecting individuals' privacy. Encryption is the process of deleting personally identifying information from data sets or encrypting the information that is already there. It is possible for the data that is disguised or masked to be representative or to be an arbitrary sequence of data. In addition, the results of anonymization might be very different, and this is entirely dependent on the approach that is used for the anonymization process. The eradication of identifiability from the dataset, which is the relationship between sensitive data and persons, is another way in which this might facilitate the preservation of data privacy. Consequently, the implementation of data anonymization may be advantageous in the defense of data privacy, which ensures that users who utilize information in production are properly protected. This is something that often takes place in production environments [10], [11]. It also benefits users when they are continuously using other applications that have functionality that is like what they will be using.

Interactive mobile environments often operate under resource-constrained conditions, including limited battery power, computational capability, and communication

bandwidth. Therefore, conventional security and encryption mechanisms may not always provide efficient performance for mobile healthcare applications. This creates a strong need for lightweight and optimized privacy-preserving frameworks capable of ensuring secure cloud data access while maintaining data utility.

This study work deals with the process of data sanitization, for which a discrete bio-inspired algorithm is developed. The contributions in this study's work are as follows:

- An effective Discrete Grey Wolf Optimizer (DGWO) is developed for an effective key generation process using the Kronecker product.
- The proposed model holds the sensitive data with security over the cloud and gives the original data back without any loss.
- The proposed model is developed and evaluated on four different sensitive data from the health care domain, and the evaluations are compared with recent state-of-the-art algorithms.

Following is the structure of the remaining parts of the paper: Previous work in the realm of cloud computing data encryption and distribution is discussed in Section 2 of this paper. Section 3 comprises background knowledge of the formulated problem and the objective functions. Section 4 provides a description of the proposed DGWO as well as the procedures for the generation of keys. Part 5 provided an overview of the procedures that would be followed to carry out and evaluate the tests, and Section 6 provided a conclusion to the investigation as well as recommendations for how the technique may be improved in the future.

2 RELATED WORKS

In this section, the several strategies that have been created and used for the purpose of securing sensitive information are discussed. Encryption of data is one way offered by specialists as a means of protecting the confidentiality of sensitive information. Encryption of data is a well-known approach that may be used to resolve concerns about privacy. There is a possibility that traditional encryption techniques will not function well in the cloud due to the need for processes that are both more memory- and space-efficient and speedier when dealing with massive volumes of data. Many studies have been conducted, and a variety of potential solutions have been suggested, in response to the essential problem of maintaining data confidentiality and cybersecurity.

[12] Presents an approach used to map the portable executable files to Hadoop-compatible files. [13] Discuss the issues of data confidentiality, which is one of the most important security issues that is sensitive data exposure. The author has worked on this study and the techniques used to reduce these risks to the data stored in the cloud.

One of the most important features that cloud storage systems provide is the ability to share data. For semi-trusted contexts, [14] developed a distributed data sharing system that combines better public key infrastructure (PKI) with block-chain technology. This system enables trusted authentication using digital certificates while also providing effective auditing of both integrity and access through digest blocks. An identity-based auditing approach was presented by [15], which allows for the concealment of sensitive information and guarantees the sharing of

files in the cloud without jeopardizing the privacy of highly sensitive data. Following that, [16] developed a better approach that makes use of the sanitizable signature to solve the issue of unauthorized access. This was done in response to the fact that the technique described above allows anybody to access the cloud data. However, this technique has a security flaw since the authorization phase is the only time that the access request is validated by bilinear pairing. It is evident that there is a real-world situation in which an access request that was made by a malevolent visitor may pass verification. In a similar manner, [17] presented an ID-based auditing approach that makes use of sanitizable signatures to address the issue of concealing private information inside shared files in organizations such as the government and the military, hence improving the efficiency of information management. [18] Introduced an ID-based auditing protocol and provided access authorization to sensitive information by allowing activation or deactivation of users. This was done to facilitate access authorization. A system for certificateless auditing was developed by [19], which included the concealment of sensitive information and the use of EDLIT support for data dynamics. An ID-based audit technique was presented by [20] for the purpose of multi-copy data sharing. This scheme reduces the number of copies by means of data merging, and it also reduces hostile behavior among group users by means of decentralized trust management. Recently, [21] introduced an ID-based strategy for multi-cloud situations. This system makes use of the blind signature to successfully resist replacement attacks. Additionally, it secures the sensitive data of data providers and maintains data confidentiality across multi-cloud servers. Although the schemes have carried out a great number of audits about sensitive data sharing, these schemes do not consider the fine-grained access permission that is involved in the process of sharing sensitive data.

[22] Propose a deep-maxout-assisted data sanitization and restoration pipeline for cloud data, where a self-adaptive Namib Beetle Optimization (SANBO) algorithm generates optimal keys, further refined by a Deep Maxout classifier before Kronecker-based sanitization. Experiments show improved restoration effectiveness, key sensitivity, and robustness against malicious attacks over existing sanitization models. [23] Perform a comparative multi-cloud security policy optimization study using several metaheuristics; GWO and the Marine Predators Algorithm consistently yield low objective values across risk, encryption overhead, and open-port penalties, highlighting GWO's suitability for large-scale cloud security tuning. [24] Design a five-phase cloud privacy framework where data sanitization uses Improved Lyrebird Optimization for optimal key generation and Improved SqueezeNet for encryption, combined with Kronecker-product–based sanitization and restoration. Their model achieves high restoration correlation (up to 0.999) and lower CPA/KPA scores than RSA, AES, and several metaheuristic baselines, demonstrating strong privacy preservation in cloud environments.

Evolutionary algorithms have been successful in a wide variety of domains, including but not limited to the following: mathematical benchmark functions, numerical optimization problems, node localization, multi-objective problems, node placement, data mining, image thresholding [25], and many more. Within the scope of this investigation, the optimization strategies that were implemented in these streams served as the source of motivation for the generation of an optimal key for the encryption of data. The existence of sensitive data in the medical domain holds a lot of potential for safety and security, and a few of the sensitive medical data include applications such as the identification of negative patterns in medical data [25], [26], etc.

3 PROBLEM DEFINITION

In this section the data sanitization and restoration process and the need for an optimal key generation are given in detail for further clarifications throughout this study work. In this section, holds the data sanitization, data restoration, and objective formulation are clearly defined.

3.1 Data sanitization

Data sanitization is a crucial process in maintaining privacy. Figure 1 provides a detailed explanation of the process used to sanitize the original database. Sanitization enables the concealment of sensitive information that exists in the data. The process of data sanitization is described here.

First, the original financial data is converted into binary format by the binary conversion procedure. Next, the ideal key derived from the suggested DGWO algorithm is transformed into its binary representation. To generate the sanitized data, the binary representation of the original data and the most efficient key are subjected to a Boolean XOR operation. Equation 1 mathematically expresses the sanitized data that is produced from the original financial data.

$$D' = Key'' \oplus D \tag{1}$$

In this context, D and Key'' represent the binary representation of the original data and the optimal key obtained from the DGWO algorithm. The sanitized data is denoted as D'. Figure 1 illustrates the step-by-step process for generating the sanitized data.

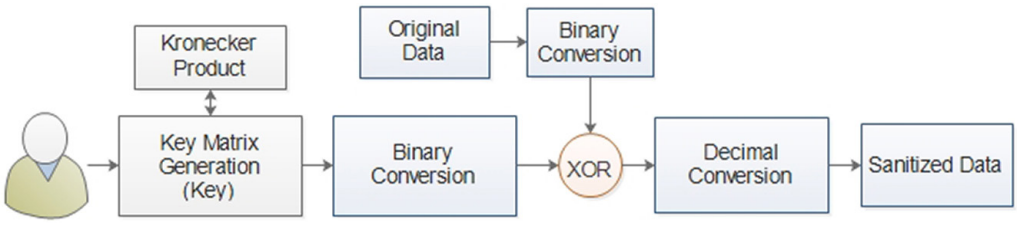


Fig. 1. Data sanitization process

Data sanitization is a process that enables the concealment of sensitive information from users other than the authorized one. Data sanitization is performed according to specific undisclosed rules. The rules before data sanitization are denoted as R, while the sanitized rules after data sanitization are denoted as R'. The sanitized data are concealed following the completion of the data sanitization process on the original database. These concealed data are then stored within the cloud environment. This task is designed to ensure the protection of sensitive information in the database and prevent cyber attacks.

The ideal key "*Key*" is generated using the DGWO technique, which ensures privacy protection. Next, the key "*Key*" is subjected to many transformations using the Kronecker product, resulting in a new key *Key*′ that is determined by using the total number of files in the database. For instance, let us assume the most efficient key is represented by $Key = \{4, 3, 8\}$. The transformation of the matrix *Key*′ is represented by Equation 2.

$$Key' = \begin{bmatrix} 4 & 3 & 8 \\ 4 & 3 & 8 \\ 4 & 3 & 8 \end{bmatrix}_{\sqrt{S}\times Q} \tag{2}$$

where the size of the *Key′* matrix is defined as square root of *S* with *Q*. In this *S* refers to the nearest square of the file size and *Q* refers to the size of the transaction, which has maximum attributes in the entire database.

To generate *Key′* the authors duplicate the rows of the key matrix *Key*. Now, the key matrix *Key′* is subjected to the Kronecker product transformation, as described in Equation 3.

$$Key'' = Key' \otimes Key' \tag{3}$$

Here, the symbol ⊗ represents the result of the Kronecker function applied to two variables. The Kronecker key *Key″* has a size that is comparable to the reconstruction matrix *Key′*. The key *Key″* is used for both the process of removing sensitive information from data (sanitization) and the process of returning data to its original state (restore). The initial key *Key* will undergo fine-tuning and be optimized using the suggested DGWO method.

3.2 Data restoration

To access the data stored in the cloud, the process of data restoration is executed. The user must submit the same key as of the key used for the data sanitization procedure in order to restore the data. Figure 2 depicts the schematic depiction of the decryption process. The *Key″* is used for both data sanitization and data restoration, following the procedure described in Equation 4.

$$\hat{D} = D' \oplus Key'' \tag{4}$$

In this context, *D′* represents the sanitized data that is kept in the data cloud, while *Key″* refers to the ideal key that is also utilized for data sanitization. An important benefit of this privacy protection paradigm is the optimized generation of a key matrix, achieved by minimizing the objective function.

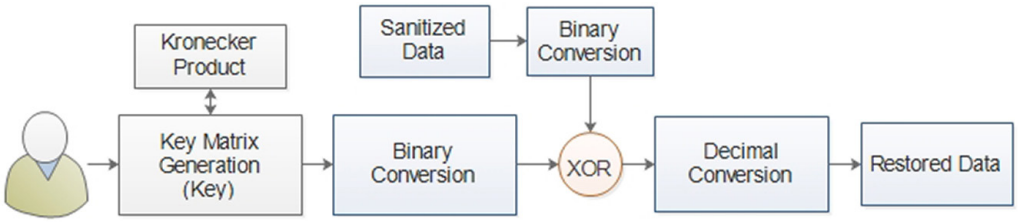


Fig. 2. Data restoration process

3.3 Objective formulation

Make sure of the sanitization and restoration process does not affect the original data; there are three objective functions framed, and they are listed below:

Degree of modification. This metric, which is defined as the difference between the original and sanitized data, is shown in Equation 5.

$$DM = Euclidian_{Distance}(D - D') \tag{5}$$

Hiding Rate. Equation 6 describes it as the total sensitive data inside the database that was initially specified for data concealing.

$$H_R = \frac{\left|R' \cap S_R\right|}{\left|S_R\right|} \tag{6}$$

where R' refers the total set of rules after sanitization and S_R refers the complete set of sanitization rules.

Preserved Information. It is the rate of nonsensitive information that is not considered when data is hidden, and it is given by Equation 7.

$$P_I = \frac{\left|R \cap R'\right|}{\left|R'\right|} \tag{7}$$

4 PROPOSED METHODOLOGY

The GWO algorithm is truly captivating due to its utilization of a group hunting technique. Muro et al. discovered that grey wolves have two distinct hunting strategies. The first involves tracking, chasing, and approaching their prey. The second strategy involves pursuing, surrounding, and tormenting the prey until it stops moving. The third strategy is launching an attack on the target animal. The remarkable adaptability of the grey wolf plays a significant role in both the exploration and exploitation phases. The objective of exploitation is to discover the most optimal solution within a limited search space. When it comes to the grey wolf, it utilizes different strategies like exploring its surroundings for prey and attacking to find the most optimal solution within a limited area. The exploration phase is characterized by the exciting pursuit of prey, as the grey wolves tirelessly search for their next meal across a vast and diverse global landscape.

In GWO wolves will look for the prey, and when they enter the origin, it will surround them after they have found them. They will do this to protect themselves. It is at this phase that the location vector of the prey is identified, and the positions of the individuals are altered in accordance with the solution that has been discovered to be the most effective.

The alpha (α) is responsible for directing the grey wolves during the hunting phase, while beta (β) and delta (δ) also make some contributions to the organization. The huge search space makes it difficult to determine the most optimal solution at the beginning of the process. However, in the hunting approach, the alpha is regarded as the first best candidate solution, the beta is the second-best candidate solution, and the delta is the third best candidate solution. These three solutions are kept and updated during each iteration to alter the position of the solution omega, which is the solution with the lowest rating. The following equation is used to establish the equation of hunting strategy:

$$D_k = c_p \times (X_k - X_i) \tag{8}$$

$$X_i = X_k - (X_y \times D_k) \tag{9}$$

where $k \in \{\alpha, \beta, \gamma\}$ and $p \in \{1, 2, 3\}$ refers to the coefficient factor that controls the exploration and are the linearly decreasing factors that balance the exploration and exploitation and i refer to the current solution and X refer to the solution vector.

4.1 Discrete Grey Wolf Optimizer

The conventional GWO is effective for continuous numerical problems. However, the key generation process is a discrete solution process where the numbers are in integer form. Hence, in the proposed DGWO, the initial solutions are rounded off, and the repeated numerals are replaced with unique integer numbers. The pseudo-code for DGWO is given in Algorithm 1. The overall architecture of the proposed framework is shown in Figure 3.

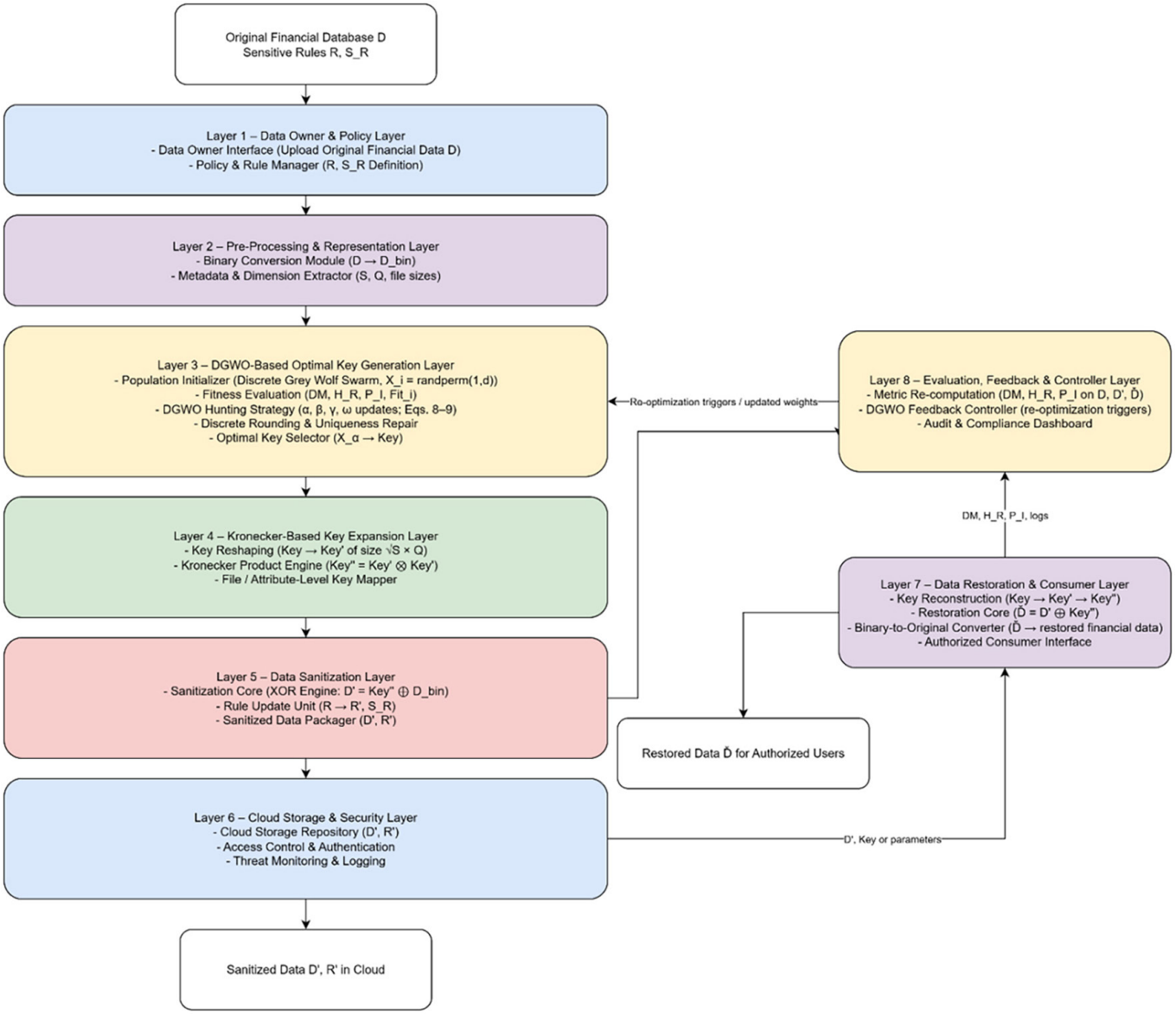


Fig. 3. Overall architecture of the proposed framework

Algorithm 1: Discrete Grey Wolf Optimizer

Input: Dataset size(S), Number of grey wolves (*Pop*), maximum Iteration (M_T), d = *key size*
Begin
//Population Initialization
for each $i = 1$ *to Pop* **do**
  $X_i = randperm(1, d)$
end for
//Fitness Computation
for each $i = 1$ *to Pop* **do**
  $Fit_i = 0.33(DM) + 0.33(1 - H_R) + 0.33(1 - P_I)$
end for
//Evolution Starts
do
  for each $i = 1$ *to Pop* **do**
    for each k & p $\{k \in \alpha, \beta, \gamma\}$ $\{p \in 1, 2, 3\}$ **do**
      $D_k = c_p \times (X_k - X_i)$
      $X_i = X_k - (X_y \times D_k)$
    end for
  end for
  //Solution Repair
  for each $i = 1$ *to Pop* **do**
    for each $j = 1$ *to* d **do**
      $X_{i,j} = roundoff(X_{i,j})$
    end for
  end for
  //Fitness Computation
  for each $i = 1$ *to Pop* **do**
    $Fit_i = 0.33(DM) + 0.33(1 - H_R) + 0.33(1 - P_I)$
  end for
  $t = t + 1$
Until $(t <= M_T)$
End
Output: X_α

5 EXPERIMENTAL ANALYSIS

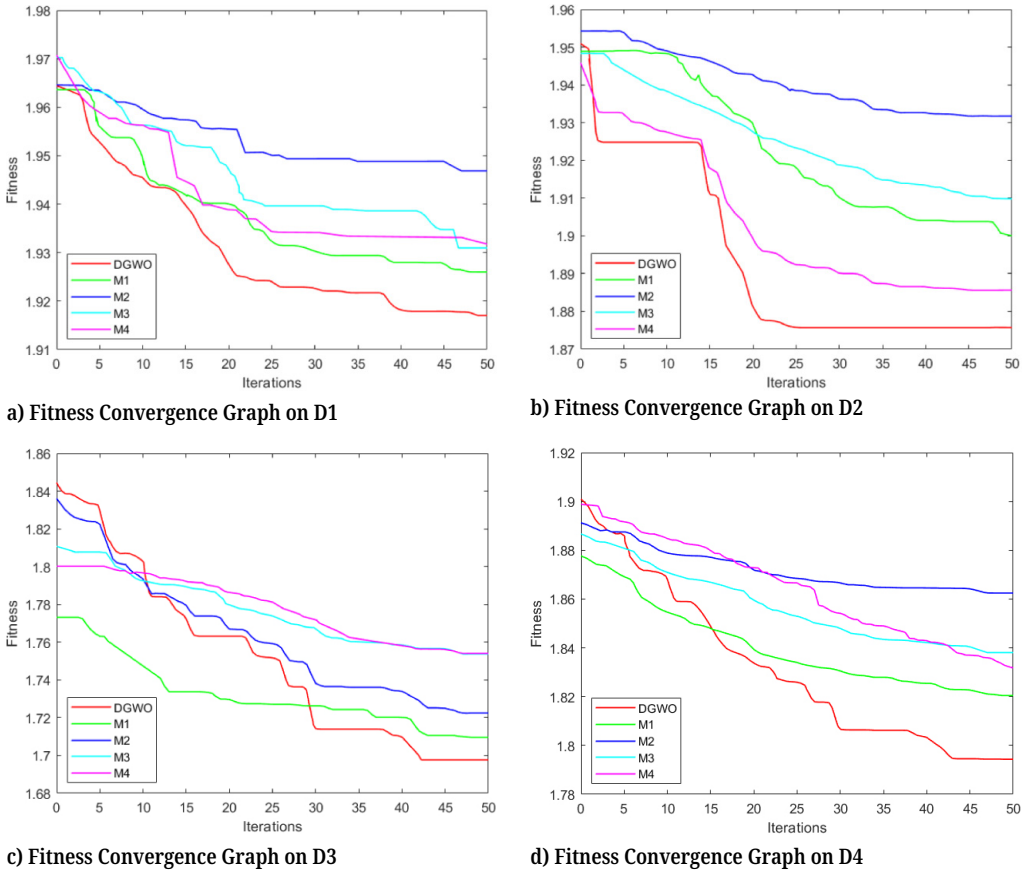
5.1 Experimental setup

Python was used to implement the DGWO algorithm that was developed based on the protection of cloud data, and the results of their experiments were evaluated throughout this process. Additionally, the dataset was gathered from. An additional comparison was made between the performance of the system that was presented and that of other schemes that were already in existence, such as TDS-NA, referred to as M1 [1]; CPAS, as M2 [6]; ID-MC, as M3 [7]; and ID-IAS, as M4 [8]. This comparison was made for many variables, including concealing ratio, information preservation ratio, fitness, and degree of modification. Datasets from different origins such as Hungary (D1), Cleveland (D2), Switzerland (D3), and Exasens (D4) are considered.

5.2 Experimental analysis in terms of fitness function

A comparison of the suggested DGWO scheme to the standard schemes is shown in Figure 4, which depicts the convergence analysis for four different datasets. It is

only after a substantial number of iterations that the approved DGWO is the best one. This is because the cost function has been simplified. Better outcomes are produced by a function with reduced costs. The number of iterations might vary anywhere from 0 to 50, with the average being 10. The selected DGWO method for this assessment results in a reduced cost function (1.917) at the 20th iteration for D1 in Figure 4a. This is since cloud data security is being considered. From the fourth to the fiftieth iterations for D2 in Figure 4b, the minimized cost function of the selected DGWO model is adequate, with results that are superior to those of other approaches such as M1, M2, M3, and M4.



a) Fitness Convergence Graph on D1

b) Fitness Convergence Graph on D2

c) Fitness Convergence Graph on D3

d) Fitness Convergence Graph on D4

Fig. 4. Convergence graph on fitness of proposed and existing algorithms

Using cloud data security for D3 in Figure 4c, the chosen DGWO model achieved the lowest cost function (1.697) when compared to M1, M2, M3, and M4, respectively, after 50 repetitions. This was the case according to the results of the comparison. Figure 4d demonstrated that the DGWO model achieved the lowest cost function (1.794) when compared to the established models such as M1, M2, M3, and M4, respectively, for D4. This was the case at the 50th iteration. The DGWO scheme that was suggested offered the greatest outcomes with the lowest cost function when compared to the models that were already in place for cloud data privacy.

5.3 Experimental analysis on objective functions

The experimental analysis on objective functions such as information preservation, hiding ratio, and degree of modifications is discussed in this section.

Analysis on information preservation

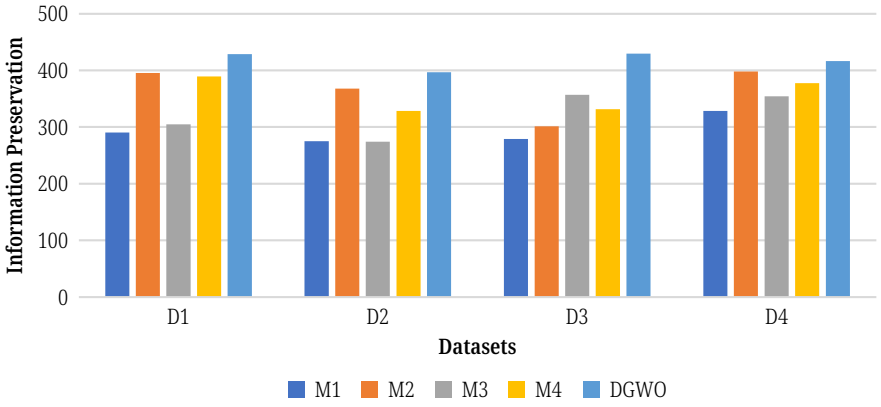


Fig. 5. Results on information preservation of algorithms on all datasets

On comparing the results of information preservation on all the datasets, the proposed DGWO outperforms the existing methodologies. On comparing the results of D1, DGWO outperforms M1 with 32.3%, M2 with 7.9%, M3 with 28.9% and M4 with 9.3% efficiency. On comparing the results of D2, DGWO outperforms M1 with 30.8%, M2 with 7.4%, M3 with 30.9%, and M4 with 17.2% efficiency. On comparing the results of D3, DGWO outperforms M1 with 35%, M2 with 29.9%, M3 with 16.9%, and M4 with 22.8% efficiency. On comparing the results of D4, DGWO outperforms M1 with 21.2%, M2 with 4.5%, M3 with 15%, and M4 with 9.4%. The complete graphical representation is shown in Figure 5.

Analysis on hiding ratio

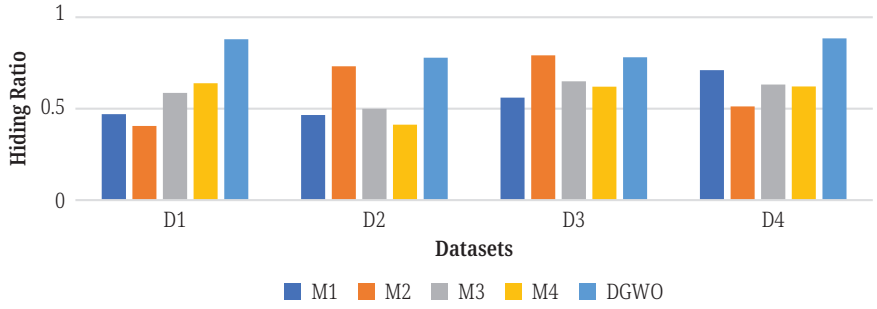


Fig. 6. Results on the hiding ratio of algorithms on all datasets

On comparing the results of the hiding ratio on all the datasets, the proposed DGWO outperforms the existing methodologies. On comparing the results of D1, DGWO outperforms M1 with 46.6%, M2 with 54%, M3 with 33.4%, and M4 with 27.4% efficiency. On comparing the results of D2, DGWO outperforms M1 with 40.2%, M2 with 6.1%, M3 with 35.9% and M4 with 47.1% efficiency. On comparing the results of D3, DGWO outperforms M1 with 28.2%, M2 with –1.3%, M3 with 16.8% and M4 with 20.7% efficiency. On comparing the results of D4, DGWO outperforms M1 with 19.7%, M2 with 42.1%, M3 with 28.6%, and M4 with 29.7% efficiency. The complete graphical representation is shown in Figure 6.

Analysis on degree of modification

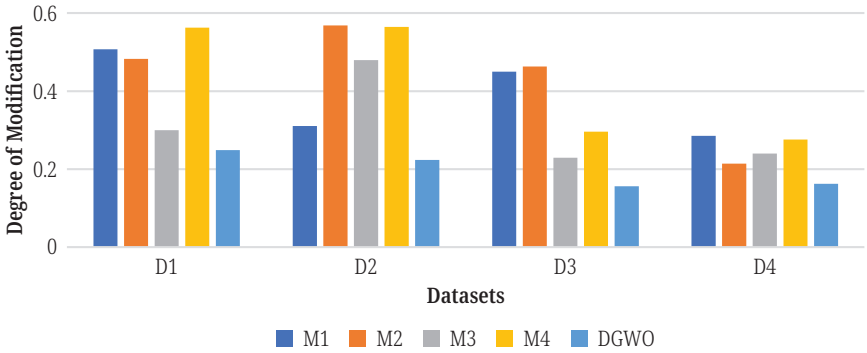


Fig. 7. Results on degree of modification of algorithms on all datasets

On comparing the results of the degree of modification on all the datasets, the proposed DGWO outperforms the existing methodologies. On comparing the results of D1, DGWO outperforms M1 with 50.9%, M2 with 48.4%, M3 with 17.1% and M4 with 55.8% efficiency. On comparing the results of D2, DGWO outperforms M1 with 28%, M2 with 0.6%, M3 with 53.3%, and M4 with 60.4% efficiency. On comparing the results of D3, DGWO outperforms M1 with 65.3%, M2 with 66.3%, M3 with 32%, and M4 with 47.2% efficiency. On comparing the results of D4, DGWO outperforms M1 with 43.1%, M2 with 24.3%, M3 with 32.4%, and M4 with 41.2% efficiency. The complete graphical representation is shown in Figure 7.

5.4 Experimental analysis on restoration effectiveness

Table 1. Experimental analysis of restoration of original data

Dataset	M1	M2	M3	M4	DGWO
D1	0.8167	0.7141	0.6231	0.7241	0.9464
D2	0.7349	0.5757	0.5116	0.7033	0.8760
D3	0.6970	0.6058	0.6219	0.6620	0.8853
D4	0.7641	0.6530	0.6223	0.7155	0.8801

Table 1 shows the effectiveness in restoring the original data from the sanitized data. On comparing the results of restoration on D1, DGWO outperforms the existing methodologies M1 with 13.7%, M2 with 24.5%, M3 with 34.2%, and M4 with 23.5%. On comparing the results of D2, DGWO outperforms M1 with 16.1%, M2 with 34.3%, M3 with 41.6%, and M4 with 19.7%. On comparing the results of D3, DGWO outperforms M1 with 21.3%, M2 with 31.6%, M3 with 29.7%, and M4 with 25.2%. On comparing the results of D4, DGWO outperforms M1 with 13.2%, M2 with 25.8%, M3 with 29.3%, and M4 with 18.7%.

5.5 Experimental analysis on CPA and KPA attack

To the CPA analysis, the correlation between the random restoration data and the random sanitized data is calculated. When calculating the KPA, it is necessary to correlate both the original data and all the sanitized data.

Table 2. Experimental analysis of KPA

Dataset	M1	M2	M3	M4	DGWO
D1	0.5096	0.5157	0.6889	0.5973	0.4772
D2	0.5656	0.6554	0.5982	0.5494	0.4106
D3	0.4899	0.6136	0.5268	0.6308	0.3806
D4	0.5106	0.5964	0.5820	0.5989	0.4130

Table 2 shows the experimental results of KPA analysis. On comparing the results of proposed DGWO on D1, DGWO outperforms existing M1 with 6.4%, M2 with 7.5%, M3 with 30.7%, and M4 with 20.1%. On comparing the results of D2, DGWO outperforms M1 with 27.4%, M2 with 37.3%, M3 with 31.4%, and M4 with 20.1%. On comparing the results of D3, DGWO outperforms M1 with 22.3%, M2 with 38%, M3 with 27.7%, and M4 with 39.7%. On comparing the results of D4, DGWO outperforms M1 by 19.1%, M2 by 30.7%, M3 by 29%, and M4 by 31%.

Table 3. Experimental analysis of CPA

Dataset	M1	M2	M3	M4	DGWO
D1	0.3369	0.3971	0.4612	0.4503	0.3287
D2	0.5344	0.4845	0.4694	0.4681	0.4064
D3	0.4189	0.4526	0.4831	0.5057	0.3860
D4	0.4234	0.4428	0.4703	0.4785	0.3776

Table 3 shows the experimental results of CPA analysis. On comparing the results of proposed DGWO on D1, DGWO outperforms existing M1 with 2.4%, M2 with 17.2%, M3 with 28.7%, and M4 with 27%. On comparing the results of D2, DGWO outperforms M1 with 23.9%, M2 with 16.1%, M3 with 13.4%, and M4 with 13.2%. On comparing the results of D3, DGWO outperforms M1 with 7.8%, M2 with 14.7%, M3 with 20.1%, and M4 with 23.7%. On comparing the results of D4, DGWO outperforms M1 with 10.8%, M2 with 14.7%, M3 with 19.7%, and M4 with 21.1%.

6 CONCLUSION

The primary objective of this study is generating the key matrix to preserve the privacy of the sensitive data. Data sanitization methods are used to encrypt the original data items into sanitized data. Sanitization approaches often focus on balancing the competing interests of privacy and data usefulness. The DGWO technique has been developed to provide an ideal key that is utilized for both the sanitization and restoration processes. The proposed DGWO was compared to several traditional techniques, including TDS-NA, CPAS, ID-MC, and ID-IAS. The comparison focused on various analyses, such as sanitization and restoration efficacy, convergence analysis, important sensitivity analysis, and statistical analysis. The findings clearly demonstrated the superiority of the suggested approach in efficiently preserving data privacy.

7 REFERENCES

[1] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, "PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs," *Inf. Sci.*, vol. 284, pp. 130–141, 2014. https://doi.org/10.1016/j.ins.2014.06.011

[2] J. Gardner *et al.*, "SHARE: System design and case studies for statistical health information release," *J. Am. Med. Inform. Assoc.*, vol. 20, no. 1, pp. 109–116, 2013. https://doi.org/10.1136/amiajnl-2012-001032

[3] S. Attuluri, M. Ramesh, R. R. Budaraju, S. Kumar, J. Swain, and J. Kurmi, "Original research article defending against phishing attacks in cloud computing using digital watermarking," *J. Auton. Intell.*, vol. 7, no. 5, pp. 1–13, 2024.

[4] A. De Giorgio, R. M. Loscalzo, M. Ponte, A. M. Padovan, G. Graceffa, and F. Gulotta, "An innovative mindfulness and educational care approach in an adult patient affected by gastroesophageal reflux: The IARA model," *J. Complement. Integr. Med.*, vol. 14, no. 4, p. 20160154, 2017. https://doi.org/10.1515/jcim-2016-0154

[5] Y. Li, C. Bai, and C. K. Reddy, "A distributed ensemble approach for mining healthcare data under privacy constraints," *Inf. Sci.*, vol. 330, pp. 245–259, 2016. https://doi.org/10.1016/j.ins.2015.10.011

[6] S. Kim, H. Lee, and Y. D. Chung, "Privacy-preserving data cube for electronic medical records: An experimental evaluation," *Int. J. Med. Inf.*, vol. 97, pp. 33–42, 2017. https://doi.org/10.1016/j.ijmedinf.2016.09.008

[7] G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records," *Int. J. Med. Inf.*, vol. 80, no. 2, pp. 94–101, 2011. https://doi.org/10.1016/j.ijmedinf.2010.11.005

[8] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," *Procedia Comput. Sci.*, vol. 113, pp. 73–80, 2017. https://doi.org/10.1016/j.procs.2017.08.292

[9] G. Poulis, G. Loukides, S. Skiadopoulos, and A. Gkoulalas-Divanis, "Anonymizing datasets with demographics and diagnosis codes in the presence of utility constraints," *J. Biomed. Inform.*, vol. 65, pp. 76–96, 2017. https://doi.org/10.1016/j.jbi.2016.11.001

[10] A. Anjum *et al.*, "An efficient privacy mechanism for electronic health records," *Comput. Secur.*, vol. 72, pp. 196–211, 2018. https://doi.org/10.1016/j.cose.2017.09.014

[11] W. Newhauser *et al.*, "Anonymization of DICOM electronic medical records for radiation therapy," *Comput. Biol. Med.*, vol. 53, pp. 134–140, 2014. https://doi.org/10.1016/j.compbiomed.2014.07.010

[12] E. Ahmed, A. A. Sorrour, M. A. Sobh, and A. M. Bahaa-Eldin, "A cloud-based malware detection framework," *Int. J. Interact. Mob. Technol. IJIM*, vol. 11, no. 2, pp. 113–127, 2017. https://doi.org/10.3991/ijim.v11i2.6577

[13] S. Alotaibi, K. Alharbi, B. Abaalkhail, and D. M. Ibrahim, "Sensitive data exposure: Data forwarding and storage on cloud environment," *Int. J. Online Biomed. Eng. IJOE*, vol. 17, no. 14, pp. 4–18, 2021. https://doi.org/10.3991/ijoe.v17i14.27365

[14] Z. Ou, X. Xing, S. He, and G. Wang, "TDS-NA: Blockchain-based trusted data sharing scheme with PKI authentication," *Comput. Commun.*, vol. 218, pp. 240–252, 2024. https://doi.org/10.1016/j.comcom.2024.02.018

[15] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 331–346, 2018. https://doi.org/10.1109/TIFS.2018.2850312

[16] Y. Xu, L. Ding, J. Cui, H. Zhong, and J. Yu, "PP-CSA: A privacy-preserving cloud storage auditing scheme for data sharing," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3730–3739, 2020. https://doi.org/10.1109/JSYST.2020.3018692

[17] Z. Liu, L. Ren, R. Li, Q. Liu, and Y. Zhao, "ID-based sanitizable signature data integrity auditing scheme with privacy-preserving," *Comput. Secur.*, vol. 121, p. 102858, 2022. https://doi.org/10.1016/j.cose.2022.102858

[18] Y. Yang, Y. Chen, F. Chen, and J. Chen, "Identity-based cloud storage auditing for data sharing with access control of sensitive information," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10434–10445, 2021. https://doi.org/10.1109/JIOT.2021.3121678

[19] Y. Ming, W. Zhang, H. Liu, and C. Wang, "Certificateless public auditing scheme with sensitive information hiding for data sharing in cloud storage," *J. Syst. Archit.*, vol. 143, p. 102965, 2023. https://doi.org/10.1016/j.sysarc.2023.102965

[20] Y. Tian, H. Tan, J. Shen, V. Pandi, B. B. Gupta, and V. Arya, "Efficient identity-based multi-copy data sharing auditing scheme with decentralized trust management," *Inf. Sci.*, vol. 644, p. 119255, 2023. https://doi.org/10.1016/j.ins.2023.119255

[21] M. Kumar, C. Maple, and S. Chand, "An efficient and secure identity-based integrity auditing scheme for sensitive data with anti-replacement attack on multi-cloud storage," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 9, p. 101745, 2023. https://doi.org/10.1016/j.jksuci.2023.101745

[22] S. D. Dhamdhere, M. Sivakkumar, and V. Subramanian, "Cloud data security with deep maxout assisted data sanitization and restoration process," *High-Confid. Comput.*, vol. 5, no. 1, p. 100238, 2025. https://doi.org/10.1016/j.hcc.2024.100238

[23] L. Karadsheh, F. Hamad, and H. Fakhouri, "Multi-cloud security policy optimization," in *2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA)*, IEEE, 2025, pp. 1–7. https://doi.org/10.1109/ICCIAA65327.2025.11013599

[24] S. Sharma and S. Tyagi, "Cloud privacy preservation using improved squeezenet based data sanitization and improved lyrebird optimization-based optimal key generation," *J. Comput. Sci.*, vol. 21, no. 7, pp. 1719–1740, 2025. https://doi.org/10.3844/jcssp.2025.1719.1740

[25] R. R. Budaraju and O. S. Nagesh, "Multi-level image thresholding using improvised cuckoo search optimization algorithm," in *2023 3rd International Conference on Intelligent Technologies (CONIT)*, IEEE, 2023, pp. 1–7. https://doi.org/10.1109/CONIT59222.2023.10205744

[26] R. Budaraju and S. K. R. Jammalamadaka, "Finding negative associations from medical data streams based on frequent and regular patterns," Preprints, 2024. https://doi.org/10.20944/preprints202402.0946.v1

8 AUTHORS

Dr. Doddi Srilatha is working as an Associate Professor in the Department of CSE at Koneru Lakshmaiah Education Foundation, Bachupally Campus, Hyderabad, India. She received her B.Tech and M.Tech from JNTU Hyderabad, India. She was awarded a Ph.D from REVA University, Bengaluru, India. Her area of interest includes software engineering, cloud computing, network security, data mining, and machine learning. She is an Oracle-certified Java programmer and AWS-certified Cloud Practitioner and Solutions Architect. She has published more than 15 research papers in reputed journals (E-mail: psrilatha@klh.edu.in).

Dr. Niroj Kumar Pani received an M. Tech in Computer Science with a specialization in Information Security from the National Institute of Technology,

Rourkela, India, in 2009, and a Ph.D. in Computer Science from Utkal University, Bhubaneswar, India in 2018. He had worked as an Assistant Professor at the Indian Institute of Science and Information Technology, Bhubaneswar, India, and as a senior analyst at ProcessMAP Corporation, India. At present, he is working as an Assistant Professor in the Department of Computer Science Engineering and Applications at Indira Gandhi Institute of Technology, Sarang, Odisha, India. He has authored many research articles in reputed international journals and books. His research interests include network security, wireless ad hoc and sensor networks, cloud computing, IoT, machine learning, and artificial intelligence (E-mail: nirojpani@igitsarang.ac.in).

Dr. Sejal Mishra holds a Ph.D. in Criminal Data Analysis using Graph Mining from Dr. C.V. Raman University (January 2025). She earned her M. Tech in Software Engineering from DAVV, Indore (2019), where she developed an arms-tracking software during her internship with the MP Police. She began her academic career as an Assistant Professor at Chouksey Engineering College, teaching C, C++, and Software Engineering. With over 5 years of teaching experience, she subsequently served as the Head of the Department (HOD) of Computer Science and Engineering at NIET, Alwar. During her tenure, she taught a wide range of subjects, including Machine Learning, Data Science, Cloud Computing Theory of Computation, and Compiler Design. Currently, Dr. Mishra is working as an Assistant Professor at Department of CSE, Chandigarh University, NH-5, Gharuan, Mohali, Punjab 140413, India. She has an established research profile with publications in reputed journals and conferences indexed in Web of Science, Scopus, IEEE, and Elsevier (E-mail: sejal.e19563@cumail.in).

Dr. A. Sree Lakshmi is currently working as an Associate Professor in the Computer Science and Engineering (AI and DS) department at ICFAI Tech (Faculty of Science and Technology), ICFAI Foundation of Higher Education, Hyderabad. She received her Ph.D. in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad, in 2020 in the area of Big Data on Cloud. She has 25 years of experience in engineering education, and her research interests include Big Data, Cloud computing, Machine Learning, and Generative AI (E-mail: asreelakshmi@ifheindia.org).

Dr. Jyoti Kanjalkar is working as Assistant Professor in the Department of Computing Science and Engineering (AI and ML) at Vishwakarma Institute of Technology, Pune (Maharashtra). She has 26 years of teaching experience. She holds a Ph.D. degree in Computer Science and Engineering from KLEF, Vijayawada, A.P., India. Her research area includes machine learning, deep learning, Image Processing, and High-Performance Computing (E-mail: jyoti.kanjalkar@vit.edu).

Ketan Anand is a seasoned, forward-looking academician, has a total of 12 years of experience teaching and training the students for UG and PG in competitive programming and sophistications of AI. He did B.Tech. (IT) and M.Tech. (Computer Science major in AI and ML) from West Bengal University of Technology and Central University in 2012 and 2015, respectively. His area of interest lies with Mathematics, Data Structures and Algorithm, Natural Language Processing and Artificial Intelligence. He is currently working in Department of CSE, School of Computing Science and Engineering, Sharda University, Greater Noida (E-mail: ketan.anand@sharda.ac.in).