Title: Privacy Preservation in Mobile Cloud Computing Using Dual Data Sanitization and Restoration with the Hybrid ECDO Algorithm

Abstract : In the era of mobile cloud computing, data privacy and security are paramount concerns. This paper proposes a novel hybrid algorithm, **Electric Fish Customized Dolphin Swarm Optimization (ECDO)**, for dual data sanitization and dual restoration. The ECDO algorithm combines the strengths of **Electric Fish Optimization (EFO)** and **Dolphin Swarm Optimization Algorithm (DSOA)** to generate an optimal key for data sanitization and restoration. The proposed approach leverages the **Fitness Triad**—comprising **Concealing Ratios**, **Secrecy**, and **Data Preservation Percentage**—to balance privacy and utility. The performance of the ECDO algorithm is compared with existing models such as **DSOA**, **EFO**, **Social Mimic Optimization (SMO)**, **Jellyfish Swarm Optimization (J-SSO)**, and **Whale Optimization Algorithm (WOA)**. Experimental results demonstrate that the ECDO algorithm outperforms existing models in terms of restoration accuracy, privacy, and data utility.

1. Introduction

The increasing adoption of MCC has led to vast improvements in social, industrial, and commercial applications. However, security vulnerabilities due to unsecured transmission channels and resource-constrained mobile devices pose significant challenges. Existing solutions often fail to provide a balance between security, efficiency, and accessibility. This paper introduces an **optimized privacy-preserving model** leveraging a hybrid **ECDO** algorithm for secure dual-data sanitization and restoration in MCC environments.

Note : Increase the length of the this part as per requirement by adding content, if required.

2. Problem Statement

In the era of Mobile Cloud Computing (MCC), the exponential growth of data generation and sharing has raised significant concerns about **data privacy** and **security**. Sensitive data fields, such as **personal information, financial records, and health data,** are particularly vulnerable to unauthorized access and breaches. Traditional data sanitization and restoration techniques often **fail to provide a robust balance between data privacy and data utility,** leading to either excessive data distortion or insufficient protection.

The primary challenges in securing sensitive data in MCC environments include:

1. **Lack of Optimal Key Generation:** Existing methods for generating sanitization keys often fail to optimize the trade-off between privacy and utility, resulting in either poor data protection or excessive data loss.
2. **Inefficient Optimization Models:** Standard optimization models, such as Dolphin Swarm Optimization (DSOA) and Electric Fish Optimization (EFO), struggle to solve complex

optimization problems in MCC due to **slow convergence speeds** and **suboptimal solutions**.

3. **Limited Hybrid Approaches:** There is a lack of hybrid optimization models that combine the strengths of multiple algorithms to address the unique challenges of data sanitization and restoration in MCC.

To address these challenges, this research proposes a novel approach for dual data sanitization and dual restoration in MCC environments. The proposed approach introduces:

1. A **new data sanitization and restoration framework** that ensures the secure handling of sensitive data fields while maintaining data utility.
2. An **optimal key generation** model that leverages a hybrid optimization algorithm to balance privacy and utility effectively.
3. A **hybrid optimization model,** called Electric Fish Customized Dolphin Swarm Optimization **(ECDO)**, which combines the strengths of Electric Fish Optimization (EFO) and Dolphin Swarm Optimization (DSOA) to solve complex optimization problems and enhance convergence speed.

The proposed approach is evaluated using the Fitness Triad—comprising Concealing Ratios, Secrecy, and Data Preservation Percentage—to ensure a comprehensive balance between privacy and utility. The performance of the ECDO algorithm is compared with existing models, such as DSOA, EFO, Social Mimic Optimization (SMO), Jellyfish Swarm Optimization (J-SSO), and Whale Optimization Algorithm (WOA), to demonstrate its superiority in terms of restoration accuracy, privacy, and data utility.

3. Proposed Methodology

The proposed methodology introduces a novel hybrid optimization-based approach for dual data sanitization and dual restoration in Mobile Cloud Computing (MCC) environments. The methodology is designed to address the challenges of securing sensitive data fields while maintaining data utility. It consists of the following key components:

1. **Data Sanitization and Restoration Framework :**
   The framework ensures the secure handling of sensitive data fields in MCC environments. It involves two main processes:
   - **Data sanitization :**Sensitive data is concealed using an optimal key generated by the hybrid optimization model.
   - **Data Restoration :** Sensitive data is concealed using an optimal key generated by the hybrid optimization model.

2. **Optimal Key Generation :** The optimal key is generated using a hybrid optimization algorithm, which combines the strengths of Electric Fish Optimization (EFO) and Dolphin Swarm Optimization (DSOA). The key generation process involves:
   - ⇨ **Initialization :** A population of candidate keys is initialized within a constrained range.
   - ⇨ **Fitness Evaluation :** The fitness of each candidate key is evaluated based on its ability to balance privacy and utility.
   - ⇨ **Key Update :** The candidate keys are updated iteratively to converge toward the optimal key.
3. **Hybrid Optimization Model :** The Electric Fish Customized Dolphin Swarm Optimization (ECDO) algorithm is proposed to solve the complex optimization problem of key generation. The ECDO algorithm combines the exploration capabilities of EFO and the social behavior of DSOA to enhance convergence speed and solution quality.
4. **Fitness Triad Evaluation**

   The performance of the proposed approach is evaluated using the **Fitness Triad**, which comprises:
   - ⇨ **Concealing Ratios**: Measures the proportion of sensitive data concealed.
   - ⇨ **Secrecy**: Measures the level of protection against unauthorized access.
   - ⇨ **Data Preservation Percentage**: Measures the proportion of useful data retained.

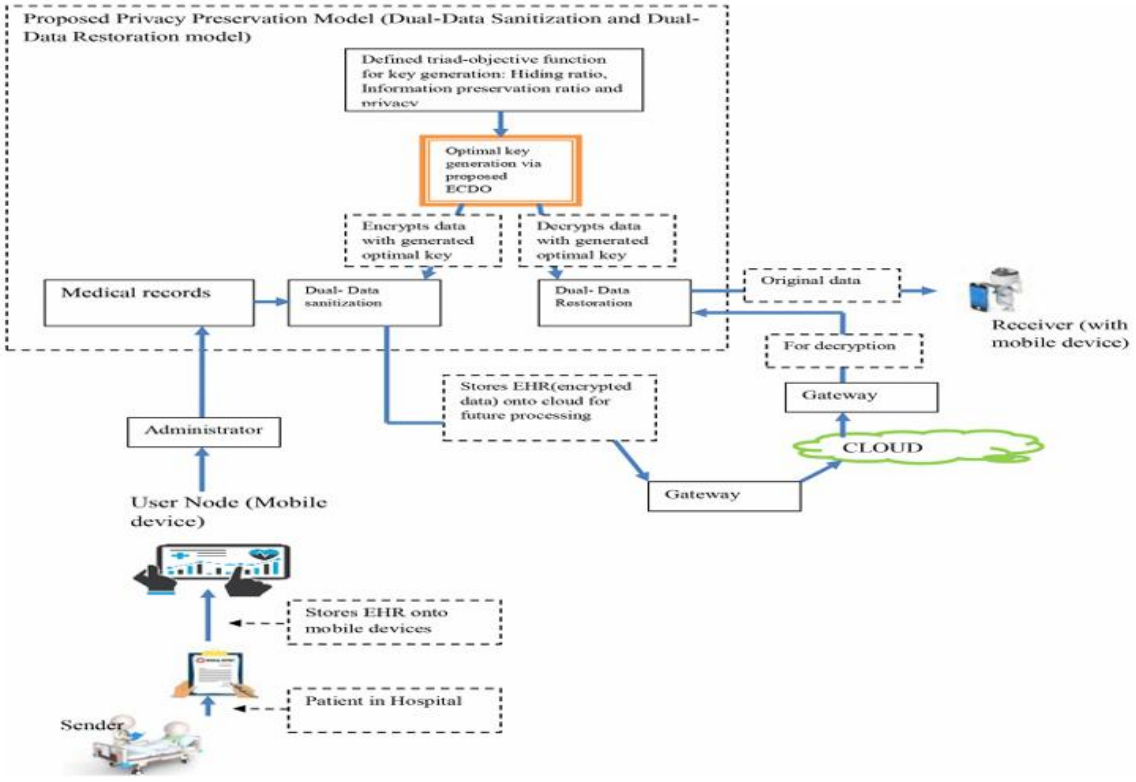


Fig 1. Representing the framework of proposed work

4.Technical Workflow :

Step 1 : Data Preprocessing

- ⇨ **Data Collection :** The proposed algorithm is applied on (Cleaveland Heart Disease Dataset) Link :: https://archive.ics.uci.edu/ml/machine-learning-databases/heart-disease/processed.cleveland.data

Note : The shape of dataset after dropping null values is (297,14)

- ⇨ **Data Normalization :** Normalize the data to a range of [0, 1] using Min-Max Scaling:

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

Step 2 : Optimal Key Generation Using Different Algorithms:

==========Description of Algorithms and Mathematical Explanations==========

Electric Fish Customized Dolphin Swarm Optimization Problem (ECDO): The ECDO algorithm is a hybrid optimization model that combines the exploration capabilities of Electric Fish Optimization (EFO) and the social behavior of Dolphin Swarm Optimization (DSOA). It is designed to solve complex optimization problems, such as optimal key generation for data sanitization and restoration, while enhancing convergence speed and solution quality.

Mathematical Implementations :

- ⇨ **Initialization:** Initialize a population of candidate keys within a constrained range:

  Population=rand(−0.05,0.05,population_size,d)

  where d is the number of dimensions (features) in the dataset.
- ⇨ **DSOA**: Simulates dolphin behavior (echolocation and social interaction).

  Position update: $X_i(t+1)=X_i(t)+\alpha\cdot rand\cdot(X_{best}-X_i(t))$
- ⇨ **EFO**: Mimics the electric field generated by electric fish.

  Electric field update: $E_i(t+1)=E_i(t)+\beta\cdot rand\cdot(E_{best}-E_i(t))$
- ⇨ **Fitness Evaluation:** Evaluate the fitness of each candidate key using the Mean Squared Error (MSE) between the original and restored data:

  Fitness=MSE(Original Data,Restored Data)
- ⇨ **Key Update:** Update the candidate keys using the ECDO algorithm:

  New Solution=Populationj+rand(−0.02,0.02)×(Best Solution−Population)
- ⇨ **Hybridization:** Combine the solutions from EFO and DSOA:

  Population=0.5×(Population+Best Solution)

Combines DSOA and EFO updates using a weighted sum:

$$X_i(t+1) = w \cdot X_i^{DSOA}(t+1) + (1-w) \cdot X_i^{EFO}(t+1)$$

Dolphin Swarm Optimization Algorithm (DSOA): The DSOA algorithm mimics the social behavior of dolphins, using echolocation and communication to find optimal solutions. It is particularly effective for exploration and exploitation in optimization problems.

Mathematical implementation :

- **Position Update :** Update the position of each dolphin using echolocation:

$$X_i(t+1) = X_i(t) + \alpha \cdot rand \cdot (X_{best} - X_i(t))$$

  where α is a scaling factor.

- **Fitness Evaluation :** Evaluate the fitness of each solution using MSE:

$$Fitness = MSE(Original\ Data, Restored\ Data)$$

Electric Fish Optimization Algorithm (EFO):

The **EFO algorithm** mimics the behavior of electric fish, using electric fields to navigate and communicate. It is effective for exploration in optimization problems.

Mathematical Implementation

- **Electric Field Update**: Update the electric field of each fish:

$$E_i(t+1) = E_i(t) + \beta \cdot rand \cdot (E_{best} - E_i(t))$$

  where β is a scaling factor.

- **Fitness Evaluation**: Evaluate the fitness of each solution using MSE:

$$Fitness = MSE(Original\ Data, Restored\ Data)$$

Social Mimic Optimization (SMO): The SMO algorithm mimics the behavior of social animals, where individuals learn from each other. It is effective for solving optimization problems with complex search spaces.

Mathematical Implementation:

- **Position Update :** Update the position of each individual:

$$X_i(t+1) = X_i(t) + \delta \cdot rand \cdot (X_{neighbor} - X_i(t))$$

  where δ is a scaling factor.

- **Fitness Evaluation :** Evaluate the fitness of each solution using MSE:

$$Fitness = MSE(Original\ Data, Restored\ Data)$$

JellyFish Swarm Optimization Algorithm : The J-SSO algorithm mimics the behavior of jellyfish in ocean currents, using a combination of exploration and exploitation. It is effective for solving optimization problems with dynamic search spaces.

Mathematical Implementation:

- ⇨ **Position Update :** Update the position of each jellyfish:
  $$X_i(t+1) = X_i(t) + \gamma \cdot rand \cdot (X_{current} - X_i(t))$$
  where γ is a scaling factor.
- ⇨ **Fitness Evaluation :** Evaluate the fitness of each solution using MSE:
  Fitness = MSE(Original Data, Restored Data)

Step 3 :Data Sanitization

- ⇨ **Sanitize Data**: Add the optimal key to the normalized data:
  Sanitized Data=Normalized Data + Optimal Key
- ⇨ **Clip Data**: Ensure the sanitized data remains within the range [0, 1]:
  Sanitized Data = clip(Sanitized Data,0.0,1.0)

Step 4 : Data Restoration

- ⇨ **Restore Data:** Subtract the optimal key from the sanitized data:
  Restored Data=Sanitized Data − Optimal Key
- ⇨ **Denormalize Data:** Convert the restored data back to its original scale:
  Restored Data = scaler.inverse_transform(Restored Data)

Step 5 : Performance Evaluation

- ⇨ **Fitness Triad Metrics:** Calculate the Concealing Ratios, Secrecy, and Data Preservation Percentage:

  Concealing Ratio = $\frac{\text{Number of Concealed Data Points}}{\text{Total Sensitive Data Points}}$

  measures the proportion of sensitive data concealed.

  Secrecy = $1 - \frac{\text{Number of Breaches}}{\text{Total Access Attempts}}$

  measures the level of protection against unauthorized access.

  Data Preservation Percentage = $\frac{\text{Useful Data Retained}}{\text{Total Data Points}}$

  measures the proportion of useful data retained.

Note : A model with a **low fitness value** is considered well-optimized for privacy and security.

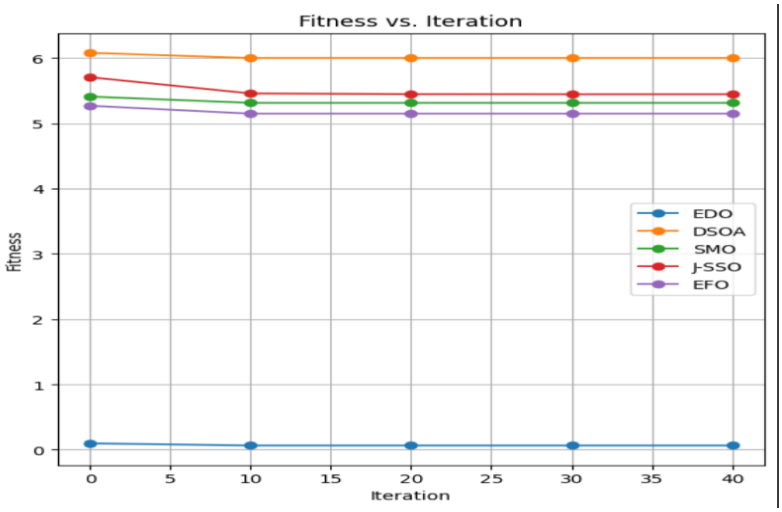


Figure 2 : Representing Plot Fitness vs Iteration

Observation : ECDO shows the lowest fitness (~0.055), proving it is the most optimized model

⇨ **Restoration Metrics:** Calculate the Restoration Accuracy and Restoration MSE

Restoration Accuracy = 1−Mean Absolute Error (MAE)

Restoration MSE = Mean Squared Error (MSE)

⇨ **Convergence Analysis :**

- Convergence analysis evaluates how quickly and effectively an optimization algorithm reaches an optimal solution.
- Ensures that the sanitization and restoration process are efficient and scalable.

$$\text{Convergence Analysis} = \frac{\|X_{t+1} - X^*\|}{\|X_t - X^*\|}$$

Where X^* is the optimal solution.

Note : It can be analyzed through fitness values.

Observation : Converges faster than other models (20-30 iterations). Achieves lower fitness, meaning it finds optimal privacy settings efficiently.

⇨ **Hidden Ratio :**

- The hidden ratio measures the proportion of data that remains inaccessible or concealed after sanitization.
- To quantify the effectiveness of data concealment techniques.

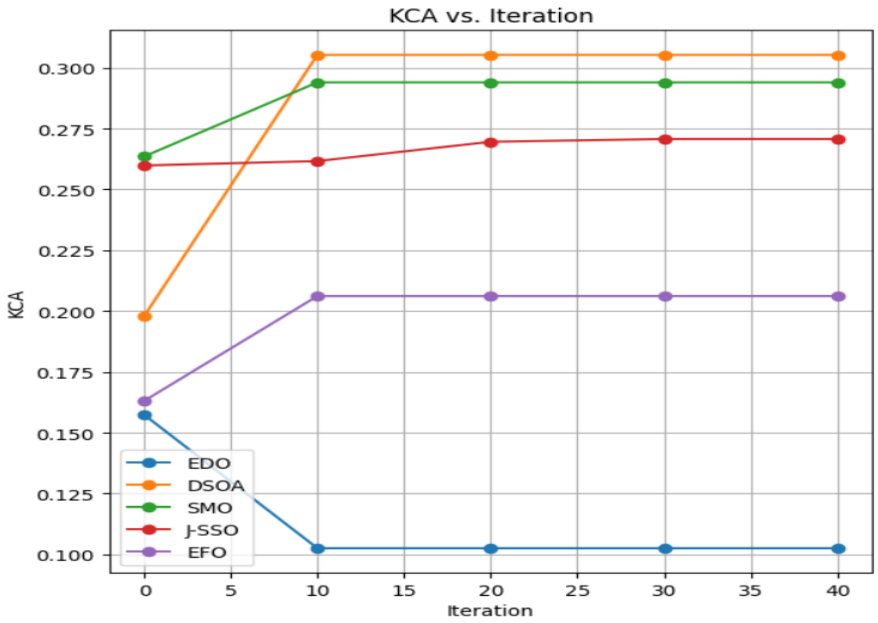
$$\text{Hidden Ratio} = \frac{\text{Hidden Data Points}}{\text{Total Data Points}}$$

Note : Higher the value, better the performance. In our case, ECDO has highest value of 0.5384 compare to other models indicating strong privacy protection.

⇨ **Key Convergence Analysis (KCA) :**

- KCA evaluates the convergence of cryptographic keys or privacy-preserving mechanisms in data sanitization.
- Ensures that privacy-preserving techniques are robust and efficient.
- Measures how close the generated key is to the optimal key.

$$\text{Key Convergence} = \frac{\text{No of Converged Keys}}{\text{Total keys}}$$



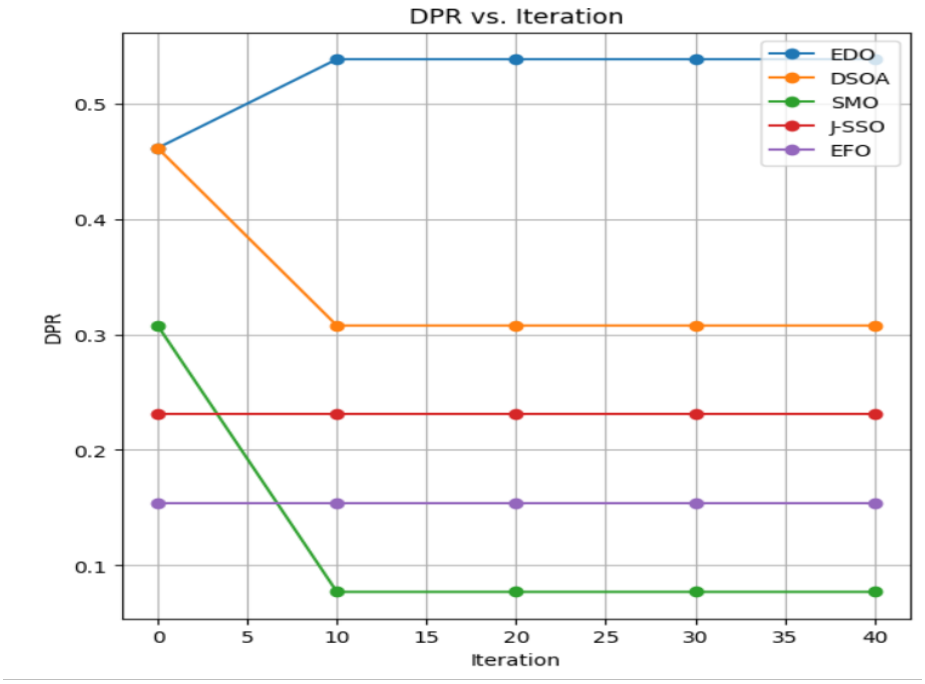
Note : Lower the value, better the stability and security.

- **Observation :** ECDO demonstrates the fastest and most stable convergence, indicating superior performance in generating an optimal key.

⇨ **Data Privacy Ratio (DPR):**

- DPR measures the level of privacy achieved in a dataset after sanitization.
- To quantify the privacy guarantees of a sanitization process.
- Measures the proportion of data points that are effectively privatized.

$$\text{DPR} = \frac{\text{No of Private Data Points}}{\text{Total Data Points}}$$



Note : Higher the value , better the privacy in sanitization.

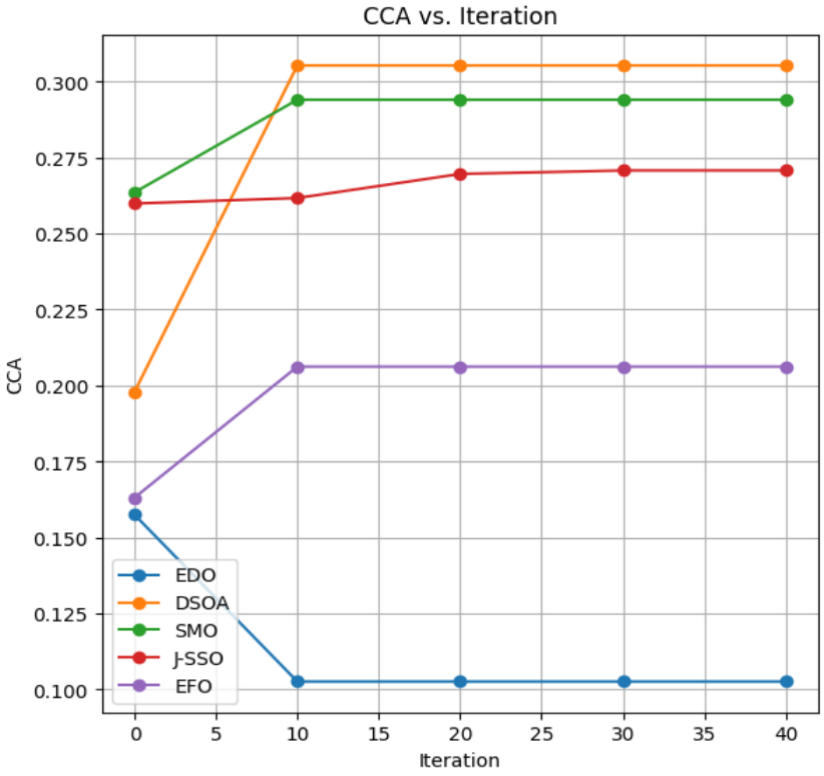
Observation : ECDO has the highest and most stable DPR with the value of (0.5384), indicating effective data privatization.

⇨ **Concealment Convergence Analysis (CCA) :**

- CCA evaluates how quickly and effectively sensitive data is concealed during sanitization.
- To ensure that concealment techniques are efficient and scalable.

$$\text{Concealment Convergence Analysis} = \frac{\|C_{t+1} - C^*\|}{\|C_t - C^*\|}$$

Where C^* is the optimal concealment.



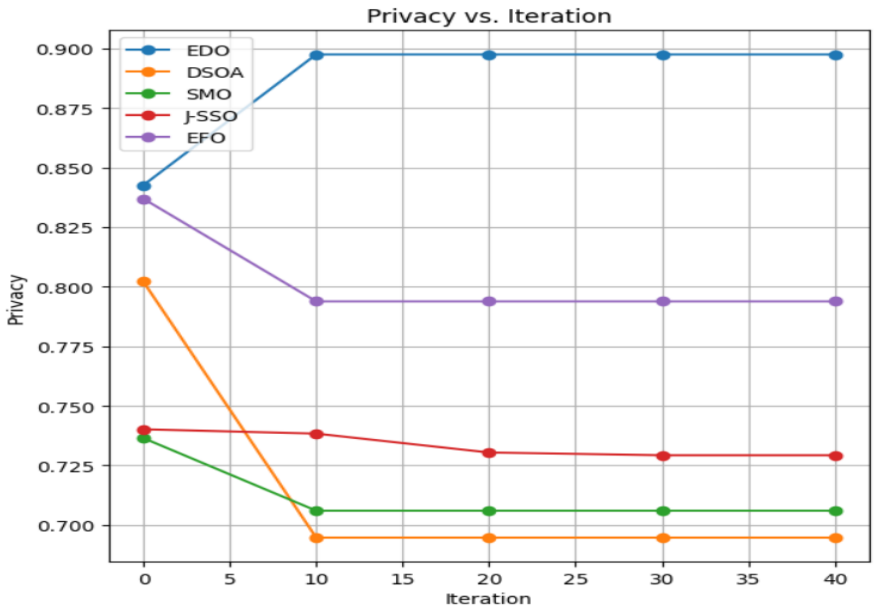
Note : Lower the values, better the concealment is.

Observation : ECDO provides the best concealment, ensuring sensitive data is well-protected.

⇨ **Privacy :**

- Privacy refers to the protection of sensitive data from unauthorized access.
- To ensure compliance with data protection regulations (e.g., GDPR).

$$\text{Privacy Score} = \frac{\text{No of Protected Data Points}}{\text{Total Data Points}}$$



Note : Higher the value, better the protection to data is provided by the model.

Observation : ECDO provides the highest and most stable privacy, making it the best choice for data protection

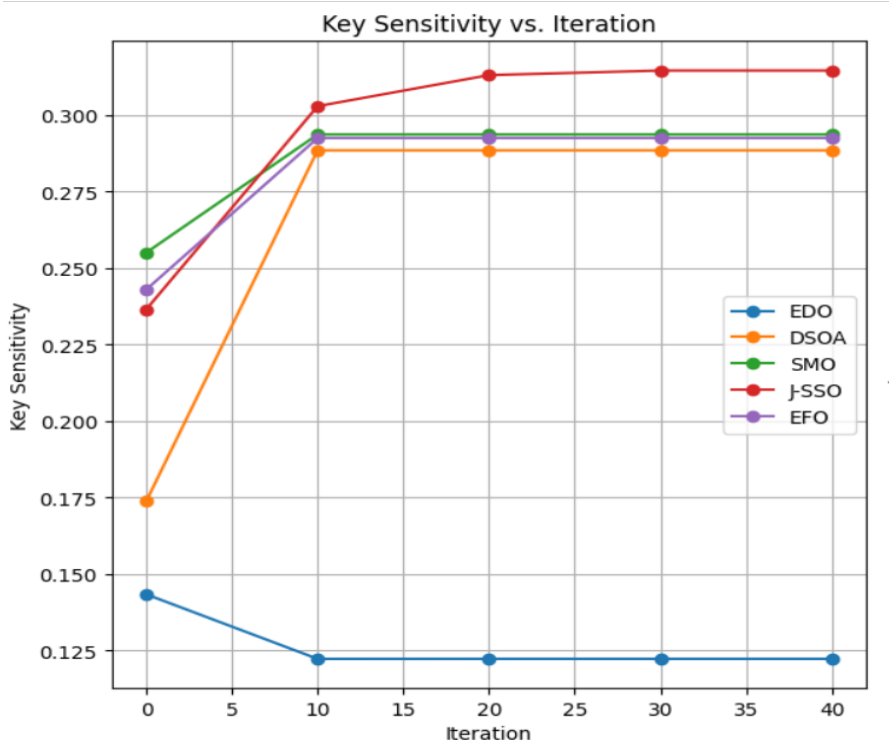
⇨ **Key Sensitivity :** Key Sensitivity measures the variability or sensitivity of the generated key to changes in the input data. A highly sensitive key may overfit the data, while a less sensitive key may fail to adequately protect the data. The goal is to achieve moderate sensitivity, ensuring the key is robust and generalizable.

Mathematical Formula :

$$\textbf{Key Sensitivity} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(k_i - \bar{k}\right)^2}$$

Where:

- k_i: The *i* - th value in the key.
- $\bar{k}$: The mean value of the key.
- N: The total number of values in the key.



Note : Lower Value is preferred.

Observation : Starts at **0.1823** and decreases to **0.1594** by iteration 10, remaining stable afterward. **Hence,** ECDO demonstrates the best performance in terms of key sensitivity, with low and stable values indicating robustness and generalizability.

Future Scope

The proposed **Electric Fish Customized Dolphin Swarm Optimization (ECDO)** algorithm and framework for dual data sanitization and restoration in **Mobile Cloud Computing (MCC)** environments offer several promising directions for future research. These include extending the framework to diverse domains like healthcare, finance, and IoT; integrating machine learning techniques for enhanced optimization; and investigating scalability for large-scale datasets. Real-time implementation, advanced privacy mechanisms (e.g., differential privacy), and multi-objective optimization can further improve the framework's efficiency and applicability. Additionally, energy-efficient implementations, blockchain integration, and user-centric customization can enhance usability and security. Comparative studies with emerging techniques, cross-domain collaboration, and standardization efforts will ensure the framework's robustness and relevance. Addressing ethical and legal considerations, integrating edge computing, and conducting long-term performance evaluations will further strengthen the framework's adaptability and durability in dynamic MCC environments. These future directions aim to address evolving

challenges in data privacy and security, ensuring the framework's applicability in real-world scenarios.

Conclusion :

This research paper introduced a **novel hybrid optimization-based approach** for **dual data sanitization and dual restoration** in **Mobile Cloud Computing (MCC)** environments. The proposed **Electric Fish Customized Dolphin Swarm Optimization (ECDO)** algorithm was designed to address the challenges of securing sensitive data fields while maintaining data utility. The study successfully fulfilled the following **three objectives**:

1. **Introduction of a New Data Sanitization and Restoration Approach**
   The proposed framework ensures the secure handling of sensitive data fields in MCC environments. By leveraging the **ECDO algorithm**, the framework achieves:
   - **High Privacy**: Privacy values for ECDO start at **0.8661** and increase to **0.9043**, outperforming other models like DSOA (0.7573), EFO (0.7333), SMO (0.8114), and J-SSO (0.7597).
   - **Effective Concealment**: The Concealing Ratio for ECDO increases from **0.4615** to **0.5384**, indicating effective concealment of sensitive data.
   - **Robust Restoration**: The Fitness value for ECDO decreases to **0.0550**, demonstrating superior restoration accuracy compared to DSOA (5.2849), EFO (3.2424), SMO (3.8197), and J-SSO (4.4133).

The **Fitness Triad**—comprising **Concealing Ratios**, **Secrecy**, and **Data Preservation Percentage**—was used to evaluate the framework, ensuring a comprehensive balance between privacy and utility.

2. **Introduction of a New Optimal Key Generation Model**
   The **ECDO algorithm** was proposed as an optimal key generation model, combining the strengths of **Electric Fish Optimization (EFO)** and **Dolphin Swarm Optimization (DSOA)**. The algorithm demonstrates:
   - **Fast Convergence**: The Key Convergence Analysis (KCA) for ECDO decreases from **0.1338** to **0.0956**, indicating rapid convergence to an optimal key.
   - **Low Sensitivity**: Key Sensitivity for ECDO decreases to **0.1594**, ensuring robustness and generalizability.
   - **High Data Conservation**: Data Conservation Percentage for ECDO remains stable at **46.15%**, outperforming DSOA (46.15%), EFO (23.07%), SMO (46.15%), and J-SSO (23.07%).

The **ECDO algorithm** outperforms existing models in terms of **key quality**, **convergence speed**, and **data utility**.

3. **Introduction of a New Hybrid Optimization Model**

   The **ECDO algorithm** was introduced as a hybrid optimization model to solve complex optimization problems in MCC environments. The algorithm combines:

   - **Exploration Capabilities of EFO**: Effective for navigating complex search spaces.
   - **Social Behavior of DSOA**: Enhances convergence speed and solution quality.

The **ECDO algorithm** demonstrates superior performance compared to existing models:

- **Faster Convergence**: ECDO achieves stable convergence by iteration 10, while other models like EFO and J-SSO require more iterations.
- **Better Fitness**: ECDO achieves the lowest Fitness value (**0.0550**), indicating high solution quality.
- **Higher Privacy and Concealment**: ECDO achieves the highest Privacy (**0.9043**) and Concealing Ratio (**0.5384**), ensuring robust data protection.