Journal of Computer Science

Research Article

Cloud Privacy Preservation Using Improved Squeezenet-Based Data Sanitization and Improved Lyrebird Optimization-Based Optimal Key Generation

Smita Sharma and Sanjay Tyagi

Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India

Article history
Received: 27-12-2024
Revised: 13-05-2025
Accepted: 26-05-2025

Corresponding Author:
Smita Sharma
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India
Email: smita148.sharma@gmail.com

Abstract: Maintaining privacy in the cloud is critical, which implies reliable and effective models that are adapted to the difficulties presented by cloud settings. This paper introduces a comprehensive privacy preservation model tailored specifically for cloud environments, comprising five important phases such as data acquisition, normalization, feature extraction, sanitization and restoration. It begins with the meticulous collection of data from diverse sources, followed by a normalization process to standardize and cleanse the acquired data, ensuring uniformity and consistency. Subsequently, crucial features such as improved entropy and statistical measures are extracted from the normalized data to provide valuable insights. The pivotal data sanitization phase employs three key processes: optimal key generation using the Improved Lyrebird Optimization Algorithm (Imp-LOA), key tuning through deep learning with the Improved SqueezeNet, and Kronecker product operation to determine the encryption process. On the other end, the data restoration process is done, which is the reverse process of sanitization, to retrieve the data. The proposed model addresses the optimization objectives including hiding failure, data preservation ratio, modification degree, and privacy. The Improved Lyrebird Optimization Algorithm generates encryption keys based on the natural behavior of lyrebirds, providing superior safety. Anticipated outcomes of this research encompass MATLAB-based simulation and investigational analysis, benchmarking against existing methods to evaluate the model's efficacy in terms of security, time efficiency, and other pertinent metrics. Through this comprehensive analysis, the proposed model's superiority in safeguarding privacy in cloud environments has been demonstrated, marking a significant advancement in privacy-preserving techniques within cloud computing.

Keywords: Privacy Preservation, Cloud Computing, Data Sanitization, Data Restoration, Optimal Key Generation, Improved SqueezeNet

Introduction

In the age of cloud computing, huge volumes of data are processed and kept on remote systems that can be accessed online. However, protecting the privacy of private data has become crucial (Kim and Kim, 2022; Yan and Gui, 2021). The inherent nature of cloud environments, characterized by shared resources and distributed infrastructure, presents numerous challenges in safeguarding data privacy (Wang and Nakachi, 2020; Ma *et al.*, 2021). As organizations increasingly rely on cloud services for their computing needs, addressing these challenges becomes imperative to maintain trust and compliance with regulatory requirements (Fang *et al.*, 2020; Mondal and Goswami, 2021). The possibility of unauthorized usage as well as information intrusion is one of the main issues regarding cloud privacy protection (Onesimu *et al.*, 2022; Ahmad and Mehfuz, 2024). With data stored on remote servers accessible via the Internet, organizations face the constant threat of malicious actors attempting to gain unauthorized access to sensitive information. Additionally, compliance with data protection regulations such as GDPR, HIPAA, and CCPA add another layer of complexity to the management of data privacy in the cloud (Liu *et al.*, 2022; Shen *et al.*, 2021).

Traditional approaches to data privacy often involve encryption techniques to protect data during transmission and storage (Son *et al.*, 2022; Yang *et al.*, 2020). While encryption provides a layer of security, it may not be sufficient to address all privacy concerns, particularly in scenarios where data needs to be analyzed or processed by third-party service providers within the cloud environment (Fugkeaw, 2022; Aminifar *et al.*, 2022). In such cases, there is a need for more sophisticated mechanisms that not only encrypt data, but also ensure that sensitive information is adequately sanitized or anonymized to avoid disclosures or unauthorized access (Yang *et al.*, 2020; Gheisari *et al.*, 2023; Patel *et al.*, 2024).

In response to these challenges, researchers and practitioners have developed various techniques and methodologies to preserve privacy in the cloud. These include encryption techniques such as homomorphic encryption and differential privacy, anonymization methods, and access control mechanisms. Additionally, advancements in technologies such as machine learning and artificial intelligence are being leveraged to enhance privacy preservation capabilities in the cloud. However, traditional sanitization methods may suffer from limitations in terms of effectiveness, efficiency, or scalability, especially when dealing with large-scale datasets in cloud environments. To address these limitations, innovative approaches are required that leverage advancements in machine learning, cryptography, and optimization techniques. This research presents an innovative privacy preservation strategy designed exclusively for cloud environments to deal with these problems. The key contributions can be summarized as follows:

- Proposing entropy-based features and basic statistical descriptors such as mean, median, minimum, and maximum into the feature extraction process. It allows the model to capture important characteristics of the data that make the preservation of data more suitable.
- Introducing an innovative sanitization technique that utilizes optimal tuned key which is produced by a combination of the proposed Imp-LOA, Improved SqueezeNet, and Kronecker product.
- Proposing an Imp-LOA method for optimal key generation, in which the enhancements are carried out in the exploration phase using the inertia weight and position refinement in the exploitation phase. These improvements significantly ensure faster convergence to the optimal solution.
- Developing an improved SqueezeNet model for the key tuning process that incorporates the proposed TriSRA activation and the batch normalization layer.Due to these enhancements, the improved SqueezeNet model enhances the quality of the key and offers better security of data within the cloud.

After the introduction, a comprehensive literature review exploring existing research and methodologies in this domain and providing a foundation for the proposed model is presented. In the section System Model, the basic cloud privacy preservation model is presented and a structured approach comprising five key phases: data acquisition, normalization, feature extraction, sanitization techniques, and data restoration is outlined. Subsequently, the outcomes obtained from applying the suggested model are presented and discussed, analyzing its efficacy in preserving privacy and achieving optimization objectives are explained. Finally, the paper concludes by summarizing the main findings and contributions.

Literature Review

Ahamad *et al.* (2022) stated that organizations operating in the cloud computing environment, are becoming more strategic, insight-driven, and efficient with artificial intelligence capabilities. Conversely, cloud computing offers businesses significant cost savings, flexibility, and agility by keeping data. The two main parts of the recommended privacy preservation approach were data sanitization and restoration processes. Furthermore, the defined sanitization process utilized a hybrid metaheuristic method to execute well in the key generation phase. As this hybrid approach combined two efficient methods, JA and SSO, it is named J-SSO. To accomplish optimal key creation, a multi-objective function incorporating metrics such as HR, DM and IPR, was derived. Ultimately, the research concluded that the suggested approach was more effective in improving cloud security than the most recent models. However, multiple algorithms and techniques need to be integrated into a cohesive privacy preservation model for cloud environments.

Yang *et al.* (2022) proposed two protocols for outsourcing biometric identification while maintaining privacy. To achieve the high efficiency goal under the recognized candidate attack paradigm, one of them primarily used the effective householder transformations and permutation technique. Under the known plain-text attack model, the other one initialized a new random split approach and combined it with the invertible linear transformation to attain a higher security requirement. Additionally, the authors rigorously analyzed the security of the two suggested methods and thoroughly assessed their effectiveness by contrasting them with earlier research. However, managing the algorithmic complexity to maintain performance and reliability is a major challenge. Zala *et al.* (2022) developed PRMS that was a record management system for the healthcare industry incorporating privacy preservation and that mainly considered throughput and latency. To confirm PRMS's applicability, a thorough performance analysis was conducted on several third-party clouds. Furthermore, through workload adjustments of up to 10,000

transactions per second, the proposed PRMS system was compared to blockchain platforms like Hyperledger Fabric v0.6 and Ethereum 1.5.8 in terms of latency and throughput. YCSB and small bank datasets were used to compare the suggested PRMS with the SRHB method. The findings of the experiment validated that PRMS was more effective than SRHB in high workload scenarios and that it could be used in cloud data centers. However, to enhance the cloud security of patient data, PRMS must have incorporated data encryption as well as cloud storage security methods. Shivaramakrishna and Nagaratna (2023) proposed a new hybrid cryptography solution to satisfy the secure data storage requirements associated with cloud computing. The corporate infrastructure included two strong encryption algorithms, RSA and AES-OTP, as well as adaptive key management and time-limited control of access. AES-OTP and RSA provided both asymmetric and symmetric encryption layers to improve data security and integrity. With the establishment of a smart system for key generation, distribution, and rotations via the adaptive key administration section, the safety of cryptographic transactions had progressively improved. Time-limited access control also helped to preserve data privacy by limiting security risks and imposing stringent temporal constraints on data access. Extensive performance evaluations validated the efficacy of the proposed framework, demonstrating astounding values for F1-score (98.56%), accuracy (99.12), precision (98.78), and recall (98.11%). However, the capabilities of increasing time-limited access control need to be focused to strengthen the security of data in the dynamic cloud computing environment.

Prasad and Rekha (2023) proposed an IAS protocol. The proposed IAS protocol was based on the use of blockchain to ensure the validity and security of the data flow in cloud computing. This enabled decentralized management of keys for recovery, cancellation, and authentication of identity. The effectiveness of the proposed paradigms with BC-IAS was evaluated through simulation in a cloud-based setting. The delivery of the message rate, the consumption of energy, the end-to-end latency, and the information access rates were some of the main performance metrics that were assessed through the experiment. Ultimately, the suggested BC-IAS protocol, which was based on blockchain technology, seemed to possess the ability to improve cloud computing safety and confidentiality. The proposed blockchain-based protocol was an acceptable option for enhancing cloud privacy and security. Because blockchain technology is decentralized, data was maintained in a transparent and tamper-proof manner. Additionally, the use of smart contracts enabled automatic implementation of access control restrictions. Furthermore, by ensuring that only authorized persons may access sensitive data, verification of identity as well as safe identification reduced the danger of information theft and cyber attacks. However, blockchain's inherent scalability limitations need to be mitigated to meet the substantial transaction and data processing demands typical in cloud computing settings.

Ragu and Ramamoorthy (2023) presented a revolutionary digital forensic architecture for the IaaS cloud. It combined the rapidly developing Blockchain as well as SDN technique. The proposed forensic framework used the blockchain system to exchange the proof collected between multiple peers, facilitating its storage. It was suggested to use the SRVA approach to guard from fraudulent accounts. Secret keys were generated throughout the HSO procedure, strengthening the cloud infrastructure. Each piece of data was encrypted using SAD-ECC and kept on a cloud server on the basis of sensitivity. The cloud-stored piece of data was constructed by the SDN manager, who also maintained metadata representing the history of the data. SHA-3 was used to construct each block as a Merkle Tree. The recommended approach enabled clients to track their data by using fuzzy-based smart contracts. The creation of a logical group of evidences, using data collected via Blockchain, allowed for the eventual possibility of evidence analysis. The Java environment as well as the network simulator 3.26 were used for the experiments. An extensive analysis showed that the suggested forensic structure exhibits evidence insertion, verification time, and positive response. However, forensic networks need to be integrated within the SDN infrastructure and incorporating cloud forensics is required to enhance the capabilities of digital forensic networks.

Transmitting sensitive data over the network can offer hackers a chance to steal information, intercept it, and prevent medical personnel, along with patients, from accessing their data. Thus, security and privacy were the primary challenges that needed to be handled for the healthcare industry to trust and use the cloud computing platform. In order to deal with this issue, Irshad *et al.* (2023) described data sanitization and restoration procedures utilizing the optimal key to ensure privacy and security. The authors employed the BFL-PSO approach to compose the optimal key on the basis of multi-objectives. The hospital discharge dataset was used to conduct the experiment. Security, encryption time, delay time, convergence speed, and error rate were evaluated during the performance analysis with the traditional works. Performance analysis showed that compared to traditional security techniques, the recommended solution was superior in providing security. However, artificial intelligence-based hashing has to be incorporated within an authorization framework for user identification in multilevel setups.

Patil and HimaBindu (2023) presented a new approach to cloud-based data security. The proposed approach used an enhanced apriori method to clean the information and protected sensitive data kept in large

datasets from misuse. Here, the primary goal was to produce a key by the application of an optimization method called CIAO-TME. The key was generated on the basis of multi-objectives and then utilized for data sanitization as well as restoration. The DM, HR and IPR were considered to analyze the performance of suggested approach and found it more effective in contrast with earlier researched schemes for all three datasets. However, data sanitization and key generation techniques should be effectively integrated so that data security can be improved more. Kumar *et al.* (2023) executed the privacy preservation paradigm in IIoT by utilizing the developments in artificial intelligence techniques. IIoT data restoration and sanitization were the two main phases of the developed system. Sensitive information in the IIoT was hidden by data sanitization to stop information leaks. The intended sanitization technique employed a new G-BHO approach to produce keys as efficiently as possible. A multiobjective strategy that included the level of modification, the hiding rate, the coefficient of correlation between the original and restored data, and the data preservation rate, was used to generate the optimal key. The outcome demonstrated that the suggested model was superior to other cutting-edge models in terms of several performance indicators. However, the approach can be improvised to address privacy concerns in IIoT environments.

Sharma and Tyagi (2024) presented a model to preserve privacy in the cloud environment by incorporating artificial intelligence with deep learning. The authors identified the sensitive data using an improved dynamic itemset counting method and then sanitized the data using an optimal tuned key. The key was developed by a combination of LSTM and MUAOA, a hybrid metaheuristic algorithm, based on fourfold objectives. The proposed scheme competed with the traditional schemes and outperformed them in terms of HR, IPR, DM, and privacy. The suggested scheme was also superior on the basis of key sensitivity, effectiveness of sanitization and restoration as well. The authors concluded that the model can be appropriate for privacy preservation and ensuring data security. However, the proposed algorithm worked effectively only for small-scale datasets, and it needs to be improvised for large-scale datasets.

Rahman *et al.* (2024) proposed an innovative method for restoring sanitized sensitive autism datasets with enhanced performance. The study utilized an optimal key generated through a hybrid PSO-GWO framework, which was applied to effectively conceal sensitive autism-related information and prevent data leakage. The same key was then used in the restoration phase, significantly improving the accuracy of recovering the original data. This dual-phase use of the optimal key contributed to stronger security and privacy measures in handling autism-related datasets. However, a notable drawback of the approach is the increased computational overhead resulting from the integration of multiple algorithms.

Dhamdhere *et al.* (2025) introduced a deep learning-assisted data sanitization method aimed at enhancing data security in cloud environments. The proposed process contained several stages such as preprocessing data, optimal key generation, deep learning-based key refinement, and application of the Kronecker product. The data were pre-processed while considering both the raw data and the extracted statistical features. A novel SANBO algorithm was developed for optimal key generation and the suitable candidates from the pool of generated keys were fine-tuned using an improved Deep Maxout classifier. The sanitization process was then completed by employing the Kronecker product. This process was reversed to restore the original data in the data restoration phase. This method effectively strengthened data security and mitigated the risk of malicious attacks in cloud settings. However, a noted limitation of the approach is its relatively limited capacity to minimize computational resource costs.

Problem Statement

Although considerable progress has been made in cloud privacy preservation research, several persistent challenges continue to limit the effectiveness of existing methods. For example, Ahamad *et al.* (2022) emphasized the importance of integrating diverse algorithms for comprehensive privacy protection, but the complexity of coordinating multiple techniques into a single cohesive model presents significant implementation challenges. Similarly, Shivaramakrishna and Nagaratna (2023) developed a hybrid cryptographic approach combining RSA and AES-OTP to enhance data storage security. Nonetheless, it does not adequately address the need for time-sensitive access controls in the dynamic cloud settings. Prasad and Rekha (2023) proposed a blockchain-based IAS protocol to ensure secure and valid data transmission. However, the protocol inherits blockchain's stability limitations which can hinder performance in data-intensive cloud environments. Irshad *et al.* (2023) introduced a BFL-PSO technique to generate optimal keys for securing health data transfer to the cloud. Yet, the model lacks integration with AI-based hashing mechanisms within an authorization framework for user identification in multi-level environments. Furthermore, Patil and HimaBindu (2023) introduced the CIAO-TME method for cloud data security, yet faced difficulties in effectively integrating data sanitization with key generation process. Additionally, Sharma and Tyagi (2024) proposed a privacy-preserving framework that generated optimal key using a combination of the LSTM model and the MUAOA algorithm, addressing factors such as HR, IPR, DM and overall privacy. However, this approach struggles with scalability; as dataset size grows, its performance in association rule hiding and key generation tends to degrade. To address

DOI: 10.3844/jcssp.2025.1719.1740

these gaps, the proposed study develops a novel privacy preservation model that integrated the Imp-LOA for robust key generation, utilized the improved SqueezeNet model for key refinement, and applies the Kronecker product to strengthen data sanitization. These enhancements together offer a scalable, efficient, and secure solution tailored for cloud environments.

System Model

The system model is designed for handling medical data privacy within cloud environment to ensure the secure, efficient, and privacy-preserving management of sensitive healthcare information. With the collaborative nature of cloud computing facilitating access to stored data by multiple users, the risk of data compromise escalates. Addressing this challenge necessitates the development of robust security solutions to safeguard data during transmission and storage. A novel healthcare privacy preservation model tailored for the cloud environment is introduced in this work. In this model, relevant data concerning heart disease, such as patient demographics, medical histories, symptoms, diagnostic results, and outcomes, are collected from various sources, including medical records, clinical trials, and research databases. Following this acquisition, the normalized dataset undergoes feature extraction to identify key attributes pertinent to heart disease diagnosis or prognosis. The subsequent phases, including data sanitization, multi-objective optimization, and restoration, remain consistent with the original model, ensuring robust privacy preservation tailored to the specific context of heart disease data. Figure 1 shows the system model architecture.

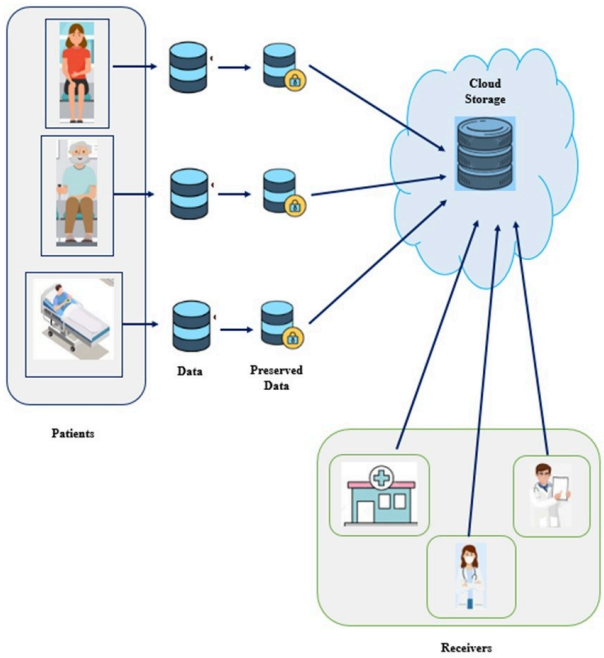


Fig. 1: System Model

Materials and Methods

The analysis of cloud privacy preservation was conducted using the Cleveland dataset, which is commonly associated with heart disease research (Janosi *et al.*, 1988; Karlekar and Gomathi, 2017). Within this dataset, there exist 76 attributes; however, research publications have predominantly centered around a subset of 14 attributes. Specifically, machine learning investigations have primarily utilized the Cleveland database due to its open accessibility, widespread use in benchmarking, and its rich clinical features, which make it suitable for evaluating privacy-preserving models. This section discusses five main stages of the complete structure of the suggested model i.e. data acquisition, normalization, feature extraction, sanitization, as well as restoration. The overall architecture of the proposed preservation model is depicted in Figure 2. Protecting the security and privacy of data generated or stored in the cloud requires considerable thought at each stage. It includes the following crucial actions:

- At first, collecting diverse datasets from relevant sources, ensuring they encompass a range of scenarios and data types pertinent to the cloud computing environment, comes under the process of data acquisition.
- Then standardizing and cleansing the acquired data in the data normalization phase to ensure uniformity, consistency and suitability for subsequent analysis.
- After the data normalization phase, the specific features are extracted, including the improved entropy and the basic statistical features such as mean, median, maximum, and minimum. These features are significant in preserving privacy and maintaining data utility.
- Afterwards, the pivotal data sanitization phase employs three key processes: optimal key generation utilizing Imp-LOA, key tuning through deep learning using Improved SqueezeNet, and Kronecker product operations to encrypt the data features.
- Here, the improved Lyrebird optimization algorithm is proposed for optimal key generation which would offer more stable convergence and a fine-tuned solution with higher precision.
- Subsequently, a deep learning model is proposed for the key tuning process, in which the improved SqueezeNet model is developed using the proposed TriSRA activation function and the batch normalization layer. This improved version enhances the security and strengthens sanitization. Thereby, the Kronecker product is performed between the tuned keys to augment the privacy of the sanitization process.
- Finally, the data restoration process is done to retrieve the original data. The model addresses optimization objectives including hiding failure,

data preservation ratio, modification degree, and privacy, ensuring a holistic approach to privacy preservation.

Data Acquisition Phase

In this phase, datasets related to heart disease *HD* are collected from the online repository (Janosi *et al.*, 1988). According to the work, a benchmark dataset is considered.

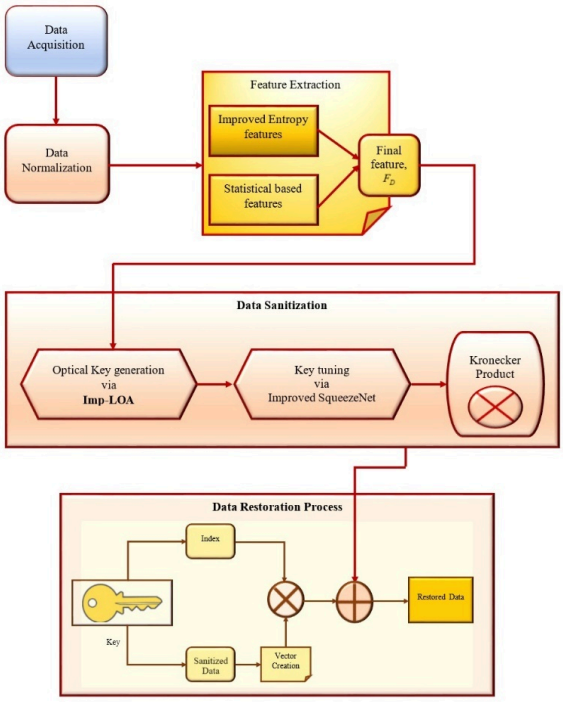


Fig. 2: Architecture of Proposed Privacy Preservation Model

Data Normalization Phase

Following data collection, the collected heart disease data undergo pre-processing for standardization, ensuring consistency and uniformity across different attributes which is called as data normalization process (Jain and Bhandare, 2013). In this proposed approach, the Min-Max Normalization (Ahamad *et al.*, 2022) method is utilized, which linearly scales un-normalized data to predefined lower (a) and upper bounds (b). The formula used in this process is expressed as per Eq. 1, wherein, *HD* represents the input data and the values of a and b are fixed as 1 and 10, respectively. The normalized data is termed as D_{N}.

$$D_N = a + \frac{HD - min(HD)}{max(HD) - min(HD)}(b - a) \quad (1)$$

Feature Extraction Phase

This section involves the extraction of relevant information (features) from the normalized data D_{N}, including entropy-based features and statistical-based features such as mean, median, minimum, and maximum. This shows the transformation of raw data into a more compact and informative representation, facilitating the subsequent analysis steps.

Improved Entropy-Based Features (IEn_i)

The entropy feature is used to assess the distribution of values within each feature of a dataset. Traditional entropy measures (Feng *et al.*, 2018), such as Shannon entropy, provide valuable insights into the uncertainty or randomness in the dataset. These features offer a more refined understanding of the data complexity compared to traditional entropy measures, but have some drawbacks. One of the main limitations is that they treat all features equally, regardless of their importance or contribution to the overall data structure. Additionally, traditional entropy measures may not adequately capture more nuanced patterns and structures within the dataset. Eq. 2 shows the traditional entropy formula which is used to quantify the amount of information present in the data or a specific feature, wherein, the entropy of i^{th} feature is denoted as En_{i}, D_{N} indicates the input (normalized data), total number of features are represented as N, probabilities of j^{th} value of i_{th} feature is denoted as Q_{ij}, which is expressed as per Eq. 3.

$$En_i = -\frac{1}{\log(N)} \sum_{j=1}^{N} Q_{ij} \log\left(Q_{ij}\right) \quad (2)$$

$$Q_{ij} = \frac{(D_N)_{ij}}{\sum_{i=1}^{N} (D_N)_{ij}} \quad (3)$$

To address these limitations, the proposed logic introduces improved entropy-based features. These enhanced features offer a more refined understanding of the data complexity compared to traditional entropy measures. The proposed method assigns weights to features based on their entropy values, which allows for a more tailored approach to feature extraction. IEn_{i} contain entropy-based weight calculation to assign weights to features based on their entropy values. This approach enhances traditional entropy-based feature extraction by incorporating a weighting mechanism that emphasizes features with higher entropy, indicating greater variability or unpredictability in the data. The proposed method calculates the entropy of each feature using Eq. 4, which is a modified version of the traditional entropy formula. This modified formula incorporates weights assigned to each feature based on their entropy values, wherein, W_{i} indicates the entropy-based weight calculation, which is expressed as per Eq. 5. The weights are assigned to features based on their entropy values, with a normalization term to ensure numerical stability ε.

$$IEn_i = -\sum_{j=1}^{N} W_i * [Q_{ij} \cdot \log\left(Q_{ij}\right) + \varepsilon] \quad (4)$$

$$W_i = \frac{1 - En_i}{N - \sum_{i=1}^{N} En_i} \quad (5)$$

Statistical Features (S)

Statistical features extracted from normalized data encompass a variety of descriptive statistics that

summarize the distribution and characteristics of the dataset. These characteristics offer useful details about the data structure, central tendency, and variability, facilitating analysis and interpretation. Some common statistical features extracted from normalized data include mean, median, minimum and maximum.

- Mean: Adding up each value in normalized data and dividing it by the total number of values, which is termed as the mean or average. It represents the central value around which the data points are distributed.
- Median: Arranging the data in ascending order, the median represents the midway value. The dataset is split in half equally, with fifty percent of the values falling below and fifty percent above the threshold. Compared to the mean, the median is less impacted by extreme numbers and gives an indication of the overall central tendency.
- Minimum: The minimum value in a dataset is the smallest value observed. It indicates the lower bound of the dataset and provides insights into the smallest value present in the data.
- Maximum: The maximum value in a dataset is the largest value observed. It indicates the upper bound of the dataset and provides insights into the largest value present in the data.

The feature extraction phase plays a crucial role in the privacy preservation model by enabling the identification and extraction of meaningful characteristics from the normalized data, which are essential for subsequent processing and analysis. Here, the final feature set is denoted as $F_D = [IEn_i\ S]$.

Data Sanitization

The data sanitization step is crucial to protect sensitive data (features) while preserving the usefulness of the data. This phase involves the application of various techniques and processes to modify or transform the data in such a way that privacy is preserved, and the risk of unauthorized access or disclosure is minimized. In this proposed model, three key processes in this phase are optimal key generation, key tuning and Kronecker product.

Optimal Key Generation using Imp-LOA

Optimal key generation is crucial for sanitization and restoration processes to ensure robust security measures. Generating strong security keys is essential for safeguarding sensitive data from unauthorized access or disclosure. In this paper, Imp-LOA is utilized for optimal key generation. This algorithm is intended to effectively search for the best possible outcomes (key generation) based on typical actions of lyrebirds (Dehghani *et al.*, 2023). The traditional LOA algorithm is effective for various optimization tasks; however, it suffers from local search capability, slow convergence speed, and a tendency to get trapped in local optima, which would limit its performance. In order to address these challenges, enhancements were made in the LOA to ensure more stable convergence and maintain diversity without compromising directionality, as well as to allow the Imp-LOA algorithm to fine-tune solutions with greater precision.

Solution Encoding: Encoding solutions in the Imp-LOA involve representing potential solutions in a format suitable for manipulation and evaluation by the algorithm. The upper and lower bounds define the feasible range of decision variables, which are taken as 1 and 0, respectively. Population size determines the number of potential solutions considered during each iteration, influencing the balance between exploration and exploitation. It is fixed as 10.

Objective Function: The objective function, also known as the fitness function or evaluation function, is a crucial component of Imp-LOA. It quantifies the quality or fitness of a potential solution based on its ability to achieve the desired objectives or criteria of the optimization problem. The objective function takes a solution as input and returns a numerical value representing how well that solution satisfies the optimization goals. Here, the multi-objectives are considered like hiding ratio (H), data preservation ratio (P), privacy (Pr), and modification degree (D). Eq. 6 indicates the objective function for finding best solution.

$$O_F = min\left(H + \frac{1}{P} + \frac{1}{Pr} + MD\right) \tag{6}$$

a. Hiding Ratio (H): This objective quantifies the effectiveness of hiding sensitive information within the sanitized data. It aims to minimize the likelihood of unauthorized access or disclosure by obscuring identifiable or sensitive attributes while retaining the data utility. Hiding ratio is computed as the ratio of the count of exposed sensitive information in sanitized data (say S_{es}) to the total count of sensitive information present in the original dataset (say D_s) as shown in Eq. 7.

$$H = \frac{S_{es}}{D_s} \tag{7}$$

b. Data Preservation Ratio (P): The data preservation ratio objective measures the extent to which useful information is retained during the sanitization process. It seeks to maximize the retention of valuable insights and patterns in the data while achieving privacy goals. According to Eq. 8, the data preservation ratio calculates the difference between the number of non-sensitive rules in the sanitized data (say S_t) and the number of non-sensitive rules that remained intact in the sanitized data (say S_i) among all the non-sensitive rules (say NS_t).

$$P = \frac{S_t - S_i}{NS_t} \tag{8}$$

c. Privacy (*Pr*): Privacy enhancement is a fundamental objective, aiming to maximize the level of privacy protection. This includes minimizing the risk of re-identification or unauthorized inference from sanitized data, thereby safeguarding the individual privacy. Privacy implies encrypting sensitive private data before storing and processing it due to data privacy concerns, which is expressed in Eq. 9 with *a* and *b* representing the length of original data (*D*) and sanitized data (*S*), respectively.

$$Pr = \frac{1}{a*b} \sum_{i=1}^{a} \sum_{j=1}^{b} \frac{D-S}{max(D,S)} \quad (9)$$

d. Modification Degree (*MD*): The modification degree objective evaluates the extent of alterations made to the original data during the sanitization process. It aims to minimize unnecessary changes to the data structure or content, preserving data integrity and accuracy while balancing the privacy requirements. This is determined by the Euclidean distance as per Eq. 10, wherein, u_i represents the i^{th} sensitive data in the original sensitive data and v_i indicates the i^{th} sensitive data in the sanitized sensitive data.

$$MD = \sqrt{\sum_{i=1}^{N} (u_i - v_i)^2} \quad (10)$$

Each objective serves as a measure of the effectiveness and impact of the sanitization process in preserving privacy and maintaining data integrity.

Mathematical Modeling of Imp-LOA: Mathematical modeling of Imp-LOA for optimal key generation is given in this section, which undergoes three key updates. Firstly, during initialization, the algorithm makes a uniform distribution of candidate keys within the search space. Secondly, in the exploration phase, dynamic inertia weights are introduced to regulate the balance between exploration and exploitation, allowing for adaptive optimization. Lastly, after both the exploration and exploitation phases, candidate solutions undergo further refinement to enhance convergence and solution quality.

a. Updated initialization by Uniform Initialization Algorithm: Inspired by the mating habits of male lyrebirds, which are renowned for their amazing capacity to reproduce noises from their surroundings, Imp-LOA has been proposed as a nature-inspired metaheuristic algorithm. Here, the Uniform Particle Initialization Algorithm (Ardiansyah *et al.*, 2022) has been used to initialize its population of solutions. This initialization strategy ensures that particles are uniformly distributed across the search space, mitigating the risk of aggregation, and facilitating effective exploration of diverse regions early in the optimization process.

It begins by randomly selecting a base point, denoted as X_1, within the feasible search space, serving as a pivotal reference for the subsequent particle distribution. This is followed by the generation of a random permutation of integers ranging from 1 to $n - 1$, where n signifies the number of particles, forming the matrix R to infuse randomness into the initialization process. Each particle, indexed from 1 to n, and each dimension, from 1 to D where D represents the dimensionality of the search space, is then assigned a position X_{id} ensuring a uniform spread across the search space while maintaining a minimum distance between particles. Boundary handling mechanisms are employed to meticulously adjust positions that surpass allowable ranges for particular dimensions, ensuring adherence to predefined boundaries and preventing solutions from straying beyond the feasible region of the search space. This holistic approach to initialization sets the stage for effective exploration and robust optimization within the Imp-LOA framework, ultimately enhancing its capacity to derive optimal encryption keys efficiently and reliably. Algorithm 1 represents the uniform initialization.

Algorithm 1 Uniform Particle Initialization

Initialize X_1 randomly within the search area
for $d = 1$ to D **do**
  Randomly rearrange [1, 2, ..., (n-1)] to get R_d = [R_{1d}, R_{2d}, ..., $R_{(n-1)d}$]
end for
for $i = 1$ to n **do**
  for $d = 1$ to D **do**
    $X_{id} = X_{id} + (R_{(n-1)d} \div n) * (X_{dmax} - X_{dmin})$
    if $X_{id} > X_{dmax}$ **then**
      $X_{id} = X_{id} - (X_{dmax} - X_{dmin})$
    end if
  end for
end for

b. Updated Exploration Phase by Dynamic Inertia Weight: The exploration phase in Imp-LOA tailored for optimal key generation is a crucial component, orchestrating the systematic exploration of the solution space to derive sanitization keys that maximize data privacy and security. Inspired by the lyrebird's behavior of escaping to safe areas, Imp-LOA dynamically adjusts the positions of candidate keys, mimicking the bird's movement to scan different regions of the problem-solving search space. This phase is pivotal in facilitating comprehensive exploration, allowing the algorithm to discover promising regions that may contain optimal solutions.

During the exploration phase of Imp-LOA, each candidate key identifies safe areas based on the other keys' locations with superior objective function values. These safe areas represent regions where the sanitization keys exhibit enhanced characteristics related to data privacy and security. The set of safe areas for each key i is determined

using Eq. 11, wherein, i = 1,2,...,N. Here, SA_{i} denotes the set of safe areas for the i_{th} sanitization key, X_{l} represents the position of the l_{th} key, and $(O_{\mathrm{F}})_{\mathrm{l}}$ is the corresponding objective function value.

$$SA_i = \left\{X_l, (O_f)_l < (O_F)_i; l \in \{1, 2, \cdots, N\}\right\} \quad (11)$$

In Imp-LOA, the displacement modeling process simulates the lyrebird's escape to one of the identified safe areas. Each key's new position is computed using Eq. 12, reflecting the dynamic movement towards regions that exhibit superior sanitization characteristics. Here, $X_{\mathrm{i}}^{\mathrm{P}_{\mathrm{j}}^{1}}$ indicates the new position of the i_{th} sanitization key in the j_{th} dimension, $R_{\mathrm{i,j}}$ is a random value, $SA_{\mathrm{i,j}}$ indicates the position of the safe area in the j_{th} dimension, and T_{ij} is a random binary value.

$$X_{i,j}^{P1} = X_{i,j} + R_{i,j} \cdot (SA_{i,j} - T_{i,j} \cdot x_{i,j}) \quad (12)$$

In this position, it is updated by using the dynamic nature of inertia weights (Fang *et al.*, 2022) and acceleration coefficients help regulate the balance between exploration and exploitation, ensuring that the algorithm effectively explores diverse regions of the search space while avoiding premature convergence to suboptimal solutions. Eq. 13 displays the key's updated location during the exploration stage. Eq. 14 depicts the calculation of dynamic inertia weight $W(t)$, wherein, T_{max} denotes the maximum number of iterations, t indicates the current iteration, and random value is denoted as b that vary dynamically around the value 1, which is expressed as per Eq. 15. Here, the normal distribution random number is denoted as r, maximum inertia weight is denoted as W_{max}, which is fixed as 0.9 and minimum inertia weight is denoted as W_{min}, which is fixed as 0.4.

$$\hat{X}_{i,j}^{P1} = X_{i,j} * W(t) + R_{i,j} \cdot (SA_{i,j} - T_{i,j} \cdot x_{i,j}) \quad (13)$$

$$W(t) = b * W_{max} \left[\frac{W_{max}}{W_{min}}\right]^{\left(\frac{t}{T_{max}}\right)} \quad (14)$$

$$b = 1 + 0.2 * r \quad (15)$$

c. Updated Mutation Strategy: Dynamic Coefficient Mutation and DE/Current to Best/3 Mutation Strategy: After the exploration phase, dynamic coefficient mutation involves dynamically adjusting mutation coefficients during the optimization process. The DE/Current to Best/3 mutation strategy (Fadhil *et al.*, 2023), tailored for key generation, mutates current solutions based on the difference between the current solution as well as the best solution among three randomly selected individuals. These mutation strategies aim to introduce diversity into the population of potential sanitization keys, enabling the technique to explore different regions of the key space and potentially discovering superior key configurations. Here, the dynamic coefficient mutation is based on the condition as per Eq. 16. The updated DE/Current to Best/3 mutation strategy is expressed in Eq. 17, wherein, the best solution is denoted as $\hat{X}_{best}$, the solution of current i_{th} position is denoted as $\hat{X}_i$, the uniform distribution random number (0,1) is denoted as F, the randomly selected individuals are denoted by $\hat{X}_{r1}$, $\hat{X}_{r2}$ and P denotes the mutation probability coefficient (Fang *et al.*, 2022), which is calculated as per Eq. 18.

$$\hat{X}_i(t+1) = \begin{cases} V_i(t) & if\ P > \text{ rand} \\ \hat{X}_i(t) & \text{else} \end{cases} \quad (16)$$

$$V_i(t) = \hat{X}_{best} + F * \left[\hat{X}_{best} - \hat{X}_i\right] + F * \left[\hat{X}_{r1} - \hat{X}_{r2}\right] \quad (17)$$

$$P = 0.2 + 0.5 * \left(\frac{t}{t_{max}}\right) \quad (18)$$

Eq. 19 updates the position of each lyrebird based on whether the objective function value for the new position is improved as compared to the current position. In the context of key generation, this could correspond to selecting key values that results in better sanitization efficacy or improved security. Here, $X^{\wedge}_{\mathrm{i}}$ represents the updated position (final generated key) in the exploration phase.

$$\hat{X}_i = \begin{cases} \hat{X}_i^{P1} & (O_F)_i^{P1} \le (O_F)_i \\ \hat{X}_i & \text{else} \end{cases} \quad (19)$$

d. Exploitation Phase of Imp-LOA: The Exploitation phase of Imp-LOA is tailored to update the positions of population members, which represents potential sanitization keys based on a strategy inspired by the movement behavior of lyrebirds seeking suitable hiding areas. This phase aims to exploit promising regions of the key space by making small adjustments to the positions of the keys. Eq. 20 computes a new position $x_{\mathrm{i}}^{\mathrm{P}_{\mathrm{j}}^{2}}$ for each lyrebird (or key) based on the hiding strategy, aiming to make small adjustments to the current position. The magnitude of the adjustment is influenced by random factors and the difference between the current position and the bounds of the key space, wherein, $x_{\mathrm{i}}^{\mathrm{P}_{\mathrm{j}}^{2}}$ represents the new position for the i_{th} encryption key in the j_{th} dimension, $R_{\mathrm{i,j}}$ represents the random numbers from interval [0,1], and u_{j}, l_{j} represent the upper and lower bounds for j_{th} dimension of the key space, respectively.

$$x_{i,j}^{P2} = x_{i,j} + (1 - 2R_{i,j}) \cdot \frac{u_j - l_j}{t} \quad (20)$$

After this, it is updated using dynamic coefficient mutation and DE/current to best/3 mutation strategy of Imp-LOA, which are already shown in Eqs. 16 to Eq. 18. Therefore, the final generated key is expressed by Eq. 21. If the new position yields an improved objective function value, indicating enhanced key quality, it replaces the current position; otherwise, the current position remains unchanged. The flowchart of Imp-LOA is shown in

Figure 3 and the hyperparameter settings are given in Table 1. This approach ensures that the algorithm effectively navigates the key space, gradually refining potential keys to better meet the optimization objectives, whether they pertain to security, efficiency, or other relevant criteria.

$$\hat{X}_i = \begin{cases} \hat{X}_i^{P2} & (O_F)_i^{P2} \leq (O_F)_i \\ \hat{X}_i & \text{else} \end{cases} \quad (21)$$

Table 1: Hyperparameter Settings of the Algorithm

Model	Hyperparameters
Imp-LOA	wmax=0.9; (Maximum Inertia Weight) wmin=0.4; (Minimum Inertia Weight) r=interval(0,1)

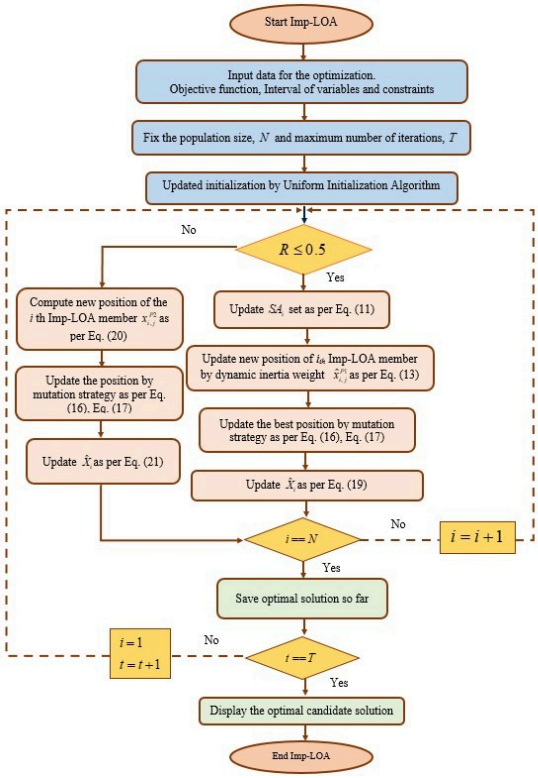


Fig. 3: Flowchart of Imp-LOA

Key Tuning Process using Improved SqueezeNet Model

Once the optimal keys are generated, the key tuning process is used to further enhance their effectiveness. Specifically, compared with the existing deep learning method, SqueezeNet is employed in the proposed privacy preservation model due to its lightweight architecture, efficiency, and effectiveness in deep learning-based feature extraction for the key tuning process. Additionally, SqueezeNet has a smaller model size and fewer parameters, which offers a balance between computational efficiency and performance, crucial for cloud environments. Despite its efficiency, the conventional SqueezeNet model suffers from the vanishing gradient problem and inefficient gradient propagation during training. This could slow down convergence and limit the model's ability to learn effectively in complex data distributions, as well as provide less stable training. In order to overcome the flaws found in the conventional SqueezeNet model, an improved SqueezeNet model is proposed in this research. This improved version enhances the model's ability to capture complex and non-linear patterns. The proposed activation function helps the model maintain a balance between efficiency and expressiveness, leading to improved training dynamics and higher model accuracy. Key tuning involves adjusting the parameters of the keys based on learned patterns and characteristics of the data. This fine-tuning process aims to optimize the keys for the specific dataset and the sanitization process being used, thereby improving overall security and efficiency.

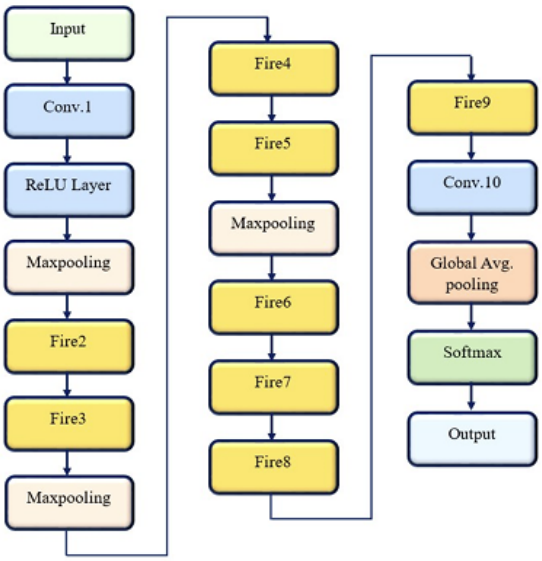


Fig. 4: Conventional SqueezeNet Architecture

The standard SqueezeNet architecture (Zia *et al.*, 2024) is a lightweight Convolutional Neural Network (CNN). It follows a sequence starting from a convolutional layer (Conv1) and concludes with a final convolutional layer (Conv10). In between, it incorporates fire modules, which consist of squeeze and expand layers. The squeeze layer comprises 1×1 convolutions to reduce the number of input channels, followed by expand layers that include a mix of 1×1 and 3×3 convolutions to capture both spatial and channel-wise information. Eight fire modules (Fire2 to Fire9), which are specialized units designed to efficiently extract features from input data, are incorporated. The network also employs max-pooling operations with a stride of 2 after Conv1, Fire3, Fire5, and Conv10, contributing to its computational efficiency and effective feature extraction. Additionally, a dropout layer with a 50% dropout ratio is applied after Fire9, enhancing the model's robustness against over-fitting. ReLU activation function is used in this network. Figure 4 shows the conventional SqueezeNet architecture.

However, in standard SqueezeNet, several key challenges emerge. Firstly, there is a perpetual struggle

DOI: 10.3844/jcssp.2025.1719.1740

between model size and performance, where achieving high accuracy with a compact architecture is challenging. In addition, Deeper networks are prone to over-fitting, especially when trained on limited data. Regularization techniques are essential to prevent overfitting.

The proposed SqueezeNet architecture introduces several enhancements to address challenges encountered in the standard architecture. Firstly, the incorporation of the TriSRA activation function enhances the model's capacity to capture complex patterns more effectively compared to the standard ReLU activation function. This improvement helps overcome the challenge of expressing intricate patterns in the data, thereby enhancing performance. The architecture of the improved SqueezeNet model is shown in Figure 5. According to this proposed model, TriSRA activation function is used, which incorporates smooth activation function like Swish (Ramachandran *et al.*, 2017), ReLU (Nwankpa *et al.*, 2018) and APTx (Kumar, 2022). By combining multiple activation functions, non-linearity to the model is introduced which enables the model to capture more complex patterns. Eq. 22 shows the proposed TriSRA activation function Z, which is based on ELU (Clevert *et al.*, 2016) and the average of the Swish function, the ReLU function, and the APTx activation function.

$$Z = \begin{cases} \alpha\left(e^{x}-1\right) & x < 0 \\ \frac{s(x)+r(x)+a(x)}{3} & x \geq 0 \end{cases} \tag{22}$$

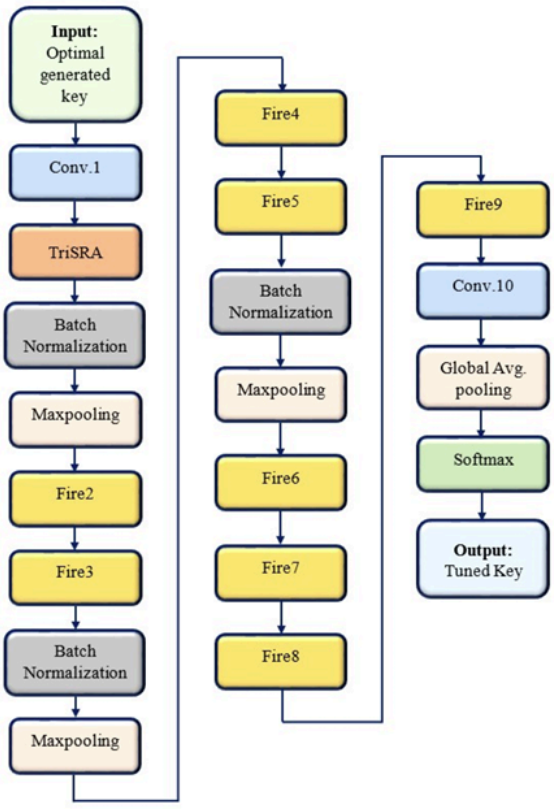


Fig. 5: Improved SqueezeNet Architecture

Here, $s(x)$ represents the Swish activation function, which is calculated as per Eq. 23. It introduces a non-linearity that is smoother than ReLU, potentially leading to improved training efficiency and generalization. The value of trainable parameter β is fixed as 0.1. ReLU activation function is represented by $r(x)$ and can be defined as per Eq. 24. It helps the network learn complex patterns by introducing non-linearity. $a(x)$ represents the APTx activation function, which is computed as per Eq. 25, where $\alpha_{aptx} = 1, \beta_{aptx} = 1, \gamma_{aptx} = 0.5$ It offers stability in training deep neural networks (improved SqueezeNet) by mitigating issues such as vanishing or exploding gradients.

$$s\left(x\right) = x.\text{sigmoid}\left(\beta x\right) \tag{23}$$

$$r\left(x\right) = max\left(0, x\right) \tag{24}$$

$$a\left(x\right) = \left(\alpha_{aptx} + \left(\tanh\left(\beta_{aptx} x\right)\right) * \gamma_{aptx} x \tag{25}$$

Algorithm 2 Pseudocode of Improved SqueezeNet Architecture

function SQUEEZENET
  Apply **Convolutional Layer** with 64 filters, 3×3 kernel and a stride of 2
  Apply **TriSRA Activation**
  Apply **Batch Normalization**
  Perform **Maxpooling** with a pool size of 3×3 and stride of 2
  Repeat for Fire Modules 2 to 9:
    if Module 3 or Module 5 **then**
      Apply **FIREMODULEUPDATED**
    else
      Apply **FIREMODULE**
    end if
  Apply **Dropout** with a rate of 0.5
  Apply **Convolutional Layer** with 10 filters, 3×3 kernel, and 'same' padding
  Apply **TriSRA Activation**
  Perform **Global Average Pooling**
  Apply **Softmax Activation**
  Return the output
end function
function FIREMODULE
  Apply **Squeeze Layer** with 1×1 convolutions
  Apply **TriSRA Activation**
  Apply **Expand Layer** with 1×1 convolutions
  Apply **TriSRA Activation**
  Apply **Expand Layer** with 3×3 convolutions
  Apply **TriSRA Activation**
  Concatenate the outputs of the two expand layers
  Return the concatenated tensor
end function
function FIREMODULEUPDATED
  Apply **Squeeze Layer** with 1×1 convolutions
  Apply **TriSRA Activation**
  Apply **Expand Layer** with 1×1 convolutions
  Apply **TriSRA Activation**
  Apply **Expand Layer** with 3×3 convolutions
  Apply **TriSRA Activation**
  Concatenate the outputs of the two expand layers
  Apply **Batch Normalization**
  Perform **Maxpooling** with a pool size of 3×3 and stride of 2
  Return the output after maxpooling
end function

DOI: 10.3844/jcssp.2025.1719.1740

Table 2: Hyperparameters of the Improved SqueezeNet

Model	Hyperparameters
Improved SqueezeNet	Activation Variables: $\alpha aptx = 1, \beta aptx = 1, \gamma aptx = 0.5$ Optimizer: Adam epoch: 50

Secondly, batch normalization layers are strategically integrated throughout the architecture to improve training convergence and mitigate over-fitting. This addresses the common challenge of overfitting in deeper networks like SqueezeNet, ensuring better generalization to unseen data. Batch normalization layers are strategically incorporated post-TriSRA activation in fire 3 and fire 5 modules to ensure stable and efficient training. By leveraging the combined benefits of the Swish, ReLU, and APTx activation functions within TriSRA, alongside batch normalization, the model aims to optimize key parameters effectively, enhancing the security and efficiency of the data sanitization process in the cloud environment. Table 2 and Algorithm 2 present the hyperparameter settings and pseudo code of the improved SqueezeNet, respectively.

Kronecker Product

In the data sanitization phase, Kronecker product operations are executed between keys to augment the security of the sanitization process. By performing Kronecker product operations between keys, additional complexity and randomness are introduced into the sanitization mechanism, bolstering its resistance against unauthorized access and cryptographic attacks. This process enhances the robustness of the process utilized during data sanitization, thereby fortifying the protection of sensitive information stored or transmitted within cloud environments. Through the strategic application of Kronecker product operations between keys, the model ensures a heightened level of security in safeguarding data privacy in cloud computing infrastructures.

Data Restoration

The data restoration phase plays a crucial role in the proposed privacy preservation model, as it facilitates the reversion of sanitized data to its original state, enhancing flexibility and usability. This phase ensures that, despite undergoing sanitization for privacy protection, the data remains accessible and usable for authorized purposes when necessary. By utilizing the tuned key to decrypt the sanitized sensitive material, the data restoration approach entails reversing the data sanitization process. Firstly, the tuned key and the sanitized data are binarized, and after that, an XOR operation is performed. The restored database is the result of this process, which successfully retrieves the original data. This procedure ensures the confidentiality and safety of the data during its transmission while enabling recipients on the other side of the cloud to safely recover and use the sensitive information of the data owners.

Results and Discussion

Simulation Procedure

The proposed cloud privacy preservation model has been implemented and simulated using MATLAB version R2021b. The simulation was executed on a processor with an 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.42 GHz, and the system was equipped with 16.0 GB of installed RAM. Three testcases i.e. testcase1, testcase2, and testcase3 are created by applying variations of 10, 20, and 30% on the heart disease dataset (Janosi *et al.*, 1988) to analyze the performance of proposed model, respectively.

Performance Analysis

A comprehensive analysis was conducted to evaluate the efficacy of both proposed (Imp-LOA + Improved-SqueezeNet) and conventional approaches in cloud privacy preservation. This thorough examination encompassed critical metrics such as data preservation ratio, key sensitivity, hiding ratio, privacy, modification degree, sanitization, and restoration effectiveness. Additionally, the evaluation integrated statistical analysis and convergence analysis. Moreover, CPA and KPA attack analyses were performed to assess resilience against security threats. The Imp-LOA + Improved-SqueezeNet method's performance was contrasted against state-of-the-art techniques like CIAO-TME (Patil and HimaBindu, 2023) and G-BHO (Kumar *et al.*, 2023), and PSO-GWO (Rahman *et al.*, 2024) as well as established methods including COA, OOA, RPO, LOA, NBO, Bi-LSTM, DCNN, S-NET, ResNET, and KNN.

Furthermore, it was compared with method LSTM+MUAOA (Sharma and Tyagi, 2024) and DeepMaxout (Dhamdhere *et al.*, 2025). Both Imp-LOA + Improved-SqueezeNet and conventional methods were analyzed using the Cleveland dataset, providing valuable insights into their effectiveness in the cloud privacy preservation.

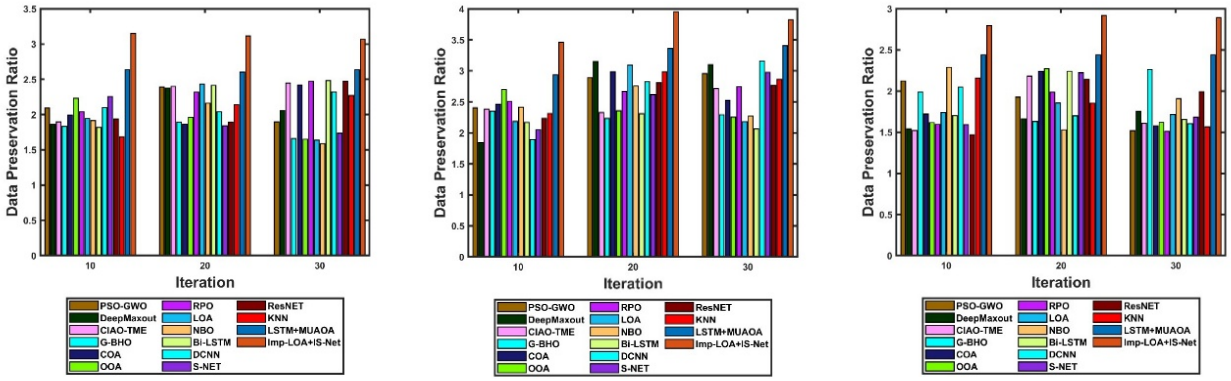
Analysis of Data Preservation Ratio

The data preservation ratio quantifies the proportion of original data retained over time, reflecting the effectiveness of preservation efforts. It measures the percentage of data preserved compared to the total amount initially present, essential for maintaining data integrity and accessibility in various domains, from research to information technology. Figure 6 illustrates the analysis of data preservation ratio comparing the proposed method with conventional approaches for cloud privacy preservation across three distinct testcases. The Imp-LOA + Improved-SqueezeNet method exhibits an increasing trend in data preservation ratio across iterations, with values ranging from 3.148 at 10^{th} iteration to 3.065 at 30^{th} iteration for testcase1. Notably, at iteration 10, the Imp-LOA + Improved-SqueezeNet

method outperforms most conventional methods, including PSO-GWO (Rahman *et al.*, 2024) (2.093), DeepMaxout (Dhamdhere *et al.*, 2025) (1.863), CIAO-TME (Patil and HimaBindu, 2023) (1.896), G-BHO (Kumar *et al.*, 2023) (1.831), COA (1.991), OOA (2.231), RPO (2.041), LOA (1.944), NBO (1.913), Bi-LSTM (1.820), DCNN (2.102), S-NET (2.258), ResNET (1.938), KNN (1.685), and also LSTM+MUAOA (Sharma and Tyagi, 2024) (2.635). The Imp-LOA + Improved-SqueezeNet method demonstrates a preservation ratio of 2.892 for tesetcase3. Despite variations in performance among conventional methods, the Imp-LOA + Improved-SqueezeNet method consistently outperforms them, emphasizing its effectiveness in preserving cloud privacy in testcase3 at the 30th iteration. The comparison reveals the Imp-LOA + Improved-SqueezeNet method's superiority in achieving higher preservation ratios, highlighting its potential for robust and secure cloud privacy preservation. This underscores the significance of continual advancements in data preservation techniques to address evolving privacy challenges in cloud computing environments.

Analysis on Hiding Ratio

The hiding ratio quantifies the proportion of sensitive data exposed relative to the total dataset. It serves as a measure of the effectiveness of hiding or obscuring sensitive data, with a lower ratio indicating greater successful concealment, typically employed in contexts prioritizing privacy and confidentiality. In Figure 7, the hiding ratio analysis is presented, comparing the Imp-LOA + Improved-SqueezeNet scheme with traditional strategies for cloud privacy preservation. It examines three distinct testcases across iterations (5, 10, 15, 20, 25, and 30). Minimized hiding ratio ratings are essential for effective privacy preservation in the cloud, highlighting the scheme's efficacy in concealing sensitive information. The hiding ratio analysis for testcase2 reveals significant insights into the effectiveness of the Imp-LOA + Improved-SqueezeNet scheme compared to traditional strategies for cloud privacy preservation. Initially, at iteration 5, the Imp-LOA + Improved-SqueezeNet scheme demonstrates exceptional performance with a hiding ratio of 0, indicating highly successful concealment of sensitive information. Although some conventional methods such as PSO-GWO (Rahman *et al.*, 2024) (0.0604), COA (0.0761), NBO (0.1029), DeepMaxout (Dhamdhere *et al.*, 2025) (0.1029), and OOA (0.1051) exhibit slightly higher ratios, the proposed scheme stands out for its ability to minimize the hiding ratio effectively. As the analysis progresses through iterations 10 to 30, the Imp-LOA + Improved-SqueezeNet scheme maintains its superiority with consistently low hiding ratio. This trend underscores its reliability in preserving privacy within cloud environments. Notably, the proposed scheme outperforms conventional methods, including CIAO-TME (Patil and HimaBindu, 2023), G-BHO (Kumar *et al.*, 2023), COA, OOA, RPO, LOA, NBO, Bi-LSTM, DCNN, S-NET, ResNET, KNN, PSO-GWO (Rahman *et al.*, 2024), DeepMaxout (Dhamdhere *et al.*, 2025), and LSTM+MUAOA (Sharma and Tyagi, 2024) across all iterations, emphasizing its effectiveness in concealing sensitive data. Overall, the findings highlight robustness of Imp-LOA + Improved-SqueezeNet scheme in achieving the minimized hiding ratio, essential for ensuring the cloud privacy preservation.



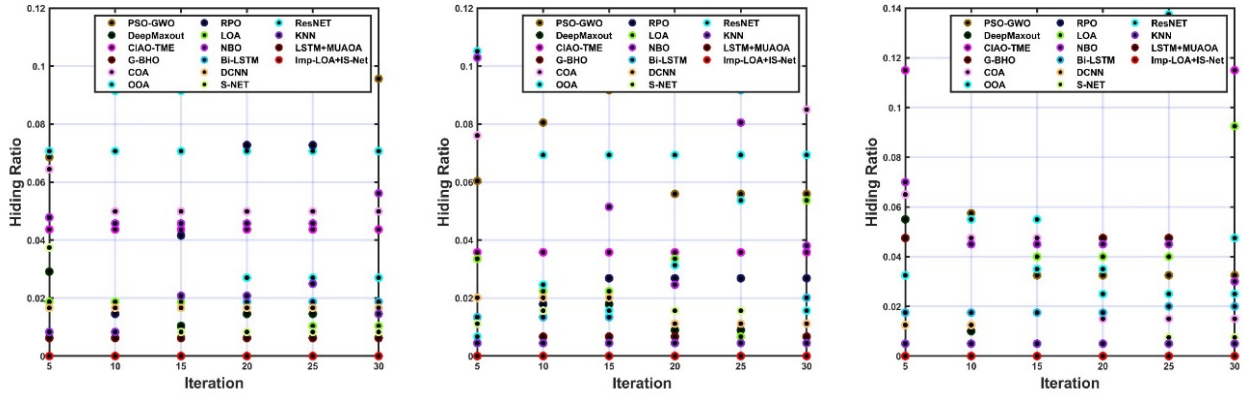
(a) (b) (c)

Fig. 6: Data Preservation Analysis of Imp-LOA+Improved-SqueezeNet and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3

Analysis on Key Sensitivity

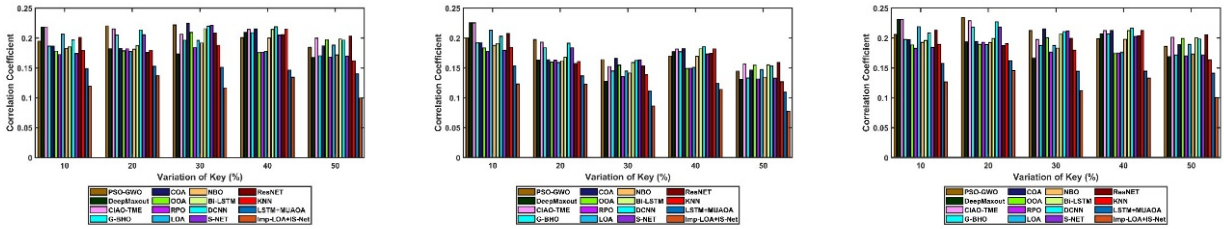
Key sensitivity denotes how responsive a system is to changes in critical factors, guiding optimization by identifying pivotal variables crucial for performance. Figure 8 illustrates the key sensitivity analysis comparing Imp-LOA + Improved-SqueezeNet and conventional methodologies across variations of key factors (10, 20, 30, 40, and 50%). Reducing key sensitivity values is imperative to ensure robust privacy

preservation in cloud environments. Initially, at 10% variation, CIAO-TME (Patil and HimaBindu, 2023), G-BHO (Kumar *et al.*,2023), COA, OOA, RPO, LOA, NBO, LSTM-MUAOA (Sharma and Tyagi, 2024), PSO-GWO (Rahman *et al.*, 2024), and DeepMaxout (Dhamdhere *et al.*, 2025) exhibit sensitivity values of 0.231, 0.198, 0.197, 0.188, 0.182, 0.219, 0.192, 0.158, 0.213, and 0.231, respectively, while the Imp-LOA + Improved-SqueezeNet scheme showcases a notably lower sensitivity of 0.127 (testcase3), indicating its superior adaptability to key variations. As the variation increases, the proposed scheme consistently maintains lower sensitivity values compared to conventional methods, emphasizing its robustness in preserving the cloud privacy effectively. At 50% variation, the Imp-LOA + Improved-SqueezeNet scheme achieves the lowest sensitivity of 0.100, underscoring its efficacy in mitigating the impact of key variations on privacy preservation.



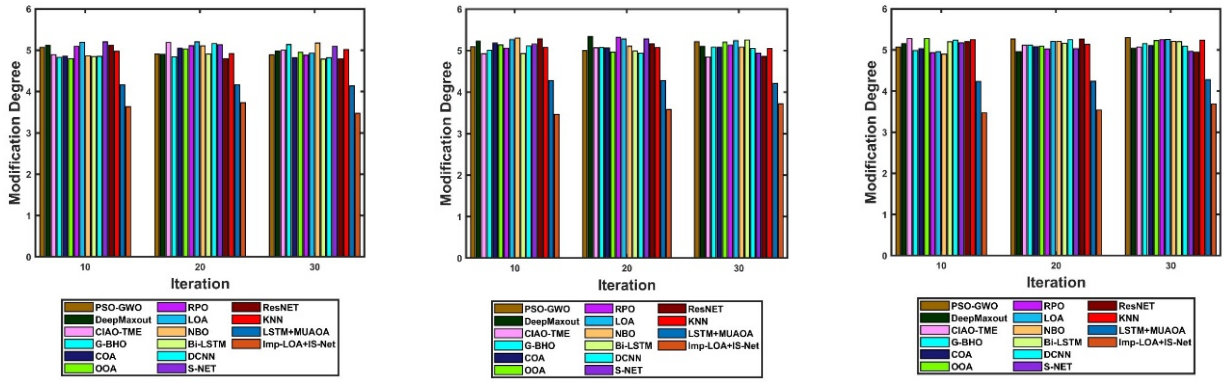
(a) (b) (c)

Fig. 7: Hiding Ratio Analysis of Imp-LOA+Improved-SqueezeNet and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3



(a) (b) (c)

Fig. 8: Key Sensitivity Analysis of Imp-LOA+Improved-SqueezeNet and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3

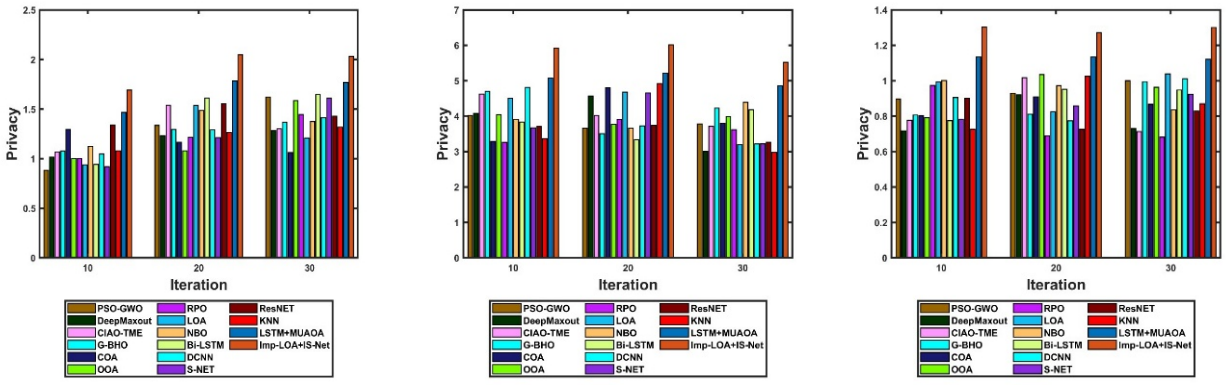


(a) (b) (c)

Fig. 9: Modification Degree Analysis of Imp-LOA+Improved-SqueezeNet and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3

Analysis on Modification Degree

Modification degree quantifies the extent of alterations made to an item or system from its original state. It measures the magnitude of changes relative to the initial condition, aiding in assessing the effectiveness of modifications. Figure 9 illustrates the analysis of modification degree, contrasting the Imp-LOA + Improved-SqueezeNet approach with conventional methods for cloud privacy preservation. Effective privacy preservation in the cloud requires minimizing the modification degree. Across all testcases, the Imp-LOA + Improved-SqueezeNet scheme consistently exhibits a minimized modification degree compared to conventional strategies. In testcase1, the modification degree analysis reveals pertinent differences among methodologies examined for cloud privacy preservation across iterations. At iteration 10, the Imp-LOA + Improved-SqueezeNet scheme demonstrates a significantly lower modification degree of 3.632 compared to conventional methods, such as CIAO-TME (Patil and HimaBindu, 2023) (4.897), G-BHO (Kumar *et al.*, 2023) (4.830), COA (4.856), OOA (4.797), RPO (5.095), LOA (5.193), NBO (4.87), LSTM+MUAOA (Sharma and Tyagi, 2024) (4.164), PSO-GWO (Rahman *et al.*, 2024) (5.062), and DeepMaxout (Dhamdhere *et al.*, 2025) (5.119). This trend persists throughout subsequent iterations, with the Imp-LOA + Improved-SqueezeNet scheme consistently exhibiting lower modification degrees compared to other conventional methods such as OOA, RPO, LOA, NBO, Bi-LSTM, DCNN, S-NET, ResNET, KNN, at LSTM+MUAOA, PSO-GWO, and DeepMaxout. For instance, iteration 30, the Imp-LOA + Improved-SqueezeNet scheme maintains a modification degree of 3.475, contrasting with higher values observed in several other conventional methods. Through meticulous analysis across varied testcases and iterations, it becomes evident that the proposed method consistently achieves lower modification degrees. This signifies its proficiency in minimizing alterations to sensitive data, crucial for maintaining data integrity and confidentiality in cloud environments. The findings accentuate the importance of adopting advanced techniques, such as the Imp-LOA + Improved-SqueezeNet method, to mitigate unauthorized modifications and uphold robust privacy standards in cloud computing.



(a) (b) (c)

Fig. 10: Privacy Analysis of Imp-LOA+Improved-SqueezeNet and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3

Analysis on Privacy

In Figure 10, the privacy assessment of the Imp-LOA + Improved-SqueezeNet methodology is done in contrast with the conventional methodologies for cloud privacy preservation. Privacy ratings serve as crucial indicators of the effectiveness of privacy measures, with higher values signifying superior protection of sensitive data within cloud environments. The comprehensive analysis of privacy ratings across iterations offers valuable insights into the efficacy of diverse methodologies for cloud privacy preservation. The Imp-LOA + Improved-SqueezeNet model achieves a privacy rating of 2.031 for testcase1, surpassing other conventional methods such as CIAO-TME (Patil and HimaBindu, 2023) (1.302), G-BHO (Kumar *et al.*, 2023) (1.368), COA (1.062), OOA (1.584), RPO (1.445), LOA (1.207), NBO (1.375), Bi-LSTM (1.674), DCNN (1.414), S-NET (1.611), ResNET (1.428), KNN (1.316), LSTM+MUAOA (Sharma and Tyagi, 2024) (1.767), PSO-GWO (Rahman *et al.*, 2024) (1.622), and DeepMaxout (Dhamdhere *et al.*, 2025) (1.283). This significant difference underscores the potential of the Imp-LOA + Improved-SqueezeNet approach to offer heightened privacy protection compared to traditional strategies. Similarly, the proposed scheme attains higher privacy ratings of 6.01 for testcase2 and 1.272 for testcase3 at iteration 20, indicative of its persistent efficacy in safeguarding privacy within cloud environments.

Convergence Analysis

Figure 11 presents a comprehensive convergence analysis contrasting the Imp-LOA method with CIAO-

DOI: 10.3844/jcssp.2025.1719.1740

TME (Patil and HimaBindu, 2023), G-BHO (Kumar *et al.*, 2023), COA, OOA, RPO, LOA, NBO and PSO-GWO (Rahman *et al.*, 2024) across three distinct test cases for cloud privacy preservation. This evaluation spans iteration counts from 0 to 30, aiming to determine models offering minimized cost ratings alongside faster convergence rates for effective cloud privacy preservation. While evaluating all testcases, initial iterations yielded higher cost values for all models, gradually decreasing with iteration advancement. Notably, the Imp-LOA approach consistently outperformed conventional methods by achieving the lowest cost values across all testcases. In testcase1, the Imp-LOA scheme achieved a minimized cost rate of 5.279 at the 30th iteration. In comparison, CIAO-TME, G-BHO, COA, OOA, RPO, LOA, NBO and PSO-GWO attained cost rates of 5.528, 5.547, 5.495, 5.445, 5.308, 5.362, 5.474, and 5.363 respectively. Likewise, in the other two test cases, the Imp-LOA approach exhibited minimum cost values compared to the conventional methods. Through rigorous assessment across multiple testcases and iterations, it is evident that the Imp-LOA method exhibits quicker convergence and lower cost ratings compared to conventional methods. This underscores its efficiency in achieving convergence towards optimal solutions, essential for enhancing privacy and security in cloud environments.

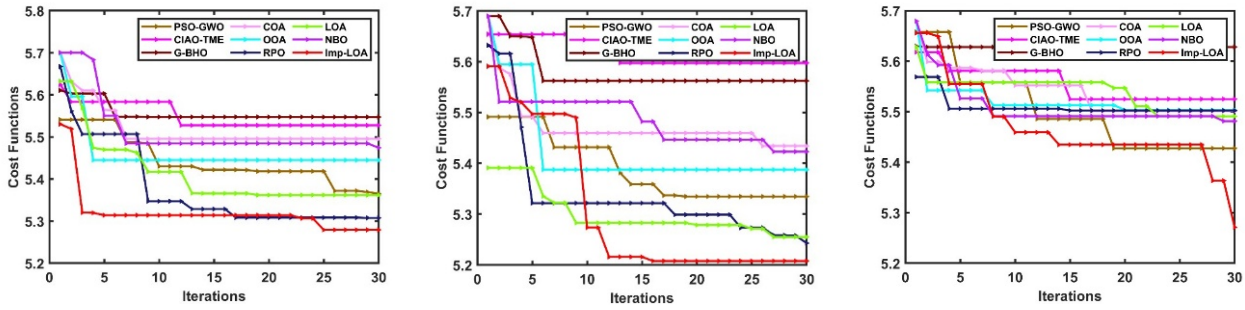


Fig. 11: Convergence Analysis of Imp-LOA and Conventional Methods for (a) Testcase1, (b) Testcase2, and (c) Testcase3

Sanitization Analysis

Sanitization involves removing sensitive data to make information safe for public release or use, protecting privacy and security by minimizing the risk of unauthorized access or disclosure. Table 3 provides a detailed overview of the sanitization analysis conducted on Imp-LOA + Improved-SqueezeNet and conventional methodologies for cloud privacy preservation across three distinct testcases. Across all the testcases, various sanitization methods were evaluated based on their correlation values, with lower correlations indicating more effective sanitization. In testcase1, the Imp-LOA + Improved-SqueezeNet method demonstrated a correlation of 0.101, surpassing conventional methods. Similarly, in testcase2 and testcase3, the proposed method exhibited the lowest correlation of 0.067 and 0.086, respectively, again outperforming all other methods. The correlation values of the conventional methods, such as LSTM+MUAOA (Sharma and Tyagi, 2024), PSO-GWO (Rahman *et al.*, 2024), DeepMaxout (Dhamdhere *et al.*, 2025), COA, G-BHO, ResNet, DCNN, and Bi-LSTM, are 0.108, 0.143, 0.161, 0.143, 0.150, 0.127, 0.136, and 0.142 for testcase3. This result demonstrates the strength of the proposed approach in minimizing the resemblance between original and sanitized data, which is critical for protecting privacy in the cloud environments. These comprehensive comparative findings highlight the consistent superiority of the Imp-LOA + Improved-SqueezeNet method in achieving effective sanitization across all testcases, underscoring its pivotal role in ensuring robust privacy and security measures by minimizing the risk of unauthorized access or disclosure.

Table 3: Sanitization Analysis of Proposed and Conventional Schemes

Methods	Testcase1	Testcase2	Testcase3
PSO-GWO	0.172	0.098	0.143
DeepMaxout	0.167	0.116	0.161
CIAO-TME	0.172	0.105	0.142
G-BHO	0.142	0.118	0.150
COA	0.158	0.114	0.143
OOA	0.152	0.118	0.130
RPO	0.139	0.110	0.132
LOA	0.157	0.094	0.130
NBO	0.175	0.096	0.159
Bi-LSTM	0.157	0.122	0.142
DCNN	0.146	0.108	0.136
S-NET	0.143	0.122	0.130
ResNET	0.142	0.120	0.127
KNN	0.159	0.104	0.130
LSTM+MUAOA	0.117	0.083	0.108
Proposed	0.101	0.067	0.086

Restoration Analysis

Restoration refers to the process of recovering data or systems to their original state or condition following breaches, data loss, or unauthorized access, aiming to ensure the continued integrity and confidentiality of

sensitive information stored or processed in cloud environments. Table 4 presents the correlation values for restoration analysis across all testcases. Higher correlation value indicates better restoration performance. In testcase1, the Imp-LOA + Improved-SqueezeNet method achieved a high correlation of 0.959, surpassing conventional methods, like CIAO-TME (Patil and HimaBindu, 2023) (0.849) and COA (0.872), while also outperforming LSTM+MUAOA (Sharma and Tyagi, 2024) (0.956), PSO-GWO (Rahman *et al.*, 2024) (0.834), and DeepMaxout (Dhamdhere *et al.*, 2025) (0.844). Similarly, in testcase2, the Imp-LOA + Improved-SqueezeNet method exhibited superior restoration effectiveness with a correlation of 0.964, surpassing LSTM+MUAOA (0.962), PSO-GWO (0.874), DeepMaxout (0.833) and other traditional methods, like RPO (0.911) and ResNet (0.840). In testcase3, the proposed method maintained its dominance with a correlation of 0.999, showcasing its effectiveness over LSTM+MUAOA (0.995) and other conventional methods, like PSO-GWO (0.937), DeepMaxout(0.801), G-BHO (Kumar *et al.*, 2023) (0.909), COA (0.939), OOA(0.851), LOA (0.939), ResNET (0.921), Bi-LSTM (0.894), and DCNN (0.830). These results demonstrate the effectiveness of the proposed framework in accurately recovering the sanitized data with minimal information loss. Overall, these findings highlight the consistent superiority of the Imp-LOA + Improved-SqueezeNet method in achieving effective restoration across all testcases, underscoring its crucial role in maintaining data integrity and confidentiality within cloud environments.

Table 4: Restoration Analysis of Proposed and Conventional Schemes

Methods	Testcase1	Testcase2	Testcase3
PSO-GWO	0.834	0.874	0.937
DeepMaxout	0.844	0.833	0.801
CIAO-TME	0.849	0.884	0.874
G-BHO	0.876	0.774	0.909
COA	0.872	0.858	0.939
OOA	0.900	0.770	0.851
RPO	0.862	0.911	0.860
LOA	0.788	0.840	0.939
NBO	0.864	0.782	0.801
Bi-LSTM	0.884	0.785	0.894
DCNN	0.810	0.866	0.830
S-NET	0.862	0.908	0.878
ResNET	0.851	0.840	0.921
KNN	0.836	0.883	0.871
LSTM+MUAOA	0.956	0.962	0.995
Proposed	0.959	0.964	0.999

CPA and KPA Analysis

The CPA analysis, conducted to evaluate the resilience of Imp-LOA + Improved-SqueezeNet and conventional methods across three testcases, is illustrated in Table 5. Across all testcases, the proposed method consistently exhibited lower CPA scores compared to conventional methods, indicating its enhanced resistance against chosen-plaintext attacks. In testcase1, the Imp-LOA + Improved-SqueezeNet method achieved a CPA score of 0.104, notably lower than competing methods, such as CIAO-TME (Patil and HimaBindu, 2023) (0.164), G-BHO (Kumar *et al.*, 2023) (0.168), PSO-GWO (Rahman *et al.*, 2024) (0.168), DeepMaxout (Dhamdhere *et al.*, 2025) (0.164), and LSTM+MUAOA (Sharma and Tyagi, 2024) (0.120). In testcase2, the Imp-LOA+ Improved-SqueezeNet method demonstrated exceptional resilience with a CPA score of 0.021, outperforming all other methods. Similarly, in testcase3, it maintained its superiority with a CPA score of 0.101, showcasing its robustness against CPA attacks compared to other conventional methods. The KPA analysis, performed to assess the susceptibility of Imp-LOA + Improved-SqueezeNet and conventional methods to known-plaintext attacks across all testcases, is summarized in Table 6. In testcase1, the Imp-LOA + Improved-SqueezeNet method exhibited a notably lower KPA score of 0.101, compared to CIAO-TME (Patil and HimaBindu, 2023) (0.146), G-BHO (Kumar *et al.*, 2023) (0.151), and other conventional methods. This suggests that the Imp-LOA + Improved-SqueezeNet method offers better resilience against known-plaintext attacks.

Table 5: CPA Analysis of Proposed and Conventional Schemes

Methods	Testcase1	Testcase2	Testcase3
PSO-GWO	0.168	0.034	0.163
DeepMaxout	0.164	0.031	0.156
CIAO-TME	0.164	0.033	0.158
G-BHO	0.168	0.034	0.162
COA	0.167	0.034	0.161
OOA	0.152	0.031	0.147
RPO	0.162	0.033	0.157
LOA	0.161	0.033	0.156
NBO	0.160	0.033	0.154
Bi-LSTM	0.164	0.034	0.159
DCNN	0.165	0.034	0.159
S-NET	0.157	0.032	0.152
ResNET	0.153	0.031	0.148
KNN	0.167	0.034	0.161
LSTM+MUAOA	0.120	0.029	0.129
Proposed	0.104	0.021	0.101

Similarly, in test case 2, the Imp-LOA+ Improved-SqueezeNet method displayed superior resistance with a KPA score of 0.021, outperforming competing methods like LSTM+MUAOA (Sharma and Tyagi, 2024) (0.024), and in testcase3, it again showcased its robustness with a KPA score of 0.098, surpassing all conventional methods, including PSO-GWO (Rahman *et al.*, 2024) (0.145), and DeepMaxout (Dhamdhere *et al.*, 2025) (0.140), and highlighting its efficacy in mitigating known-plaintext attacks.

Table 6: KPA Analysis of Proposed and Conventional Schemes

Methods	Testcase1	Testcase2	Testcase3
PSO-GWO	0.150	0.031	0.145
DeepMaxout	0.145	0.030	0.140
CIAO-TME	0.146	0.030	0.141
G-BHO	0.151	0.031	0.146
COA	0.152	0.031	0.147
OOA	0.147	0.030	0.142
RPO	0.157	0.032	0.151
LOA	0.148	0.030	0.143
NBO	0.152	0.031	0.147
Bi-LSTM	0.149	0.031	0.145
DCNN	0.155	0.032	0.150
S-NET	0.154	0.031	0.149
ResNET	0.154	0.032	0.149
KNN	0.148	0.030	0.144
LSTM+MUAOA	0.116	0.024	0.112
Proposed	0.101	0.021	0.098

Analysis of CPA and KPA in terms of Encryption Algorithms

Tables 7 and 8 demonstrate the security analysis of the proposed model against CPA and KPA compared to conventional encryption methods such as RSA and AES, in terms of correlation coefficient. As shown in Table 7, the Imp-LOA + Improved-SqueezeNet model consistently achieved the lowest correlation coefficients of 0.104, 0.021, and 0.101 against CPA analysis for testcases 1, 2, and 3, respectively. In contrast, RSA and AES yield higher values across the same testcases, with RSA recording 0.122, 0.029, and 0.198, while AES reporting 0.162, 0.033, and 0.157. The results indicate a reduced statistical relationship between plaintext and ciphertext with the proposed model.

Table 7: CPA Analysis of Proposed and Conventional Encryption Schemes

Methods	Testcase1	Testcase2	Testcase3
Proposed	0.104	0.021	0.101
RSA	0.122	0.029	0.198
AES	0.162	0.033	0.157

Table 8: KPA Analysis of Proposed and Conventional Encryption Schemes

Methods	Testcase1	Testcase2	Testcase3
Proposed	0.101	0.021	0.098
RSA	0.122	0.026	0.130
AES	0.150	0.031	0.145

Similarly, in the KPA analysis shown in Table 8, the proposed model maintained lower correlation coefficients of 0.101, 0.021, and 0.098 for testcases 1, 2, and 3, respectively. RSA and AES, on the other hand, yield 0.122 and 0.150 for testcase1, 0.026 and 0.031 for testcase2, and 0.130 and 0.145 for testcase3, respectively. These lower coefficients in both attack scenarios confirm that the proposed model makes it more difficult for the attacker to infer the original data. The performance improvement is primarily due to the advanced key generation with the Imp-LOA and adaptive key tuning through the improved SqueezeNet architecture, which collectively increase the privacy of cloud data.

Statistical Analysis on Fitness

The statistical analysis of Imp-LOA and conventional methods with a focus on fitness function parameters, such as the best, worst, mean, median, and standard deviation, is presented in Table 9. This comparison includes the Imp-LOA method alongside CIAO-TME (Patil and HimaBindu, 2023), G-BHO (Kumar *et al.*, 2023), COA, OOA, RPO, LOA, NBO, and PSO-GWO (Rahman *et al.*, 2024) for a thorough assessment. The Imp-LOA method demonstrated competitive fitness across all metrics, with a fitness score of 5.321 at the mean statistical metric, which is comparable to or better than most conventional methods, such as CIAO-TME (5.549), G-BHO (5.557), COA (5.519), OOA (5.463), RPO (5.376), LOA (5.413), NBO (5.517), and PSO-GWO (5.444). The Imp-LOA method obtained the lowest fitness score of 5.279 (best statistical metric), showcasing its competitive performance relative to other conventional methods such as CIAO-TME (5.528), G-BHO (5.547), COA (5.495), OOA (5.445), RPO (5.308), LOA (5.362), NBO (5.474), and PSO-GWO (5.365). The overall results demonstrate that the proposed method shows exceptional performance over the existing metaheuristic algorithms.

Table 9: Statistical Assessment in terms of Fitness

Methods	Best	Worst	Mean	Median	Standard Deviation
Imp-LOA	5.279	5.530	5.321	5.314	0.057
PSO-GWO	5.365	5.541	5.444	5.422	0.058
CIAO-TME	5.528	5.624	5.549	5.528	0.030
G-BHO	5.547	5.611	5.557	5.548	0.022
COA	5.495	5.700	5.519	5.495	0.052
OOA	5.445	5.700	5.463	5.445	0.059
RPO	5.308	5.667	5.376	5.329	0.101
LOA	5.362	5.632	5.413	5.366	0.079
NBO	5.474	5.700	5.517	5.484	0.074

Ablation Study

Ablation analysis is a technique used to assess the contribution of individual components in a model by systematically altering or removing certain features. In this study, the proposed Imp-LOA + Improved-SqueezeNet model is compared against model with statistical features and conventional entropy feature, model with statistical features and skewness features, model with statistical features and kurtosis features, model with conventional LOA, and the model with conventional SqueezeNet, to understand their effectiveness in privacy preservation presented in Table 10. The results show that the proposed model outperforms all other models in terms of privacy (2.031)

and DPR (3.065), indicating its strong ability to restore original data while maintaining privacy and security. On the other hand, model with statistical and conventional entropy features, model with statistical and skewness features, model with statistical and kurtosis features, model with conventional LOA, and model with conventional SqueezeNet exhibit lower privacy values of 1.429, 1.299, 1.454, 1.207, and 1.611, respectively. Moreover, the proposed model acquires better values of modification degree and sanitization effectiveness of 3.475 and 0.101, respectively, which is superior to the results of other models. Overall, the proposed model offers the best balance for privacy preservation and data restoration as compared to other models.

Table 10: Ablation Analysis of the Proposed Imp-LOA + Improved SqueezeNet Model and the Model with Statistical Features and Conventional Entropy Feature, Model with Statistical Features and Skewness Features, Model with Statistical Features and Kurtosis Features, Model with Conventional LOA, and the Model with Conventional SqueezeNet

Measures	Model with Statistical Features + Conventional Entropy Feature	Model with Statistical Features + Skewness Features	Model with Statistical Features + Kurtosis Features	Model with Conventional LOA	Model with Conventional SqueezeNet	Imp-LOA + IS-Net Model
Sanitization Effectiveness	0.144	0.157	0.169	0.157	0.143	0.101
Restoration Effectiveness	0.835	0.814	0.813	0.788	0.862	0.959
Hiding Ratio	0.011	0.239	0.24	0.01	0.008	0
Data Preservation Ratio	1.758	2.191	2.326	1.635	1.736	3.065
Privacy	1.429	1.299	1.454	1.207	1.611	2.031
Modification Degree	4.986	5.033	4.426	4.926	5.095	3.475

Table 11: Parametric Analysis of the Proposed Model

Parameter (random value) Variation	Hiding Ratio	Data Preservation Ratio	Privacy	Modification Degree
0.2	0	3.157	2.008	3.633
0.4	0	4.048	5.657	3.546
0.6	0	2.876	1.336	3.508

Table 12: Computational Time Analysis of Proposed and Conventional Schemes

Models	Computational Time (s) Models		
	Testcase1	Testcase2	Testcase3
Proposed	14.659	12,257	10.569
PSO-GWO	20.234	17.831	19.21
DeepMaxout	24.805	15.699	15.097
CIAO-TME	20.411	17.541	12.568
G-BHO	30.663	29.673	22.665
COA	22.234	20.678	18.654
OOA	29.298	26.584	25.688
RPO	32.091	35.688	28.561
LOA	19.023	16.547	12.659
NBO	19.675	15.359	12.557
Bi-LSTM	16.007	13.833	12.849
DCNN	19.877	13.877	13.137
S-NET	17.562	17.086	14.152
ResNET	16.122	15.926	13.507
KNN	16.045	15.64	12.059

Parametric Analysis

The analysis of parameter variation for the Imp-LOA + Improved-SqueezeNet model, presented in Table 11, provides valuable insights into the impact of different parameter settings on the performance of the model, specifically in terms of HR, DPR, Privacy, and MD. In this case, the parameter being varied is the random value used in equations (13) to (15), which seems to influence the model's behavior in terms of these key metrics. The random values are varied as 0.2, 0.4, and 0.6. HR and MD should be minimum, whereas DPR and privacy should be maximum for an optimum solution. The results show that with the parameter value 0.4, the proposed model generates better outcomes for DPR, MD, and privacy than other two values. However, MD continued to attain better outcome at 0.6 value also, but privacy and DPR are not as good as at 0.2 and 0.4 values. Overall, this analysis illustrates a clear trade-off between privacy and data integrity for the cloud data.

Analysis of Computational Time

Computational time refers to the total amount of time an algorithm takes to complete a specific task. The computational time analysis, presented in Table 12, highlights the efficiency of the Imp-LOA + Improved-SqueezeNet model compared to other state-of-the-art and traditional models. Across all test cases, the proposed model consistently demonstrates the lowest computational time, performing significantly faster than many of the alternative models. For testcase1, the computational time for proposed model is 14.659s, notably faster than CIAO-TME (20.411s), G-BHO (30.663s), COA (22.234s), OOA (29.298s), LOA (19.023s), NBO (19.675s), Bi-LSTM (16.007s), DCNN

(19.877s), S-NET (17.562s), ResNET (16.122s), KNN (16.045s), PSO-GWO (20.234s) and DeepMaxout (24.805s). Similarly, for testcase2 and testcase3, Imp-LOA + Improved-SqueezeNet maintains minimum computing times of 12.257s and 10.569s, respectively, outperforming models like PSO-GWO, DeepMaxout Bi-LSTM, DCNN, ResNET, RPO, G-BHO, and OOA. These results highlight the efficiency of the proposed model that provides high performance without excessive computational overhead, further strengthening its position as an effective solution for cloud-based privacy preservation.

Conclusion

In conclusion, this paper presented a comprehensive privacy preservation model tailored specifically for cloud environments, with a focus on safeguarding sensitive medical data related to heart disease. Through meticulous data acquisition, normalization, feature extraction, sanitization, and restoration phases, the suggested model ensures the security, privacy, and utility of the data while leveraging innovative techniques such as optimal key generation by using Imp-LOA and Improved SqueezeNet-based key tuning. By addressing optimization objectives including hiding ratio, data preservation ratio, privacy, and modification degree, the model offers a holistic approach to privacy preservation. MATLAB-based simulations and investigational analyses demonstrate the efficacy of the model with respect to security, time efficiency, and other pertinent metrics, showcasing its superiority in safeguarding privacy in cloud computing environments. Overall, this paper marks a significant advancement in privacy-preserving techniques within cloud computing, with implications for enhancing healthcare data security and facilitating the adoption of cloud-based solutions in the medical domain. However, the proposed approach has some limitations, as the employed Cleveland dataset has only clinical features, focusing on the tissues of the heart by analyzing radiomics features like pericoronary adipose tissue and thoracic and epicardial subcutaneous fat texture, and has a limited count of samples. This will be considered in future research to investigate the performance of the model by using large datasets.

Acknowledgment

The authors express their profound gratitude to Kurukshetra University, Kurukshetra for providing necessary facilities to conduct this research.

Funding Information

This research was carried out independently by the authors without external financial support or assistance.

Author's Contributions

Smita Sharma: Designed the research plan, performed the experiments by coding. She also evaluated the results and wrote the manuscript.

Sanjay Tyagi: Provided essential guidance, reviewed the manuscript, and provided insightful, constructive feedback.

Ethics

The present study represents an original research effort. The corresponding author confirms that the coauthor has reviewed and approved the manuscript, without raising ethical issues.

Nomenclature

Abbreviation	Description
AD	Average Delay
AES-OTP	Advanced Encryption Standard - One Time Password
BC-IAS	Block Chain based Identity Management, Access Control and Secure Sharing
BFL-PSO	Bee-Foraging Learning-based Particle Swarm Optimization
Bi-LSTM	Bidirectional Long Short Term Memory
CIAO-TME	Corona-Integrated Archimedes Optimization with Tent Map Estimation
CSR	Compressed Sensing Reconstruction
COA	Coati Optimization Algorithm
CPA	Chosen Plain-text Attack
DE	Differential Evolution
DCNN	Deep Convolutional Neural Network
DM	Degree of Modification
G-BHO	Grasshopper–Black Hole Optimization
HR	Hiding Ratio
HSO	Harmony Search Optimization
IaaS	Infrastructure as a Service
IAS	Identity Management, Access Control and Secure Sharing
IIoT	Industrial Internet of Things
IPR	Information Preservation Ratio
JA	Jaya Algorithm
J-SSO	Jaya-based Shark Smell Optimization
KNN	K-Nearest Neighbor
KPA	Known Plain-text Attack
LOA	Lyrebird Optimization Algorithm
LSTM	Long Short-Term Memory
MUAOA	Mouse Updated Arithmetic Optimization Model
NBO	Namib Beetle Optimization
OOA	Osprey Optimization Algorithm
PRMS	Patient's E-Healthcare Records Management System
PSO-GWO	Particle Swarm Optimization-Grey Wolf Optimization
RPO	Red Panda Optimization
ResNET	Residual Network
SAD-ECC	Sensitive Aware Deep Elliptic Curve Cryptography
SANBO	Self-Adaptive Namib Beetle Optimization
SDN	Software Defined Networking
SET	System Execution Time
SHA-3	Secure Hashing Algorithm-3
SRHB	Secure and Robust Healthcare-Based Blockchain
SRVA	Secure-Ring-Verification-based Authentication
S-NET	SqueezeNet
SSO	Shark Smell Optimization
YCSB	Yahoo Cloud Serving Benchmark

References

Ahamad, D., Alam Hameed, S., & Akhtar, M. (2022). A Multi-Objective Privacy Preservation Model for Cloud Security Using Hybrid Jaya-Based Shark Smell Optimization. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 2343-2358. https://doi.org/10.1016/j.jksuci.2020.10.015

Ahmad, S., & Mehfuz, S. (2024). Efficient time-oriented latency-based secure data encryption for cloud storage. *Cyber Security and Applications*, *2*, 100027. https://doi.org/10.1016/j.csa.2023.100027

Aminifar, A., Shokri, M., Rabbi, F., Pun, V. K. I., & Lamo, Y. (2022). Extremely Randomized Trees With Privacy Preservation for Distributed Structured Health Data. *IEEE Access*, *10*, 6010-6027. https://doi.org/10.1109/access.2022.3141709

Ardiansyah, A., Ferdiana, R., & Permanasari, A. E. (2022). MUCPSO: A Modified Chaotic Particle Swarm Optimization with Uniform Initialization for Optimizing Software Effort Estimation. *Applied Sciences*, *12*(3), 1081. https://doi.org/10.3390/app12031081

Dehghani, M., Bektemyssova, G., Montazeri, Z., Shaikemelev, G., Malik, O. P., & Dhiman, G. (2023). Lyrebird Optimization Algorithm: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems. *Biomimetics*, *8*(6), 507. https://doi.org/10.3390/biomimetics8060507

Dhamdhere, S. D., Sivakkumar, M., & Subramanian, V. (2025). Cloud data security with deep maxout assisted data sanitization and restoration process. *High-Confidence Computing*, *5*(1), 100238. https://doi.org/10.1016/j.hcc.2024.100238

Fadhil, S., Zaher, H., Ragaa, N., & Oun, E. (2023). A Modified Differential Evolution Algorithm Based on Improving A New Mutation Strategy and Self-Adaptation Crossover. *MethodsX*, *11*, 102276. https://doi.org/10.1016/j.mex.2023.102276

Fang, C., Guo, Y., Wang, N., & Ju, A. (2020). Highly efficient federated learning with strong privacy preservation in cloud computing. *Computers & Security*, *96*, 101889. https://doi.org/10.1016/j.cose.2020.101889

Fang, H., Fu, X., Zeng, Z., Zhong, K., & Liu, S. (2022). An Improved Arithmetic Optimization Algorithm and Its Application to Determine the Parameters of Support Vector Machine. *Mathematics*, *10*(16), 2875. https://doi.org/10.3390/math10162875

Feng, Y., Xinglei, Z., Chengzhi, X., Bei, T., & Chenglin, L. (2018). Improvement on Entropy Weighting Model in Groundwater Quality Evaluation. *IOP Conference Series: Earth and Environmental Science*, *178*, 012006. https://doi.org/10.1088/1755-1315/178/1/012006

Fugkeaw, S. (2022). Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain. *IEEE Access*, *10*, 49028-49039. https://doi.org/10.1109/access.2022.3172973

Gheisari, M., Shojaeian, E., Javadpour, A., Jalili, A., Esmaeili-Najafabadi, H., Bigham, B. S., Vorobeva, A. A., Liu, Y., & Rezaei, M. (2023). An Agile Privacy-Preservation Solution for IoT-Based Smart City Using Different Distributions. *IEEE Open Journal of Vehicular Technology*, *4*, 356-362. https://doi.org/10.1109/ojvt.2023.3243226

Irshad, R. R., Sohail, S. S., Hussain, S., Madsen, D. Ø., Ahmed, M. A., Alattab, A. A., Alsaiari, O. A. S., Norain, K. A. A., & Ahmed, A. A. A. (2023). A Multi-Objective Bee Foraging Learning-Based Particle Swarm Optimization Algorithm for Enhancing the Security of Healthcare Data in Cloud System. *IEEE Access*, *11*, 113410-113421. https://doi.org/10.1109/access.2023.3265954

Jain, Y. K., & Bhandare, S. K. (2013). Min Max Normalization Based Data Perturbation Method for Privacy Protection. *International Journal of Computer and Communication Technology*, *4*(4), 233-238. https://doi.org/10.47893/ijcct.2013.1201

Janosi, A., Steinbrunn, W., Pfisterer, M., & Detrano, R. (1988). Heart Disease. *UCI Machine Learning Repository*. https://doi.org/10.24432/C52P4X

Karlekar, N. P., & Gomathi, N. (2017). Kronecker product and bat algorithm-based coefficient generation for privacy protection on cloud. *International Journal of Modeling, Simulation, and Scientific Computing*, *08*(03), 1750021. https://doi.org/10.1142/s1793962317500210

Kim, D., & Kim, K. S. (2022). Privacy-Preserving Public Auditing for Shared Cloud Data With Secure Group Management. *IEEE Access*, *10*, 44212-44223. https://doi.org/10.1109/access.2022.3169793

Kumar, M., Mukherjee, P., Verma, S., Kavita, Shafi, J., Wozniak, M., & Ijaz, M. F. (2023). A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm. *Scientific Reports*, *13*(1), 5372. https://doi.org/10.1038/s41598-023-32098-2

Kumar, R. (2022). APTx: Better Activation Function than MISH, SWISH, and ReLU's Variants used in Deep Learning. *International Journal of Artificial Intelligence and Machine Learning*, *2*(2), 56-61. https://doi.org/10.51483/ijaiml.2.2.2022.56-61

Liu, Z., Ren, L., Li, R., Liu, Q., & Zhao, Y. (2022). ID-based sanitizable signature data integrity auditing scheme with privacy-preserving. *Computers & Security*, *121*, 102858. https://doi.org/10.1016/j.cose.2022.102858

Ma, R., Li, J., Xing, B., Zhao, Y., Liu, Y., Yan, C., & Yin, H. (2021). A Novel Similar Player Clustering Method With Privacy Preservation for Sport Performance Evaluation in Cloud. *IEEE Access*, *9*, 37255-37261. https://doi.org/10.1109/access.2021.3062735

Mondal, A., & Goswami, R. T. (2021). Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. *Microprocessors and Microsystems*, *81*, 103719. https://doi.org/10.1016/j.micpro.2020.103719

Nwankpa, C., Ijomah, W., Gachagan, A., & Marshall, S. (2018). Activation functions: Comparison of trends in practice and research for deep learning. *ArXiv:1811.03378*.

Onesimu, J. A., Karthikeyan, J., Eunice, J., Pomplun, M., & Dang, H. (2022). Privacy Preserving Attribute-Focused Anonymization Scheme for Healthcare Data Publishing. *IEEE Access*, *10*, 86979-86997. https://doi.org/10.1109/access.2022.3199433

Patel, C., Pasikhani, A., Gope, P., & Clark, J. (2024). User-empowered secure privacy-preserving authentication scheme for Digital Twin. *Computers & Security*, *140*, 103793. https://doi.org/10.1016/j.cose.2024.103793

Patil, R., & HimaBindu, G. (2023). Improved Association Rule Mining-Based Data Sanitization for Privacy Preservation Model in Cloud. *Journal of Telecommunications and Information Technology*, *1*(2023), 51-59. https://doi.org/10.26636/jtit.2023.166922

Prasad, S. N., & Rekha, C. (2023). Block chain based IAS protocol to enhance security and privacy in cloud computing. *Measurement: Sensors*, *28*, 100813. https://doi.org/10.1016/j.measen.2023.100813

Ragu, G., & Ramamoorthy, S. (2023). A blockchain-based cloud forensics architecture for privacy leakage prediction with cloud. *Healthcare Analytics*, *4*, 100220. https://doi.org/10.1016/j.health.2023.100220

Rahman, Md. M., Muniyandi, R. C., Sahran, S., Usman, O. L., & Moniruzzaman, Md. (2024). Restoring private autism dataset from sanitized database using an optimized key produced from enhanced combined PSO-GWO framework. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-66603-y

Ramachandran, P., Zoph, B., & Le, Q. (2017). Swish: A self-gated activation function. *ArXiv:1710.05941v1*.

Sharma, S., & Tyagi, S. (2024). A fourfold-objective-based cloud privacy preservation model with proposed association rule hiding and deep learning assisted optimal key generation. *Network: Computation in Neural Systems*, 1-36. https://doi.org/10.1080/0954898x.2024.2378836

Shen, J., Yang, H., Vijayakumar, P., & Kumar, N. (2022). A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2198-2210. https://doi.org/10.1109/tdsc.2021.3050517

Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. *Alexandria Engineering Journal*, *84*, 275-284. https://doi.org/10.1016/j.aej.2023.10.054

Son, S., Kwon, D., Lee, J., Yu, S., Jho, N.-S., & Park, Y. (2022). On the Design of a Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain. *IEEE Access*, *10*, 75365-75375. https://doi.org/10.1109/access.2022.3191414

Wang, Y., & Nakachi, T. (2020). A Privacy-Preserving Learning Framework for Face Recognition in Edge and Cloud Networks. *IEEE Access*, *8*, 136056-136070. https://doi.org/10.1109/access.2020.3011112

Yan, H., & Gui, W. (2021). Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving. *IEEE Access*, *9*, 45822-45831. https://doi.org/10.1109/access.2021.3066497

Yang, L., Tian, C., Zhang, G., Li, L., & Wang, H. (2022). Efficient Biometric Identification on the Cloud With Privacy Preservation Guarantee. *IEEE Access*, *10*, 115520-115531. https://doi.org/10.1109/access.2022.3218703

Yang, X., Wang, M., Wang, X., Chen, G., & Wang, C. (2020). Stateless Cloud Auditing Scheme for Non-Manager Dynamic Group Data With Privacy Preservation. *IEEE Access*, *8*, 212888-212903. https://doi.org/10.1109/access.2020.3039981

Zala, K., Thakkar, H. K., Jadeja, R., Singh, P., Kotecha, K., & Shukla, M. (2022). PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms. *IEEE Access*, *10*, 85777-85791. https://doi.org/10.1109/access.2022.3198094

Zia, A., Mahum, R., Ahmad, N., Awais, M., & Alshamrani, A. M. (2023). Eye diseases detection using deep learning with BAM attention module. *Multimedia Tools and Applications*, *83*(20), 59061-59084. https://doi.org/10.1007/s11042-023-17839-9