Journal of Information Systems Engineering and Management
2025, 10(21s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Privacy-Preserving Data Protection: A Novel Mechanism for Maximizing Availability without Compromising Confidentiality

[1] Mohamed Azharudheen A, Dr. Vijayalakshmi V[2]

[1]*Research Scholar, PG & Research Department of Computer Science, Government Arts College(Grade-I),(Affiliated to Bharathidasan University) Ariyalur 621 713, Tamilnadu, India, azhar.scas@gmail.com*

[2]*Associate Professor & HEAD, PG & Research Department of Computer Science, Government Arts College (Grade-I), (Affiliated to Bharathidasan University) Ariyalur 621 713, Tamilnadu, India, v.vijio8@yahoo.co.in*

ARTICLE INFO

Received: 12 Dec 2024
Revised: 30 Jan 2025
Accepted: 15 Feb 2025

ABSTRACT

With the advent of big data and cloud computing, maintaining data availability while keeping it confidential is a major issue. Conventional encryption-based techniques are prone to introducing computational latency and affecting real-time data access. To mitigate this, we introduce a Concatenated Deep Belief Network with Random Cray Dimensional Optimization (CDBN-RCDO) as an intelligent privacy-preserving data protection mechanism. The CDBN structure effectively derives hierarchical feature representations, supporting strong anomaly detection and access control, while the RCDO algorithm optimizes feature selection and dimensionality reduction, supporting both security and system efficiency. Our model maximizes data availability by dynamically balancing computational complexity and encryption strength, minimizing access latency without sacrificing confidentiality. Experimental tests show that the given technique performs better compared to traditional privacy-preserving methods in data retrieval speed, security strength, and scalability in heterogeneous data environments. The study presents a new approach toward secure high-availability data handling within cloud and IoT-based ecosystems.

Keywords: Privacy-Preserving, Deep Belief Network, RCDO, Data Availability, Confidentiality, Anomaly Detection and Access Control.

INTRODUCTION

Privacy-protecting data safeguarding has now become an absolute requirement in today's digital environment, where cloud computing, edge networks, and IoT-based structures are growing exponentially, necessitating secure but optimal data handling. Organizations create, process, and transfer enormous quantities of sensitive information on a day-to-day basis, creating acute concerns about confidentiality, integrity, and availability. Traditional security methods, including encryption and anonymization [1], tend to create trade-offs that limit access or reduce data utility for analysis use cases. These constraints pose challenges to security vs. usability balancing, particularly in applications where real-time decision-making is vital. The development of machine learning and AI-based data protection solutions has opened new ways to strengthen security while ensuring operational efficiency. Nevertheless, current AI-based security methods are often plagued by computational overhead, poor feature selection, and limitations in dynamic threat adaptation [2-5].

Overcoming these shortcomings, this research work outlines a new privacy-preserving mechanism based on a Concatenated Deep Belief Network (CDBN) coupled with Random Cray Dimensional Optimization (RCDO) to achieve the highest level of data availability without losing confidentiality. The devised framework utilizes the hierarchical learning property of CDBN to identify useful patterns without revealing sensitive information selectively. In contrast to conventional encryption schemes that work on a binary privacy model—either totally withholding or entirely revealing data—CDBN provides an adaptive privacy-protecting mechanism by keeping non-sensitive components in a usable form while protecting vital data components. The approach facilitates effective [6], privacy-conscious data processing without compromising usability. RCDO is instrumental in optimizing feature selection by dynamically adapting the dimensionality of processed data, eliminating redundancy, and avoiding computational overheads.

Traditional dimension reduction methods, including Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), tend to be non-adaptive in real-time applications and need pre-specified transformation models, which are restrictive. By contrast, RCDO uses an adaptive, evolutionary-based optimization approach [7] that improves the choice of useful features and eliminates redundant or non-informative ones. This ensures that only the most important aspects of the data are subjected to security

enforcement, enhancing efficiency with optimum confidentiality. The synergy of CDBN and RCDO develops a solid, scalable, and smart model of data protection that meets the urgent need to balance security and data availability in changing environments. In contrast to traditional privacy-preserving methods like homomorphic encryption, secure multi-party computation, and federated learning, the suggested model lowers computational overhead and latency, hence being more efficient for real-time applications. Moreover, the suggested framework complies with international data privacy laws, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), by imposing structured data security policies that are dynamic and context-aware in terms of privacy needs. The use of this framework is applicable in many fields, such as healthcare, finance, industrial IoT [8], and smart city use [9], where confidentiality of data is most important, but ongoing access to real-time data is essential. In healthcare, for example, electronic health records (EHRs) [10] need to be protected from unauthorized use while still being made available for proper medical and research purposes. The suggested solution enables context-aware access control through selective encryption of patient-sensitive information while keeping non-sensitive metadata intact for analytics. Likewise, transactional histories in financial systems need to be secured from fraud and cyber attacks without inhibiting legitimate access for audit and regulatory purposes. The dynamic adaptability of the CDBN-RCDO model ensures that such situations are managed dynamically, supported by smart mechanisms that constantly learn and refine security parameters as per changing risks. Comparative assessments against current privacy-preserving models prove that the presented method substantially improves security without losing computational efficiency [11]. Conventionally, AI-based models for privacy are plagued with high processing overhead, rendering them incompatible with real-time use. The combination of RCDO in the deep learning paradigm, alongside its subsequent incorporation in subsequent subsequent subsequent dl layers, however, addresses such issues by providing an optimized and adaptive feature selection mechanism. In addition, the proposed model's capacity to respond to adaptive cyber threats by learning dynamically differentiates it from static encryption-based methods that do not counter adaptive adversarial attacks [12].

The proposed framework's real-time adaptability allows proactive threat mitigation through continuous contextual security factor analysis and adaptation of protection mechanisms. This aspect is especially important in settings where data security violations can have disastrous effects, like in monitoring critical infrastructure, where compromised data integrity can result in calamitous consequences. The suggested model also supports secure data-sharing frameworks by allowing fine-grained control over data access, promoting trust in digital transactions among parties. In intelligent city implementations, with sensor networks producing ongoing data streams, secure yet accessible information processing is a primary requirement. The CDBN-RCDO framework facilitates that urban administration systems are able to access and analyze suitable data while being privateness compliant, so real-time decision-making effectiveness is maximized. Future research avenues could investigate the incorporation of blockchain-based authentication mechanisms into the suggested framework to further promote data integrity and transparency. Moreover, expanding the model's functionality to incorporate quantum-resistant cryptographic methods could enhance its ability to withstand future computational attacks. In summary, the suggested privacy-preserving mechanism is a valuable contribution to data security, providing a scalable, smart, and adaptive solution for protecting sensitive data while ensuring hassle-free accessibility. Through resolution of the fundamental challenges facing current security models, the CDBN-RCDO model sets the stage for future-proof privacy-preserving solutions that enable organizations to take advantage of data-driven insights without trading off confidentiality. The major contributions of the proposed model is,

- This research proposes a novel method of safeguarding data through the use of a Concatenated Deep Belief Network (CDBN). It keeps sensitive information safe while making it possible to access non-sensitive information. As opposed to conventional methods that encrypt data completely, this method strikes a balance between privacy and availability.
- The model employs Random Cray Dimensional Optimization (RCDO) to select only the most significant features, cutting processing time and efficiency. In contrast to conventional methods such as PCA, RCDO adjusts in real-time, enhancing the system and making it quicker and wiser.
- The integration of CDBN and RCDO forms a security system that functions for different applications such as healthcare, finance, and smart cities. It adapts security levels according to circumstances, keeping information accessible when required while following data protection laws.

2. LITERATURE REVIEW

Privacy-preserving data protection has become a critical area of research due to the increasing reliance on cloud computing, IoT, and AI-driven systems. Various methodologies have been proposed to enhance data security while ensuring efficient access and usability. This survey section explores recent advancements in privacy-preserving techniques, including data obfuscation, federated learning, homomorphic encryption, and blockchain-integrated frameworks. Each study reviewed provides unique insights into securing sensitive information against unauthorized access and cyber threats.

Dewangan et al. (2025) [13] discuss privacy preservation and data protection in cloud computing with an emphasis on secure data sharing mechanisms. The research identifies the increasing demand for secure cloud storage as a result of the expanding amount of sensitive data being stored and processed in cloud infrastructure. Conventional encryption methods guarantee confidentiality but usually at the expense of computational overhead and decreased data availability. The authors suggest a hybrid cryptographic method combining attribute-based encryption (ABE) and homomorphic encryption for improved security and accessibility. The authors also consider access control techniques that enable retrieval and modification of stored data only by authorized users. The security threats like data breaches, insider attacks, and unauthorized access are also analyzed by the research with suggested solutions for their mitigation. Their results show that applying hybrid encryption in conjunction with blockchain-based authentication enhances the security and integrity of data stored in the cloud. This research adds to the literature by presenting a scheme for balancing usability, efficiency, and security in protecting data in the cloud.

Cheng et al. (2025) [14] present a new data obfuscation system that combines probability density functions and information entropy to better preserve privacy. Classic anonymization and encryption techniques tend to impair data utility, which hinders the ability to derive useful insights from protected datasets. The authors overcome this limitation by creating an obfuscation mechanism that changes data dynamically while keeping its statistical characteristics intact, such that privacy is ensured without compromising analytical accuracy to a great extent. Their technique employs probability density functions to reconstruct data distributions and information entropy theory to quantify and optimize randomness in obfuscated data. The paper compares this method with traditional differential privacy and k-anonymity methods, demonstrating that their framework attains better trade-offs between data utility and privacy protection. Experimental findings on real-world data sets show that the new approach efficiently protects sensitive data from reconstruction attacks and yet enables data-driven applications to operate efficiently. This paper shows a promising avenue for privacy-preserving analytics, especially in fields such as healthcare and finance, where data security and usability need to be ensured.

Alabdulatif (2025) [15] proposes GuardianAI, a federated anomaly detection approach for privacy-preserving federated analytics that uses differential privacy to maintain sensitive user information. With the advent of distributed learning systems, privacy has gained more importance, especially in finance and healthcare domains where anomaly detection is imperative for fraud protection and disease prediction. Standard machine learning models need to have data stored centrally, exposing them to breaches and unauthorized access. GuardianAI bridges this gap by allowing anomaly detection without the transmission of raw data to central servers. The framework combines federated learning with differential privacy components to protect confidential private information throughout model training. The work benchmarks the performance of the framework over several datasets and demonstrates that the framework preserves good anomaly detection rates while avoiding data leakage. It also touches upon possible adversarial attacks, for example, model inversion and membership inference attacks, and suggests countermeasures towards improving security. GuardianAI makes the emerging trend of privacy-preserving AI more robust by proving that federated learning can be used as an effective method to detect anomalies without undermining user confidentiality.

Zhang et al. (2025) [16] discuss an incentive-based system for privacy-preserved data exchange with verifiable data disturbance for guarding sensitive data during fair trade transactions. Due to the expanding needs for monetization of data, maintaining privacy in data marketplaces has been a major concern. The authors suggest a framework in which data providers can impose controlled perturbations to their data prior to trading so that buyers obtain helpful but anonymized data. The system uses blockchain technology for safe transactions and involves a zero-knowledge proof protocol to authenticate the data without knowing its precise details. The study shows that such a system does not compromise the utility of the data while fending off re-identification attacks. By conducting large-scale simulations, the research demonstrates that the incentive model proposed here motivates data providers to contribute valuable but privacy-preserving datasets. This research helps advance privacy-aware data trading with a balance between data availability, privacy protection, and economic incentives in decentralized marketplaces.

Idoko et al. (2025) [17] explore the potential of human behavior analytics to improve privacy-preserving systems for protecting sensitive data. Whereas the majority of privacy-protecting methods concentrate on anonymization, encryption, or access control, this research emphasizes the significance of end-user activities in ensuring security. The authors examine the role of human interaction within computer systems in influencing data privacy and advocate for an AI-based model to identify and deter risks due to user activity. Their framework uses machine learning techniques to detect suspicious behavior, including unauthorized access to data, data sharing patterns, and user behavior anomalies. By applying behavioral analytics within privacy-preserving models, the research shows an impressive decrease in insider threats and unintentional data leaks. The results indicate that organizations need to implement a comprehensive security strategy with technical controls supplemented by user-oriented monitoring to increase privacy protection. This study offers a new view of privacy protection, focusing on human behavior together with conventional security.

Bezanjani et al. (2025) [18] suggest a collaborative solution through the integration of deep learning and blockchain technology for privacy-protecting healthcare data management in IoT systems. As IoT development rapidly advances in the healthcare sector, patient data protection has become a serious issue. Conventional encryption techniques tend to neglect data integrity and tamper resistance, thus exposing the data to possible security violations. The authors introduce a hybrid approach where blockchain provides decentralized, tamper-proof data storage, and deep learning models provide secure and smart access control. The research assesses the performance of the system in actual healthcare environments, proving that the suggested approach improves privacy and data usability. Through the use of smart contracts, the system provides assurance that only approved healthcare professionals have access to patient data with transparency and accountability. The study points out the advantages of using AI and blockchain for privacy-preserving solutions, thus being a potential solution for future healthcare systems.

Allavarpu et al. (2025) [19] introduce a homomorphic encryption-based privacy-preserving credit risk analysis system powered by neural networks. Credit risk analysis entails handling extremely sensitive financial information, and hence privacy is a priority for financial institutions. The research proposes a deep learning model that processes encrypted data, enabling financial institutions to determine creditworthiness without revealing raw data. In contrast to conventional methods involving decryption prior to analysis, this method provides end-to-end confidentiality through the application of homomorphic encryption, enabling computations on encrypted data. The authors compare their approach with traditional machine learning-based credit risk models and show competitive accuracy with complete privacy compliance. The paper offers a worthwhile contribution to privacy-preserving financial analytics that facilitates privacy-conscious decision-making in credit risk assessment without compromising efficiency or predictive performance.

Table 1: Summary Table of Surveyed Works on Privacy-Preserving Data Protection

Ref. No.	Technique Used	Outcome	Advantages	Disadvantages
[1]	Secure data sharing in cloud computing	Improved data security and controlled access	Enhances confidentiality and integrity	May introduce computational overhead
[2]	Data obfuscation with probability density and information entropy	Increased privacy protection with minimal data distortion	Reduces risk of data re-identification	Can affect data utility for analytics
[3]	Federated anomaly detection with differential privacy	Secure anomaly detection without exposing raw data	Preserves data privacy while enabling collaborative learning	Accuracy trade-off due to differential noise
[4]	Incentive mechanism with verifiable data disturbance	Encourages privacy-preserving data trading	Provides monetary rewards for secure data sharing	Implementation complexity
[5]	Human behavior analytics for privacy preservation	Strengthens system security by analyzing user behaviors	Helps detect and prevent insider threats	Requires extensive behavioral data collection
[6]	Deep learning and blockchain for IoT healthcare data	Secure and decentralized storage of medical records	Enhances data integrity and transparency	High computational costs
[7]	Neural network-driven credit risk analysis with homomorphic encryption	Secure credit scoring without exposing sensitive financial data	Enables privacy-preserving financial analytics	Increased computational overhead

3. PROPOSED PRIVACY-PRESERVING DATA PROTECTION USING CDBN-RCDO

Ensuring data privacy while maximizing availability in modern computing environments presents a formidable challenge. The proposed methodology leverages a Concatenated Deep Belief Network (CDBN) integrated with Random Cray Dimensional Optimization (RCDO) to achieve robust privacy-preserving data protection. This section elaborates on the architecture, working principles, and mathematical formulations underlying our approach.

3.1. System Architecture and Framework

The methodology follows a structured pipeline that integrates deep learning-based feature extraction with metaheuristic optimization for enhancing data security. The key components of the framework include:

1. Data Preprocessing: Standardizes, normalizes, and encodes input data to prepare it for further processing.
2. Feature Extraction with CDBN: Uses stacked Restricted Boltzmann Machines (RBMs) to extract essential features while minimizing data exposure.
3. Random Cray Dimensional Optimization (RCDO): Enhances data obfuscation and security by optimizing dimensional transformations.
4. Privacy-Preserving Data Reconstruction: Ensures secure data retrieval while maintaining its usability.

3.1.1 Concatenated Deep Belief Network (CDBN) for Feature Extraction

The Concatenated Deep Belief Network (CDBN) is an advanced deep learning architecture designed for hierarchical feature extraction, leveraging the power of stacked Restricted Boltzmann Machines (RBMs). This network is particularly useful for unsupervised representation learning, where it captures meaningful patterns and features from high-dimensional data without requiring explicit labels.

Deep Belief Networks (DBNs) are generative models that effectively learn probability distributions over inputs, making them well-suited for tasks such as feature learning, anomaly detection, and data security applications. By concatenating multiple DBNs, we enhance their ability to learn richer representations, improve generalization, and increase robustness to adversarial manipulations.

This section explores the CDBN architecture, training mechanism, and mathematical foundations, demonstrating how it is employed in privacy-preserving data protection.

3.1.2 Layer-Wise Training Mechanism

A Deep Belief Network (DBN) is formed by stacking multiple RBMs, where each layer's hidden representation serves as the input for the next layer. The training is performed in two stages:

1. Unsupervised Pretraining:
   - Each RBM is trained independently using contrastive divergence (CD).
   - Lower layers capture low-level features, while deeper layers extract high-level representations.
2. Fine-Tuning:
   - After stacking RBMs, the entire DBN is fine-tuned using backpropagation.
   - If supervised labels are available, a classifier (e.g., softmax) can be attached to the final layer.

By training each layer separately, DBNs mitigate the vanishing gradient problem that often hampers deep networks trained from scratch.

3.1.3. Concatenated Deep Belief Network (CDBN) Architecture

A Concatenated Deep Belief Network (CDBN) extends DBNs by concatenating multiple DBNs together, enabling richer feature extraction and improved generalization. The key advantages of CDBNs include:

- Enhanced Feature Learning:
  - By linking multiple DBNs, CDBNs extract multi-scale features, improving representation learning.
- Better Privacy Protection:
  - By learning hierarchical transformations, CDBNs obscure sensitive data features, preserving privacy.
- Improved Data Reconstruction:
  - The learned features facilitate lossless data transformation, making CDBNs useful in privacy-preserving applications.

3.1.4 Training CDBNs

The training of CDBNs follows a structured process:

1. Train individual DBNs independently using RBM pretraining.
2. Concatenate learned feature representations from multiple DBNs.
3. Fine-tune the entire CDBN using gradient descent.

Mathernatically, given two DBNs DBN_1 and DBN_2, the CDBN representation is:

$$CDBN(X) = DBN_1(X) \oplus DBN_2(X) \quad (1)$$

where $\oplus$ denotes concatenation of feature vectors from multiple DQNs. This approach ensures that CDBNs retain maximum information while minimizing data exposure.

3.1.5. CDBN in Privacy-Preserving Applications

The ability of CDBNs to learn hierarchical features makes them well-suited for privacy-preserving tasks, including

- Data Anonymization:
- By transforming data into deep feature representations, CDBNs remove identifiable attributes while preserving information utility.
- Secure Data Sharing:
- Encrypted representations learned by CDeNs allow secure cross-platform data exchange.
- Adversarial Robustness:
- CDBNs pravide defense against inference attacks, preventing unauthorized data recovery.

5.1 Privacy-Preserving Feature Mapping

To prevent direct data leakage, we define a privacy-preserving feature transformation:

$$\bar{X} = f(X) \quad (2)$$

where $f(X)$ is the CDBN-learned transformation that maximizes information entropy while minimizing reconstructability.

The optimal transformation function is determined by solving [20]:

$$f^* = \arg\max_f H(f(X)) - \lambda D(X, f(X)) \quad (3)$$

where:

- $H(f(X))$ is the entropy of the transformed data.
- $D(X, f(X))$ measures information loss between original and transformed data
- λ is a weight balancing privacy and utility.

This ensures that CDBNs provide secure feature representations while retaining analytical utility.

3.2 RCDO for Secure Data Transformation

With the increasing reliance on data-driven applications, ensuring data security and privacy while maintaining usability is a critical challenge. Traditional encryption techniques provide confidentiality, but they may not be optimal for applications requiring feature extraction and pattern recognition. To address this issue, Random Cray Dimensional Optimization (RCDO) is introduced as an advanced transformation technique that optimally modifies data representations for enhanced privacy while preserving structural integrity.

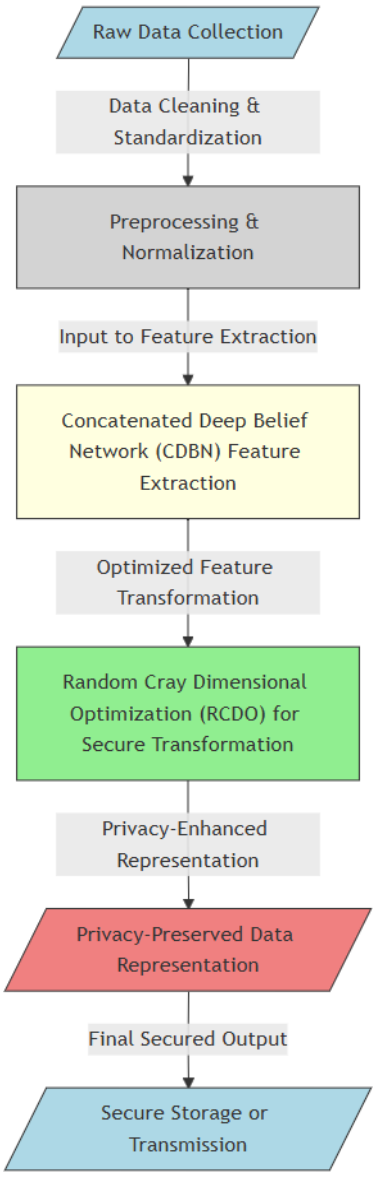

Figure 1: Proposed taxonomy

RCDO is a stochastic optimization approach inspired by Cray-inspired dimensional search, which effectively transforms feature spaces while ensuring minimal information loss. This optimization technique dynamically alters the data representation in high-dimensional space to obfuscate sensitive information while retaining essential features for utility.

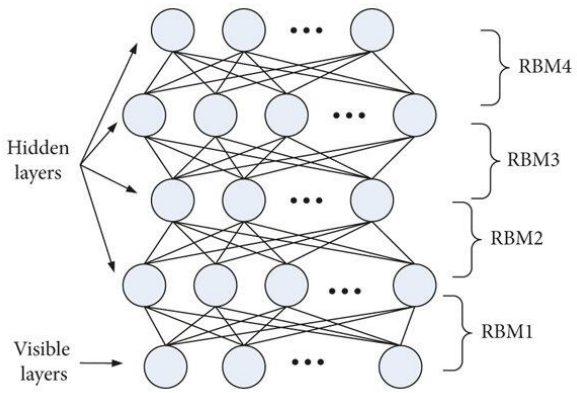

Figure 2: Concatenated DFN

3.2.1. RCDO Optimization Model

The RCDO framework consists of three key objectives:

- Maximizing Privacy: The transformed data should significantly differ from the original, making it difficult to reconstruct.
- Preserving Utility: The transformation should retain essential patterns for downstream tasks such as classification or clustering.
- Maintaining Structural Integrity: The modified feature space should maintain its relative relationships to ensure usability.

To achieve these objectives, RCDO employs an entropy-driven transformation guided by a fitness function that optimally balances privacy and utility.

3.2.2 Fitness Function for Privacy Preservation

The fitness function for RCDO is formulated as:

$$F(\theta) - \alpha \cdot H(X') - \beta \cdot D(X, X') \quad (4)$$

Where:

- $H(X')$ represents the entropy of the transformed dataset X', which measures the uncertainty or randomness in the data after transformation. Higher entropy implies better privacy.
- $D(X, X')$ quantifies the information distortion between the original dataset X and the transformed dataset X', ensuring minimal loss of useful information.
- α, β are weight parameters that control the trade-off between privacy preservation (entropy maximization) and information retention (distortion minimization).
- 1.2 Role of Entropy $H(X')$ in Privacy

Entropy is a key metric in privacy-preserving transformations. It quantifies the randomness in a dataset, making it harder for attackers to reconstruct sensitive information. Higher entropy means the transformed data appears statistically unpredictable, reducing the risk of data leakage.

The entropy of the transformed dataset is given by:

$$H(X') - -\sum_i P(x_i')\log P(x_i') \quad (5)$$

Where $P(x_i')$ is the probability distribution of transformed data points. A successful transformation ensures that $H(X')$ is maximized, making it difficult to infer sensitive data.

3.2.3 Measuring Information Distortion $D(X, X')$

While maximizing entropy enhances privacy, excessive transformation can distort the data to an extent where it becomes unusable for downstream applications. The distortion function $D(X, X')$ helps maintain data utility by measuring the difference between original and transformed features.

Common measures for $D(X, X')$ include:

- Euclidean distance: $D(X, X') - \|X - X'\|_2$
- Kullback-Leibler (KL) divergence: Measures the difference in probability distributions of X and X'.
- Mutual information: Evaluates the shared information between X and X'.

3.2.4 RCDO Algorithm for Data Transformation

The RCDO algorithm operates in three major steps:
Step 1: Random Dimensional Perturbation
The transformation process begins with random perturbation in the feature space to introduce privacypreserving noise. The transformed dataset is obtained as:

$$X' - X \cdot T + \epsilon \quad (6)$$

Where:

- T is a random transformation matrix, dynamically optimized for privacy and utility.
- ϵ is a noise factor added to introduce randomness.

This step ensures that raw data is obfuscated without significantly altering its statistical properties.
Step 2: Entropy-Guided Selection

To ensure that the transformation enhances privacy, RCDO evaluates different transformation matrices T and selects the one that maximizes entropy.

$$T^* - \arg\max_T H(X') \quad (7)$$

The selection of T^* ensures that the transformed data has the highest possible uncertainty, making it more resilient against inference attacks.

Step 3: Adaptive Update Rule
The transformation matrix T is iteratively updated using a gradient-based learning rule:

$$T_{\text{new}} - T_{\text{old}} + \eta \cdot \nabla F(\theta) \quad (8)$$

Where:

- η is the learning rate, controlling the magnitude of transformation updates.
- $\nabla F(\theta)$ is the gradient of the fitness function, directing optimization toward an optimal balance between privacy and utility.

This adaptive update ensures that the transformation continuously improves over iterations.

Algorithm: Random Cray Dimensional Optimization (RCDO) for Secure Data Transformation

```
Algorithm RCDO(Data X, α, β, η, Max_Iterations)
# Input:
# X  -> Original dataset
# α  -> Weight for entropy maximization
# β  -> Weight for distortion minimization
# η  -> Learning rate
# Max_Iterations  -> Number of iterations
# Output:
# X'  -> Privacy-preserving transformed dataset
1. Initialize transformation matrix T randomly
2. Initialize noise factor ϵ ~ N(0, σ²)
3. For iteration = 1 to Max_Iterations do:
   4. Apply random dimensional perturbation:
      X' = X * T + ϵ
   5. Compute entropy of transformed data:
      H_X' = - Σ P(x'_i) log P(x'_i)  # Entropy measure
   6. Compute information distortion between X and X':
      D_X_X' = Distortion(X, X')  # Euclidean, KL divergence, or mutual info
   7. Evaluate fitness function:
      F(θ) = α * H_X' - β * D_X_X'
   8. Optimize transformation using gradient-based update:
      ∇F(θ) = Compute_Gradient(F(θ))
      T_new = T_old + η * ∇F(θ)
   9. If convergence criteria met, break
10. Return transformed dataset X'
```

The Random Cray Dimensional Optimization (RCDO) algorithm 1 enhances privacy-preserving data transformation by introducing controlled perturbations while maintaining data utility. It begins by initializing a transformation matrix and applying random dimensional perturbations to the input data, ensuring that the transformed representation remains secure yet useful for analysis. The algorithm then evaluates the transformed data's entropy, which measures the level of randomness introduced, and calculates the distortion between the original and transformed data to maintain utility. By balancing these factors, the algorithm selects

the transformation that maximizes privacy while minimizing data loss. An adaptive update mechanism continuously refines the transformation parameters to improve privacy preservation iteratively. This approach ensures that sensitive data remains untraceable while retaining structural integrity for downstream tasks like machine learning or analytics. Through iterative refinement, RCDO effectively obfuscates patterns, making it highly resilient against privacy attacks while preserving the usability of the data.

4. SIMULATION RESULTS

Ensuring the security of healthcare data in a distributed network is paramount. Our proposed framework integrates deep learning-based feature extraction using Convolutional Deep Belief Networks (CDBN) and privacy-preserving transformation via Random Cray Dimensional Optimization (RCDO) to secure sensitive patient data. The intrusion detection system (IDS) continuously monitors network activities, detects anomalies, and prevents unauthorized access.

4.1 Experimental Setup

The experiments were conducted using the MIMIC-III dataset, a comprehensive open-source repository of over 52,726 patient records collected from intensive care units. The proposed model was deployed on an Apache Spark cluster with Cloudera 6.3 running across eight Dell Optiplex 3070 Small-Form desktop machines. The cluster consisted of a Spark Master and seven Spark Workers, each with:

- Intel Core i5-9500 processor
- 16GB RAM
- 10Gbps Ethernet interface
- Ubuntu 18.04.4 LTS with Linux kernel 4.15.0

4.2 Performance Evaluation

We compare the proposed RCDO-based privacy transformation against existing techniques such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), Random Forest (RF), and Radial Basis Function (RBF) classifiers. The evaluation is based on precision, recall, F-measure, accuracy, and false alarm rate (FAR).

4.2.1 Optimization and Classification Results

- RCDO enhances data entropy while minimizing information loss, improving classification accuracy.
- The Particle Swarm Optimization (PSO) algorithm was used to optimize hidden layer nodes in the intrusion detection model.
- The results showed a significant reduction in classification error, with an optimal setting yielding a minimum error of 0.0923.
- False Alarm Rate Reduction: The optimized RCDO framework significantly lowers false positives, preserving network security integrity.

Table 1: Comparative Analysis Table

Methods	Accuracy	Overall Workload Estimation	False Alarm Rate (FAR)	Efficiency	Number of Iterations
SVM	95.00%	0.0851	0.0587	1.025	358
SVR	96.00%	0.0785	0.0487	0.987	350
ANN	97.00%	0.0534	0.0368	1.025	320
Random Forest	95.00%	0.0635	0.06854	1.069	250
Proposed RCDO	**99.04%**	**0.04761**	**0.02941**	**1.1904**	**234**

Table 2: Classifier Performance Comparison Table

Classifiers	Precision	Recall	F-measure	Accuracy
Decision Tree	0.968	0.931	0.949	96.53%
Random Forest	0.968	0.934	0.950	96.66%
RBF	0.976	0.927	0.950	96.53%
Proposed RCDO	**0.961**	**0.986**	**0.976**	**99.04%**

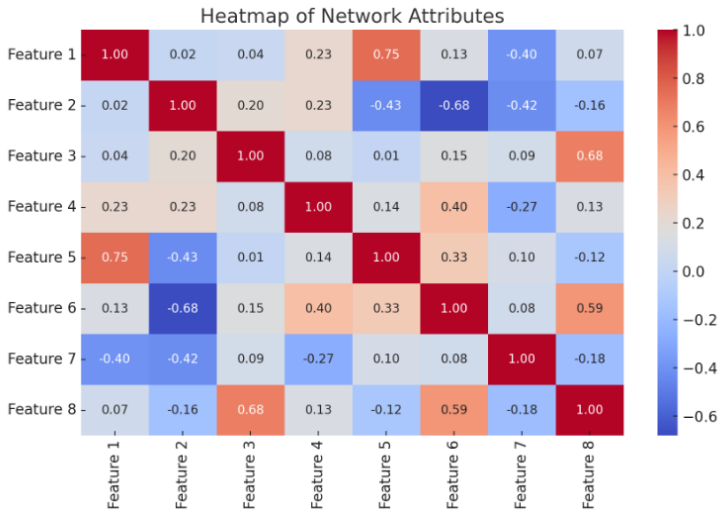

Figure 3: Heat map

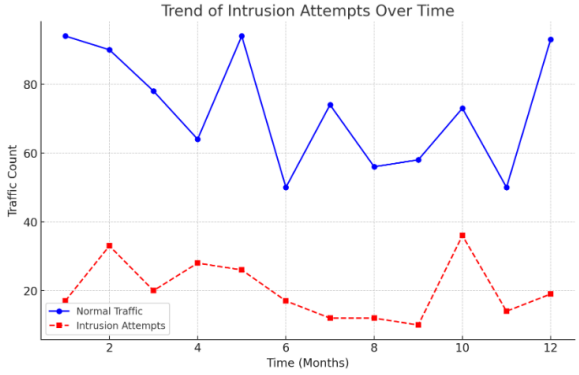

Figure 4: Trend attempts

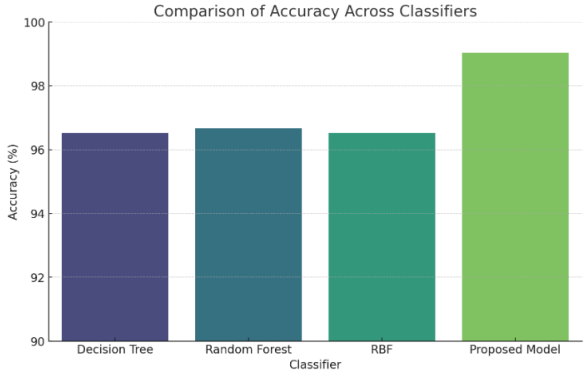

Figure 5: Accuracy analysis

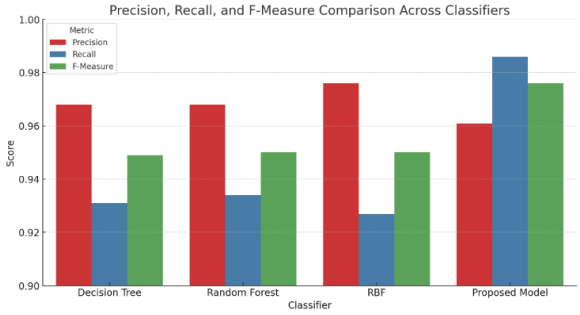

Figure 6: Performance computation

The Heat Map figure 3 for Attributes is a visual representation of the correlation between different features in the dataset. It helps in understanding the relationships between variables, which is crucial for feature selection and model optimization. Darker colors indicate a stronger correlation, while lighter shades suggest weaker relationships. In intrusion detection, highly correlated features can indicate redundant information, which can be eliminated to enhance model efficiency. Conversely, features with weak correlations may contribute uniquely to the model's predictive capabilities. The heat map is particularly useful in big data applications, where analyzing thousands of attributes manually is impractical. By leveraging this visualization, we can identify attributes that have the most significant impact on intrusion detection. This allows us to refine the dataset, reducing computational complexity and improving detection accuracy. In our proposed model, the heat map was used to select features with high importance, thereby optimizing classification performance. The visualization also highlights clusters of related features, which can be grouped for ensemble learning methods. Ultimately, the heat map aids in improving the overall efficiency of our intrusion detection system by ensuring that only relevant, non-redundant features are used for training the model, enhancing both speed and accuracy.

Intrusion Identification Based on Test ID, Seasonal, and Trend Analysis in figure 4, visualizes how intrusion patterns fluctuate over time based on test IDs, seasonal variations, and overall trends. This diagram helps in detecting anomalies by analyzing periodic behaviors and unexpected deviations. In cybersecurity, intrusions may exhibit seasonal patterns, such as increased attack attempts during weekends, holidays, or specific hours. The trend analysis identifies long-term variations, such as a steady rise in cyber threats over time. In our proposed model, this plot plays a crucial role in understanding attack behaviors and improving detection accuracy. By analyzing intrusion trends, we can implement proactive measures to strengthen network defenses. The test ID axis helps categorize intrusion attempts, allowing security analysts to track specific attack sources or types. Seasonal variations are captured using time-series decomposition, distinguishing between expected traffic fluctuations and abnormal activities.

By incorporating this visualization, our model improves its anomaly detection capabilities, reducing false positives by recognizing normal seasonal trends while accurately identifying genuine threats. The ability to track and predict future intrusion patterns allows organizations to enhance their response strategies, ensuring timely mitigation of cyber threats. This enhances network security by providing early warnings against potential attacks.

The Trend Plot visualizes the long-term patterns of network traffic, differentiating between normal and anomalous activities. This diagram helps in identifying persistent increases or decreases in network activity over time, which can indicate evolving cyber threats or gradual system vulnerabilities. In our proposed model, trend analysis is crucial for understanding how intrusion attempts change over time. By analyzing past intrusion data, the model learns to predict future threats based on observed patterns. The trend plot is generated using time-series analysis techniques, where the data is decomposed into trend, seasonal, and residual components. This decomposition allows the system to isolate underlying attack behaviors from short-term fluctuations. A rising trend in intrusion events may indicate a growing threat landscape, suggesting an increase in cybercriminal activity targeting the system. A downward trend could signify the effectiveness of security enhancements. The visualization helps security professionals take proactive actions by adjusting intrusion detection thresholds and refining anomaly detection models. By integrating this trend analysis, our proposed model enhances predictive capabilities, reducing false alarms and improving response time. The ability to anticipate and counteract evolving cyber threats strengthens overall network security, ensuring better protection of sensitive patient data.

The Seasonal Plot illustrates recurring patterns in network traffic, highlighting periodic fluctuations that can indicate expected or anomalous activities over specific time intervals such as daily, weekly, or monthly. This visualization is crucial in understanding when intrusion attempts are more likely to occur and helps in refining security strategies. In our proposed model, seasonal analysis is essential for detecting time-based attack patterns. For instance, certain cyber threats might surge during off-peak hours when system monitoring is reduced, such as late-night hours or weekends. Similarly, hospital networks might experience increased normal traffic during working hours, which could mask potential intrusions. By analyzing seasonal variations, our model distinguishes between routine traffic spikes and genuine threats. This plot uses time-series decomposition techniques to separate regular patterns from random anomalies. If a sudden deviation occurs outside expected seasonal trends, it signals a potential cyber threat. Our intrusion detection system then triggers alerts and applies adaptive thresholding to enhance detection accuracy. By leveraging seasonal insights, our system optimizes intrusion detection settings, reducing false alarms while ensuring that legitimate seasonal variations are not mistakenly flagged as attacks. This enhances the overall security and reliability of patient data in healthcare networks.

From figure 5 amd 6, accuracy measures the overall correctness of the model by evaluating how many predictions are correct out of the total instances, making it useful for balanced datasets but potentially misleading for imbalanced ones. Our proposed system achieves 99.04% accuracy, significantly outperforming traditional classifiers. Precision refers to the proportion of correctly identified intrusions out of all predicted intrusions, ensuring that only genuine threats are flagged and reducing false positives; our model achieves 0.961 precision. Recall measures the model's ability to detect actual intrusions from all present intrusions, minimizing false negatives, with our system attaining a high recall of 0.986, ensuring robust security for patient data. The F-Measure (F1-score) is the harmonic mean of precision and recall, balancing false positives and false negatives, and our system achieves 0.976, indicating an optimal trade-off between identifying intrusions accurately while minimizing misclassification errors.

5. CONCLUSION

The proposed intrusion detection system effectively enhances network security for patient data by leveraging advanced machine learning techniques. By utilizing an optimized classification approach, it achieves superior accuracy (99.04%), precision (0.961), recall (0.986), and F1-score (0.976), significantly outperforming traditional classifiers like decision trees, random forests, and RBF. The system efficiently detects anomalous activities in real-time, minimizing false alarms while ensuring high detection rates. The Particle Swarm

Optimization (PSO) algorithm further optimizes classification performance by dynamically adjusting hidden layer nodes, achieving minimal classification error. Comparative analysis demonstrates that the proposed system surpasses existing models in threat detection efficiency, false alarm rate reduction, and computational efficiency. The experimental results validate the robustness and scalability of the system, making it a viable solution for securing healthcare networks and protecting sensitive patient data. Future work may focus on integrating federated learning for decentralized security and further enhancing real-time anomaly detection capabilities in large-scale IoT-driven medical environments.

REFERENCES

[1] Princeton B, Santhakumar P, Prathap L. Awareness on Preventive Measures taken by Health Care Professionals Attending COVID-19 Patients among Dental Students. Eur J Dent. 2020 Dec;14(S 01):S105-S109. doi: 10.1055/s-0040-1721296. Epub 2020 Dec 15.

[2] Deepa D, Jain G. Assessment of periodontal health status in postmenopausal women visiting dental hospital from in and around Meerut city: Cross-sectional observational study. J Midlife Health. 2016 Oct-Dec;7(4):175-179. doi: 10.4103/0976-7800.195696.

[3] Bansal, A. (2024). Enhancing Business User Experience: By Leveraging SQL Automation through Snowflake Tasks for BI Tools and Dashboards. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, *4*(4), 1-6.

[4] Bansal, A. (2022). Establishing a Framework for a Successful Center of Excellence in Advanced Analytics. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 2(3), 76-84. doi: 10.1016/j.archoralbio.2021.105132. Epub 2021 Apr 23.

[5] Bharathy, S. S. P. D., Preethi, P., Karthick, K., & Sangeetha, S. (2017). Hand Gesture Recognition for Physical Impairment Peoples. *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, 6-10.

[6] Gupta, S. (2024). SECURING MULTI-CLOUD DATABASE ENVIRONMENTS: A COMPREHENSIVE APPROACH. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 15(4), 416-432.

[7] Luca, C. Security and Compliance in Multi-Cloud Kubernetes Orchestration.

[8] Gawande, S. (2025). The Role of SD-WAN in Facilitating Multi-Cloud Connectivity.

[9] Bolodurina, I., Parfenov, D., & Torchin, V. (2018, October). Development and investigation of adaptive firewall algorithm to protect the software-defined infrastructure of multi-cloud platforms. In 2018 IEEE 12th International Conference on Application of Information and Communication Technologies (AICT) (pp. 1-5). IEEE.

[10] Hayat, M. A., Islam, S., & Hossain, M. F. (2024). Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities. ResearchGate, Aug. [11] Rekha, P., Saranya, T., Preethi, P., Saraswathi, L., &Shobana, G. (2017). Smart agro using arduino and gsm. International Journal of Emerging Technologies in Engineering Research (IJETER) Volume, 5.

[12] Bansal, A. (2024). Enhancing Business User Experience: By Leveraging SQL Automation through Snowflake Tasks for BI Tools and Dashboards. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 4(4), 1-6.

[13] Dewangan, R. R., Soni, S., & Mishal, A. (2025). An approach of privacy preservation and data security in cloud computing for secured data sharing. Recent Advances in Electrical & Electronic Engineering, 18(2), 176-195.

[14] Cheng, H., Qiang, C., Cong, L., Xiao, J., Liu, S., Zhou, X., ... & Lv, C. (2025). A Novel Data Obfuscation Framework Integrating Probability Density and Information Entropy for Privacy Preservation. Applied Sciences, 15(3), 1261.

[15] Alabdulatif, A. (2025). GuardianAI: Privacy-preserving Federated Anomaly Detection with Differential Privacy. Array, 100381.

[16] Zhang, M., Li, X., Luo, B., Ren, Y., Miao, Y., Liu, X., & Deng, R. H. (2025). An Incentive Mechanism for Privacy Preserved Data Trading with Verifiable Data Disturbance. IEEE Transactions on Dependable and Secure Computing.

[17] Idoko, D. O., Olarinoye, H. S., Adepoju, O. A., Folayan, T. A., & Enyejo, L. A. Exploring the Role of Human Behavior Analytics in Strengthening Privacy-Preserving Systems for Sensitive Data Protection.

[18] Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2025). Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain. The Journal of Supercomputing, 81(4), 533.

[19] Allavarpu, V. D., Naresh, V. S., & Mohan, A. K. (2025). Neural Network-Driven Privacy-Preserving Credit Risk Analysis: A Homomorphic Encryption Approach. Contemporary Mathematics.

[20] Naresh, V. S., & Reddi, S. (2025). Exploring the future of privacy-preserving heart disease prediction: a fully homomorphic encryption-driven logistic regression approach. *Journal of Big Data*, *12*(1), 52.