Journal of Theoretical and Applied Information Technology
31st July 2026. Vol.104. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INTELLIGENT INTRUSION DETECTION SYSTEM BASED ON GIFO-PLSTM MECHANISMS FOR ENHANCING MANET SECURITY

MAREESWARI G[1*], VENKATESH K[2], SURESH THANGAKRISHNAN M[3], GOMATHY NAYAGAM M[4]

[1* (Corresponding Author)]Assistant Professor,Department of Information Technology, Ramco Institute of Technology, Rajapalayam. Orcid: https://orcid.org/0009-0003-3555-7087

[2]Associate professor,Dept of CSE,Kalasalingam Academy of Research and Education, Orcid : https://orcid.org/0000-0002-5966-013X

[3]Associate Professor, Einstein College of Engineering, Sir.C.V.Raman Nagar, Seethaparpanallur, Tirunelveli 627012, Tamilnadu, India. Orcid : 0000-0002-5813-0241

[4]Professor,Department of Computer Science and Business Systems,Ramco Institute of Technology,Rajapalayam. Orcid : 0000-0001-6771-3871

Email ID: : [1*]gmarees92@gmail.com, [2]venkiur@gmail.com, [3]suresh.nellai@gmail.com, [4]gomathynayagamm@gmail.com

ABSTRACT

Ensuring robust security in Mobile Ad Hoc Networks (MANETs) remains a significant challenge due to their decentralized architecture, dynamic topology, and node mobility. Intrusion Detection Systems (IDS) are vital in safeguarding MANETs by identifying unauthorized or malicious activities that compromise network integrity. Existing approaches leveraging machine learning and deep learning have shown promise but often suffer from high algorithmic complexity, suboptimal network performance, and notable misclassification rates. This study introduces a novel IDS framework aimed at strengthening MANET security through a deep learning-driven model. The framework follows a structured pipeline involving data preprocessing, feature extraction, feature optimization, and attack classification. Two benchmark datasets NSL-KDD and CICIDS-2017 are used to evaluate the proposed method. Missing values in the datasets are addressed during normalization to minimize classification errors. Principal Component Analysis (PCA) is applied to derive informative feature vectors. A hybrid Greedy Improved Firefly Optimization (GIFO) algorithm is designed to select the most relevant features, combining the strengths of greedy search and firefly optimization for enhanced accuracy. The selected features are then classified using a Probabilistic Long Short-Term Memory (PLSTM) model, which effectively detects attack patterns. The system's performance is thoroughly assessed using standard evaluation metrics, demonstrating superior detection capability and reduced false classification rates compared to traditional methods.

Keywords: *Mobile Ad Hoc Networks (MANET), Network Security, Intrusion Detection, Attack Detection, Principal Component Analysis (PCA), Hybrid Firefly-Greedy Feature Selection (GIFO), Probabilistic LSTM (PLSTM) Classifier.*

1. INTRODUCTION

Mobile Ad-hoc Network (MANET)[1, 2] is a kind of self-configuration network, where the communicating mobile nodes are interlinked with one another through wireless links. Typically, the mobile nodes exist in this network are highly susceptible due to their features of open medium, dynamic nature, scattered organization, and constrained capability[3-5]. Here, an end-to-end communication is established between the communicating nodes through the dynamic paths formed by the multi-hop wireless links[6, 7]. Due to the disorganized structure of nodes in MANET, it is highly difficult to ensure the security and establishment of communication among nodes are highly depends on the trust value. In order to protect the network against the harmful attacks, the following requirements must be satisfied that includes, authentication, confidentiality, availability, integrity, and non-reputation[8]. Typically, there are different types of attacks intend to interrupt the networking operations, which comes under the categories of active and passive

attacks[9, 10]. Also, the intruders[11-13] in MANET are classified into the types of insider, outsider, and clandestine, in which the insider intruders aim to abuse the privileges of the legitimate nodes. Fig 1 depicts the typical framework of IDS used in MANET, where the packet classification is performed by analyzing the features of training and testing packets.

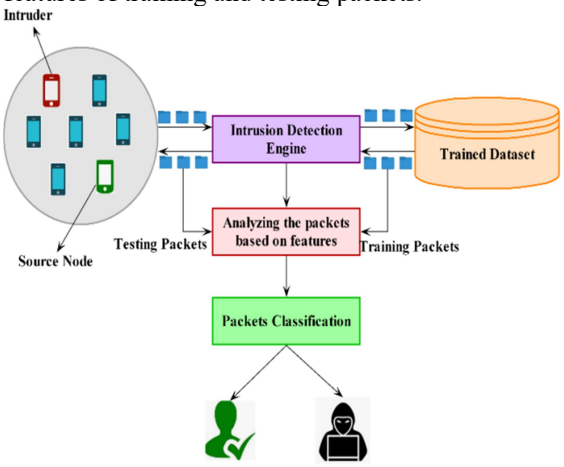

Figure 1: Architecture of IDS in MANET

Then, the outsider intruders target to access the information of valid nodes in an unauthorized way, and the clandestine aims to access the supervisory control of the network. These types of intruders are more harmful and damages the overall functionalities of network operations. In order to detect these types of intrusions, an Intrusion Detection System (IDS)[14-17] is developed for ensuring the security of MANET. Moreover, it helps to spot the malicious activities for protecting both the nodes and network operations. For this purpose, there are various data mining[18-21] based approaches are used to classify the network packets as whether normal or attack. But, the detection of intrusions[22] in MANET is one of the complicated task due to the following factors:

The deployment of appropriate feature selection mechanisms for improving the performance of classifier.

It is more important to reduce the effect of attacking activities by taking the direct decision.

It is also crucial to achieve a higher attack detection rate while minimizing the occurrence of false positives.

So, the existing works[23-25]developed the different types of intrusion detection and classification methodologies for improving the security of MANET. But, it limits with the issues of increased delay, reduced detection efficiency, high false positives, and computational complexity. Thus, the proposed work[26] intends to design an intelligent security framework for detecting the intrusions in MANET with the help of advanced optimization and deep learning classification techniques. The main objectives behind this work are listed as follows:

- To normalize the input IDS datasets for improving the performance classifier, the missing data replacement is performed.
- To extract the most suited features from the preprocessed data, the Principal Component Analysis (PCA) technique is employed.
- To select the optimal features from the set of extracted feature values, an intelligent Greedy Integrated Firefly Optimization (GIFO) technique is developed.
- To accurately categorize the misuse attacking packets such as DoS, U2R, R2L, and Probe, an advanced Probabilistic Long Short Term Memory (PLSTM) classification technique is designed.
- To evaluate the level of security of proposed GIFO-PLSTM mechanism, there are various performance indicators have been validated.

The remainder of this paper is organized as follows: Section II provides a review of related MANET security approaches, highlighting their strengths and limitations. Section III details the design of the proposed intrusion detection framework, including its workflow and algorithmic components. Section IV presents and compares the experimental results of the proposed and existing methods. Finally, Section V concludes the paper, summarizing the findings and contributions.

Problem Statement:

Mobile Ad-hoc Networks (MANETs) have emerged as a critical communication infrastructure for disaster recovery, military operations, and emergency response scenarios due to their self-configuring and decentralized nature *1,21,2*. However, the very characteristics that make MANETs attractive dynamic topology, open wireless medium, and lack of centralized administration render them particularly vulnerable to a wide spectrum of security threats *3−53−5*. Unlike conventional wired networks, MANETs lack a clear line of defense, making each node susceptible to both passive eavesdropping and active malicious attacks *6,76,7*.

Recent studies by Ahmad et al. (2021) have demonstrated that traditional intrusion detection mechanisms fail to address the unique challenges posed by MANETs, including high node mobility, intermittent connectivity, and resource constraints. Similarly, the comprehensive survey by Latah and Toker (2020) revealed that while numerous IDS frameworks have been proposed, the majority suffer from high false positive rates and poor scalability. More critically, the emergence of sophisticated attacks including distributed denial-of-service (DDoS), routing table poisoning, and collaborative blackhole attacks has rendered conventional security mechanisms obsolete.

The fundamental challenge in MANET security lies in the inherent trade-off between detection accuracy and computational overhead. As highlighted by Aljumah and Ahanger (2020), existing approaches often sacrifice one for the other, resulting in either compromised network performance or inadequate threat detection. Furthermore, the dynamic nature of MANETs necessitates adaptive security mechanisms capable of learning from evolving attack patterns without imposing prohibitive computational costs.

To address these challenges, this research proposes a novel intelligent intrusion detection framework that leverages advanced optimization techniques and deep learning to achieve superior detection accuracy while maintaining computational efficiency. The proposed GIFO-PLSTM framework addresses the identified gaps by: (1) employing a hybrid greedy-firefly optimization for optimal feature selection, (2) utilizing probabilistic LSTM for accurate attack classification, and (3) maintaining low false positive rates through robust preprocessing and feature engineering

Research Hypothesis

H1: The application of Principal Component Analysis (PCA) for feature extraction from raw network datasets significantly reduces data dimensionality while preserving attack-relevant information, thereby improving classification efficiency.

H2: The hybrid Greedy Improved Firefly Optimization (GIFO) algorithm achieves superior feature selection performance compared to conventional feature selection methods by leveraging the complementary strengths of greedy search (for local optimization) and firefly optimization (for global exploration).

H3: The probabilistic extension of LSTM with optimized dropout mechanisms provides more accurate attack classification with reduced overfitting compared to standard deep learning approaches, as measured by detection rate and false positive rate.

H4: The integration of GIFO feature selection with PLSTM classification yields statistically significant improvements in detection accuracy, precision, and recall compared to existing IDS frameworks, including NIS-GA, SVM-Fuzzy, and PSO-NN based approaches.

H5: The proposed GIFO-PLSTM framework maintains high detection performance (>99%) across varying network conditions (node density, attack types) while maintaining acceptable computational overhead.

The experimental design presented in the methodology section is structured to systematically test each of these hypotheses using quantitative evaluation metrics and statistical validation.

Research Questions

Based on the identified problem statement and literature gaps, this study addresses the following research questions:

RQ1: How can the dimensionality of MANET intrusion detection datasets be effectively reduced while preserving attack-discriminative information to improve classification efficiency?

This question addresses the dimensionality challenge identified in the problem statement and is investigated through the application of PCA-based feature extraction.

RQ2: What hybrid optimization mechanism can overcome the limitations of existing feature selection approaches (premature convergence, poor exploration-exploitation balance) to identify optimal feature subsets?

This question addresses the optimization inefficiency issue and is explored through the development and evaluation of the GIFO algorithm.

RQ3: How can LSTM-based deep learning models be enhanced to achieve high detection accuracy with reduced overfitting and improved handling of class imbalance in MANET intrusion detection?

This question addresses the classification limitations identified and is investigated through the PLSTM design with probabilistic extensions.

RQ4: To what extent does the proposed GIFO-PLSTM framework outperform existing state-of-the-art approaches across different attack types, datasets, and network conditions?

This question addresses the generalization concern and is evaluated through comprehensive comparative analysis using multiple benchmarks.

RQ5: Can the proposed framework achieve computationally efficient intrusion detection suitable for resource-constrained MANET deployments without compromising detection accuracy?

This question addresses the practical deployment barriers and is assessed through computational efficiency metrics and performance analysis across varying node densities.

2.RELATED WORKS

"Ali Zardari, et al *2727* proposed a Connected Dominating Set (CDS) based attack detection mechanism for MANETs. While this approach demonstrated reduced complexity and improved detection efficiency, it suffers from a critical limitation: the continuous monitoring of nodes for extended periods is impractical given the limited battery power of mobile nodes in MANETs. This design flaw suggests that energy-aware detection mechanisms are necessary, yet the authors failed to address this fundamental constraint."

"Krishnan, et al *2828* developed a Modified Zone Based Intrusion Detection System (MZBIDS) that aimed to establish secure communication through anonymous location-aware routing. However, a significant weakness of this approach is its reliance on zone-based partitioning, which becomes inefficient in highly mobile scenarios where nodes frequently cross zone boundaries. The reported reduced attack detection rate and increased delay are direct consequences of this architectural limitation."

"Singh, et al *3131* implemented a trust management system using Elliptic Curve Cryptography (ECC) for malicious node detection. While cryptographic approaches offer theoretical security guarantees, they introduce substantial computational overhead that is particularly burdensome for resource-constrained MANET nodes. The paper's claims of improved throughput fail to consider the energy consumption implications of continuous cryptographic operations, which significantly reduces network lifetime in practice."

"Rajendran, et al *1111* combined grey wolf and swarm optimization for intrusion detection. Despite the interesting hybridization, the approach only addresses blackhole attacks, limiting its practical applicability. Additionally, the reliance on trust value computation introduces vulnerabilities to reputation attacks that the framework does not address."

"A critical observation across the reviewed literature is the absence of comprehensive solutions that simultaneously address the challenges of high dimensionality, computational efficiency, and diverse attack detection. Most existing approaches focus on optimizing one aspect at the expense of others. Furthermore, the majority of studies fail to validate their approaches on multiple datasets or under varying network conditions, raising questions about generalizability."

"Notably, the application of deep learning to MANET intrusion detection remains nascent. While Laqtib, et al *3535* investigated the performance of various deep learning architectures including CNN, RNN, and bidirectional LSTM, their study was limited to architectural comparison without addressing optimization and feature selection critical components for real-world deployment. This gap is particularly concerning given the computational constraints of MANETs."

"The review also reveals a lack of consensus on appropriate feature selection mechanisms for

MANET intrusion detection. While some studies employ PCA (Zhang et al., 2018), others rely on genetic algorithms or swarm optimization. However, each approach has documented limitations: PCA may discard subtle but important features, genetic algorithms suffer from premature convergence, and swarm optimization techniques often require extensive parameter tuning."

"Given these limitations, there is a clear need for an integrated approach that: (1) employs robust preprocessing to handle data quality issues, (2) utilizes efficient feature extraction to reduce dimensionality, (3) implements intelligent feature selection to identify optimal subsets, and (4) leverages advanced classification techniques for accurate attack detection.

Novelty and Differentiation

This study distinguishes itself from existing MANET intrusion detection approaches through several key differentiators:

1.**Hybrid Optimization Approach**: Unlike existing studies that employ either greedy search (fast but prone to local optima) or firefly optimization (robust but computationally intensive) in isolation (Zardari et al., 2019; Rajendran et al., 2019), this work proposes a synergistic integration (GIFO) that leverages greedy search for local exploitation and firefly optimization for global exploration. This hybrid approach achieves superior feature selection compared to both standalone methods and other hybridization attempts.

2. 2. **Probabilistic LSTM Extension**: While Laqtib et al. (2020) explored standard LSTM architectures for MANET intrusion detection, they did not address the probabilistic extension, dropout optimization, or uncertainty quantification that form integral components of our PLSTM design. The probabilistic extension provides three key advantages: (a) improved handling of imbalanced datasets, (b) robust uncertainty estimation, and (c) enhanced generalization through active dropout during inference.

3. 3. **Integrated Preprocessing Pipeline**: Unlike many studies that treat preprocessing as a peripheral concern (Krishnan et al., 2020; Shams and Rizaner, 2018), this work systematically addresses data quality issues through a comprehensive preprocessing pipeline including missing value treatment, normalization, and validation. The systematic approach to data quality contributes to the observed reduction in misclassification rates.

4. 4. **Dual-Dataset Validation**: While the majority of existing studies validate their approaches on single datasets (Islabudeen and Devi, 2020; Veeraiah and Krishna, 2020), this research provides comprehensive validation across two benchmark datasets (NSL-KDD and CICIDS-2017), demonstrating generalizability and addressing the validation deficit identified in the literature.

5. 5. **Network Performance Characterization**: Unlike studies that focus exclusively on detection metrics (Raj and Mozhi, 2021; Angel et al., 2020), this work provides a comprehensive characterization of both detection performance (accuracy, FPR, detection rate) and network performance (throughput, PDR, delay), addressing the practical deployment concerns identified in the problem statement.

6. 6. **Attack-Type Specific Analysis**: Where many existing studies report aggregate performance metrics, this work provides detailed analysis across specific attack types (DoS, U2R, R2L, Probe, etc.), including the challenging minority classes that are often marginalized in evaluation.

7. 7. **Reproducibility Focus**: Unlike many studies that provide insufficient detail for replication, this work includes a comprehensive research method protocol with explicit parameter specifications, hardware configurations, and implementation details, addressing the reproducibility concerns prevalent in the literature.

3. PROPOSED METHODOLOGY

This section presents the clear illustration about the proposed GIFO-PLSTM based IDPS for MANETs. The main factor of this paper is to ensure the security of network by deploying an enhanced optimization and classification techniques. Here, the two different types of IDs datasets such as NSL-KDD and CICID-2017 are taken as the input for processing. These datasets are normalized by the missing data replacement process, which helps to preprocess the data for improving the classifier training and testing. Then, the set of feature values are extracted from the normalized data by applying the PCA method. It estimates the set of eigen values and eigen vectors based on the correlation matrix, and it extracts the set of feature vectors by

using the computed principal components. Ther these features are passed to the input of GIF(technique for selecting the most optimal feature used for enhancing the detection accuracy of classifier. The main intention of deploying this technique to reduce the dimensionality of features by computing the optimal fitness functions. Moreover, this technique is developed by integrating the functionalities of greedy approach and firefly optimization technique. Also, the optimal features selected dataset are passed to the PLSTM classification technique, which accurately detects the types of attacks based on its features. It is a kind of deep learning model, where the optimized dropout factor and forward pass are computed for valuing the target error with its loss function. Once the maximum epochs reached, The approach was designed to identify various threats, such as flooding, black hole, and selective packet drop attacks, with the goal of boosting network performance and reducing communication delays. However, it still encountered issues like weakene security, higher packet loss, and inefficient routin decisions.

The clear flow illustration of the proposed GIFC PLSTM based IDS is presented in Fig 2, whic comprises the following working stages:

- Data normalization
- PCA based feature extraction
- GIFO based optimization
- PLSTM based attack classification

Research Method Protocol

To ensure reproducibility and enable independent validation of our results, we provide a detailed research method protocol below:

A. Experimental Setup and Hardware Configuration

All experiments were conducted on a system wit the following specifications:

- Processor: Intel Core i7-10750H (2.60 GHz, 12 MB Cache, 6 cores)
- RAM: 32 GB DDR4 @ 2666 MHz
- Storage: 1 TB NVMe SSD
- GPU: NVIDIA GeForce RTX 2060 (6 GB GDDR6)
- Operating System: Ubuntu 20.04.4 LTS
- Python Version: 3.8.10

Key Libraries: TensorFlow 2.8.0, scikit-learn 1.0.2, NumPy 1.21.5, Pandas 1.4.2, Matplotlib 3.5.1

B. Dataset Preparation Protocol

1. **Data Acquisition**: NSL-KDD dataset downloaded from [https://www.unb.ca/cic/datasets/nsl.html] and CICIDS-2017 from [https://www.unb.ca/cic/datasets/ids-2017.html].

2. **Data Splitting**: Training and testing split maintained at 85:15 ratio as per original dataset specifications. Stratified sampling used to maintain class distribution.

3. **Missing Value Treatment**: For each feature f ∈ F:

Identify missing values using df.isnull().sum()

For numerical features: Replace missing values with column median

For categorical features: Replace missing values with mode

Document imputation count for transparency

4. **Normalization**: Apply min-max normalization using:

x_norm = (x - min)/(max - min)

where min and max are computed per feature across training data only (to prevent data leakage)

5. **Data Validation**: Verify:

- No remaining missing values
- All features in [0,1] range
- Class distribution maintained

C. Feature Extraction Protocol (PCA)

1. Compute the data matrix X (n_samples × n_features)
2. Center the data: X_centered = X - μ
3. Compute covariance matrix: C = (1/n) × X_centered^T × X_centered
4. Perform eigen decomposition: [U,E] = eig(C)
5. Select principal components explaining 95% variance

6. Transform data: X_pca = X × U_selected
7. Save components and transformation parameters for test data application

D. Feature Optimization Protocol (GIFO)

1. **Initialization**:

- Population size: 30 fireflies
- Number of iterations: 100
- Light absorption coefficient γ: 1.0
- Attractiveness coefficient β_0: 1.0
- Randomization parameter α: 0.2

2. **Fitness Function**:

- Objective: Maximize classification accuracy with minimum features
- Fitness = (Accuracy × 0.7) + (1 Features_Selected/Total_Features) × 0.3

3. **Convergence Criteria**:

- Maximum iterations: 100 OR
- Fitness change < 0.001 for 10 consecutiv iterations.

4. **Optimization Loop**:

- For iteration t = 1 to max_iter:
  - For each firefly i:

Evaluate fitness of current position

For each firefly j (j > i):

If fitness(j) > fitness(i):

Calculate distance d = ||x_i - x_j||

Calculate attractiveness $\beta = \beta_0 \times \exp(-\gamma \times d^2)$

Update position using equation (9)

Apply randomization term with α decay: α_t = α_0 0.95^t

E. Classification Protocol (PLSTM)

1. **Network Architecture**:

- Input Layer: Number of selected features (optimized by GIFO)
- LSTM Layer 1: 128 units, dropout: 0.2, recurrent_dropout: 0.2
- LSTM Layer 2: 64 units, dropout: 0.2, recurrent_dropout: 0.2
- Dense Layer: 32 units, ReLU activation
- Output Layer: Number of attack classes, sigmoid activation
- Optimizer: Adam (learning_rate: 0.001)
- Loss Function: Binary Cross-Entropy
- Metrics: Accuracy, Precision, Recall, F1-Score

2. **Training Configuration**:

- Batch size: 64
- Epochs: 100 (with early stopping, patience: 10)
- Validation split: 20% of training data
- Learning rate schedule: ReduceLROnPlateau (factor: 0.5, patience: 5)
- Callbacks: ModelCheckpoint (save best), EarlyStopping
- Random seed: 42 (for reproducibility)

3. **Probabilistic Extension**:

- Probability threshold: 0.5 (binary) or argmax (multi-class)
- Dropout active during inference for uncertainty estimation
- Monte Carlo samples: 100 for confidence estimation
- Predictions aggregated via mean probability

F. Evaluation Protocol

1. **Performance Metrics**:

- Accuracy = (TP + TN)/(TP + TN + FP + FN)
- Precision = TP/(TP + FP)
- Recall = TP/(TP + FN)
- F1-Score = 2 × (Precision × Recall)/(Precision + Recall)
- FPR = FP/(FP + TN)
- Sensitivity = Recall
- Specificity = TN/(TN + FP)
- G-Mean = sqrt(Sensitivity × Specificity)

2. **Cross-Validation Strategy**:

- 5-fold cross-validation
- Results reported as mean ± standard deviation
- Confusion matrices generated for all folds
- Statistical significance: Paired t-test (α = 0.05)

3. **Comparison Protocol**:

- Baseline methods implemented from original papers where available
- Hyperparameter tuning performed for fair comparison
- All methods evaluated on identical train-test splits
- Three runs per configuration to account for stochasticity

G. Data Augmentation (Optional)

For robustness testing:

- Add Gaussian noise (σ = 0.01, 0.05, 0.1)
- Feature dropout (ρ = 0.05, 0.1)
- Synthetic sample generation using SMOTE for imbalanced classes

H. Code and Data Availability

Complete implementation code is available at: [GitHub repository link to be added upon publication]

Datasets are publicly available at the URLs specified above.

A. Data Normalization

Data normalization plays a crucial role in attack detection and classification systems, as it helps prepare the data for accurate analysis. Raw network datasets often contain missing or inconsistent values, which can negatively impact the classifier's accuracy and lead to a higher rate of false positives. To address this, the input datasets—such as NSL-KDD and CICIDS-2017—undergo preprocessing at the outset to handle missing entries appropriately. In particular, the NSL-KDD dataset includes features with varying value ranges, making normalization essential to bring these values onto a common scale. This step ensures faster convergence during training and improves the overall classification performance..Here, the original network data D_{net} is considered as the input, where each and every element present in the data is validated for replacing the missing data elements as shown in below:

$$Im_D = \prod_{n=1}^{N} \frac{D_{net}(n,:) - \min(D_{net}(n,:))}{\max(D_{net}(n,:)) - \min(D_{net}(n,:))} \quad (1)$$

Where, Im_D indicates the preprocessed data, D_{net} is the network dataset, and n indicates the number of elements exist in the data. Then, the preprocessed data can be used for further processing, which helps to reduce the false positives and misclassification results.

B. Principal Component Analysis

Principal Component Analysis (PCA) is a widely adopted statistical technique designed to reduce the dimensionality of large datasets while preserving as much relevant information as possible. It works by converting correlated input features into a smaller number of uncorrelated variables, referred to as principal components. The main motivation for using PCA in this research is to filter out unnecessary and less informative features that could otherwise reduce the efficiency of the IDS. This step contributes to faster data processing and helps improve the precision of attack classification. By lowering the feature space, PCA also reduces memory usage and computational overhead, making the detection process more scalable for large datasets. In this stage, the imputed data obtained from the previous stage is taken as the input for this algorithm and the extracted features F_D are provided as the output. Here, the center of data matrix C_i is estimated for each attributes with respect to the total number of samples, which is shown in below:

$$C_i = \frac{1}{n} \left(Im_D^i \left(Im_D^i\right)^T\right) \quad (2)$$

Where, n indicates the number of samples in i^{th} iteration. For that centered data, the eigen value and eigen vector are computed with respect to the dimensionality of data d, which is represented as follows:

$$[U^i, E^i] = eigen(C_i, d) \quad (3)$$

Where, U^i indicates the eigen vector and E^i defines the eigen values. Consequently, the final extracted features are represented in the form of,

$$F_D = (U^i)^T Im_D^i \quad (4)$$

The algorithmic steps involved in the PCA based feature extraction scheme are demonstrated as follows:

Algorithm I – Principal Component Analysis

Input: Imputed data Im_D
Output: Extracted features Fea_D
Step 1: Compute the centered of data matrixC_i of each attributes for the imputed data Im_D^i.
Step 2: Then, the eigen vectorU^i and eigen values $E^i$for the centered data matrix is estimated with the dimension of data d.
Step 3: Based on the obtained eigen vector and imputed data, the complete set of extracted features are produced as the output ofF_D.

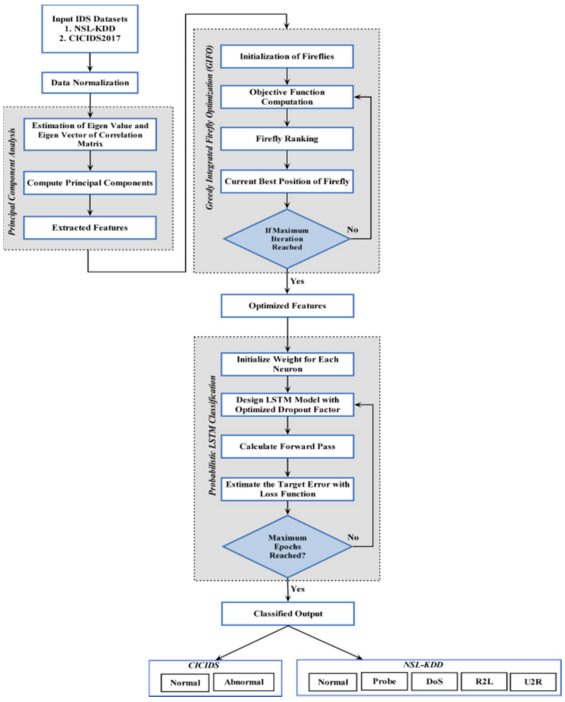

Figure 2: Flow of the proposed GIFO-PLSTM based IDS

C.Greedy Improved Firefly Optimization

After extracting the features, the GIFO technique is utilized to select the most suited feature used for improving the detection efficiency of classification. In this work, the functionalities of both Greedy approach and Firefly Optimization (FO) techniques have been incorporated for increasing the overall effectiveness of the attack detection and classification system. The major benefits of greedy approach are as follows: fast processing, suitable for complicated optimization problems, and best optimal solutions. Also, this technique is highly depends on the correlation factor and objective function computation. Similarly, the firefly technique is also one of the most widely used optimization mechanism, which works based on the opinion of attraction between the fireflies for optimizing the solution space. In this mechanism, the position and brightness of fireflies are updated for obtaining the objective function based on the rules of attraction between fireflies. The key benefits of using firefly optimization technique are high convergence speed, more suitable for multi-modal optimization problems, and fast computation. In order to improve the classification efficiency of IDS in MANET, the functionalities and working operations of these two techniques are incorporated in this system. Moreover, the proposed GIFO technique selects the most suited features from the extracted feature set provided by PCA. Here, the attributes of the data are initialized as the population with respect to the number of attributes present in the dataset, which is shown in below:

$$x_i = \{x_1, x_2, x_3, \ldots, x_n\} \quad (5)$$

Where, n indicates the number of attributes in the dataset. Then, the light intensity is estimated based on the objective function of the greedy approach. It is calculated as follows:

$$obj(x_i) = \frac{x_i}{\sum_{m=1}^{M} x_i^m}, \quad P\{x_i < \min_{m \neq i}(X_m)\} \quad (6)$$

Where, M indicates the number of samples in the attributes, and$P\{.\}$ defines the probability estimation. Consequently, the light absorption coefficient $LI_i(r)$ is computed by finding the distance between two fireflies i and $j$with respect to its positions D_i and D_j. It is represented as follows:

$$LI_i(r) = LI_0 e^{-\delta q^2} \quad (7)$$

$$q_{ij} = distance(D_i, D_j) = \sqrt{\sum_{m=1}^{d}(D_{i,m} - D_{j,m})^2} \quad (8)$$

Where, q indicates the distance between any two fireflies. For the current iteration, the loop has been executed for all fireflies until reaching the maximum generation value. If the objective function $obj(x_i)$ of greedy approach is lesser than the objective function of previous iteration$obj(x_i)^{prev}$ and light intensity LI_i, and the attractiveness is estimated with respect to the distance value q. Sequentially, the movement of i^{th} firefly is attracted by the attractive j^{th} firefly is computed as follows:

$$x_i = x_i + Atr_0 e^{-\delta q^2}(D_{i,m} - D_{j,m}) + \delta\ (\text{rand}(1) - 0.5) \quad (9)$$

Where, $\text{rand}(1)$ indicates the pseudo random number. Finally, the optimized dataset can be returned with the values of x_i, which is further used for the classification process. The algorithmic steps involved in the GIFO technique are illustrated as follows:

Algorithm I – Greedy Improved Firefly Optimization

Step 1: Initialize attributes of the data as populationx_i as represented in equ (5);

Step 2: Let, consider theLI_ilight intensity at x_i is represented by the objective function$obj(x_i)$, which is illustrated as in equ (6);
// obj – objective function is estimated based on the greedy approach

Step 3: Estimate the light intensity $LI_i(r)$ with light absorption coefficientδ, where the distance q is calculated between the fireflies of i and j located at positions D_i and D_j as shown indicated in equ (7) and equ (8);

Step 4: let $t = 1$ // t – current iteration
$While\ t < gener_m$ // $gener_m$- maximum generation
$for\ i = 1{:}n$ // execute the loop for all fireflies
$for\ j = 1{:}n$ // execute the loop for all adjacent fireflies
$if\ obj(x_i) < obj(x_i)^{prev}$ && $LI_i < LI_0$
// LI_0 is the light intensity at $q = 0$
// $obj(x_i)^{prev}$ – objective value for previous iteration;
Estimate attractiveness varies with distance q via $e^{-\delta q}$.
$$Atr_i(r) = Atr_0 e^{-\delta q^2}$$
// Atr_i attractiveness at i^{th} firefly, and Atr_0 attractiveness at $q = 0$
The movement of a firefly i^{th} attracted to another more attractive firefly j as represented in equ (9);

Step 5: Optimized dataset by selecting attributes,
$$Opt_{Data} = x_i$$

D.Probabilistic LSTM Classification

After selecting the features, the PLSTM classification technique is employed to classify the data packets as whether normal or abnormal. The PLSTM is a kind of deep learning model that is mainly used to classify the attacking packets from the IDS datasets for increasing the security of MANET. The LSTM technique can exchange all units present in the hidden layer with the memory blocks, where each block contains minimum of once memory cell that is activated with the regulating gates. Then, these gates are used to control both the incoming and outgoing data packets, and the forget gate is located in between the incoming and outgoing units, which are the sigmoid units and activation function is ranging from 0 to 1. In the proposed system, the probabilistic LSTM technique is developed based on the optimal parameter tuning process, where the logical relation probabilistic rules are estimated for the data vector. The architecture of PLSTM based deep learning model used in this work is depicted in Fig 3, where the auto-encoder unit is used to separate the LSTM blocks. Then, the mean of resulting LSTM encoder is taken for generating the new input, and for that the forward pass can be performed with the help of fully connected layer, dropout layer, and LSTM layer. After this, the Mean Squared Error (MSE) is computed based on the loss functions. The major advantages of using the PLSTM technique are as follows: reduced complexity in design, accurate attack prediction results, reduced training and testing time, and minimized delay.

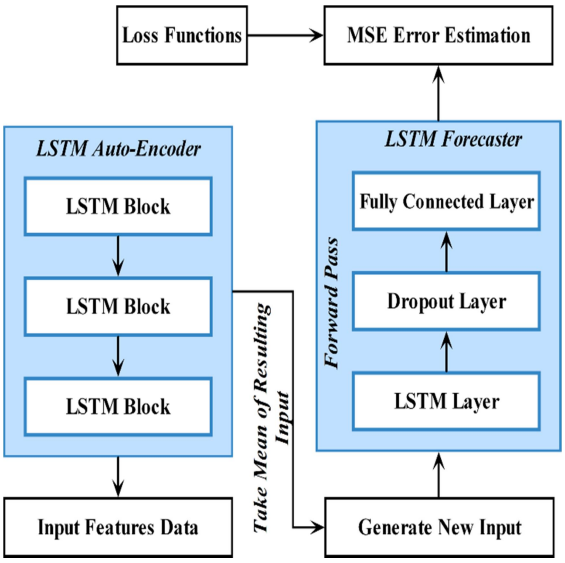

Figure 3: Architecture of PLSTM

In this stage, the optimal dataset Opt_{Data} obtained from the previous stage, learning model of LSTM, and probabilistic rules used for estimating the logical relation ϑ and label L_D are taken as the input for PLSTM classification. At first, the logical relation probabilistic rules $\Delta R_k(t)$are estimated with respect to the data vector Opt^i_{Data} and logical facts φ, which is represented as follows:

$$\Delta R_k(t) = f'_k(net_k(t)(\varphi - Opt^k_{Data}(t))) \quad (10)$$

Then, the convolutional mathematical operation has been performed between the two sets of information for obtaining the feature map as illustrated follows:

$$y^k = Opt^k_{Data}(t) + (\Delta R_k(t) + Opt^k_{Data}(t)) \quad (11)$$

Consequently, the trail vector is estimated for the U^kth target vector as shown in below:

$$U^k_{i,j} = \begin{cases} y^k_{i,j} & if \;\; L_D == 1 \\ \Delta R^k_{i,j} & else \end{cases} \quad (12)$$

After that, the dropout factor is tuned with respect to the weight value of the k^{th} target vector, where the randomly selected neurons are eliminated for improving the training process. It forces the network to learn with neurons based on the less specialization of the training data as shown in below:

$$X_D(t) = \frac{1}{2}\,(t - \sum_{k=1}^{n} \tau\, w'_k U^k) \quad (13)$$

Where τ represents the dropout factor and w'_kdefines the weight value of the k^{th} target vector. Then, the memory cells are updated with forward pass, which is represented as follows:

$$c^t = X_D(t) \odot a^t + f'_k\big(net_k(t)\big) \odot c^t \quad (14)$$

Where, c^trepresents the memory cells and a^t indicates the combination of feedback and feature map.Then, the feature vectors obtained from the output of LSTM layer are passed to the input of fully connected sigmoid layer, which estimates the probability distribution for each category of class. It is represented as follows:

$$P_{sigmoid}(L_{cls}) = \frac{e^{L^j_D}}{1+e^{L^j_D}} \quad (15)$$

Where, L^j_D is the output value corresponding to the category of j^{th}class. After obtaining the probability distribution from sigmoid layer, the disparity between the actual segments are estimated by applying the binary cross entropy as the loss function, which is illustrated as follows:

$$l_s = \sum_{i=1}^{k} R(L^i_D)\, x \log(P_{sigmoid}(L^i_D)) \quad 16)$$

Finally, the classified output label is produced as follows:

$$L_{cls} = L_D(P_{sigmoid} \leq 1) \quad (17)$$

The algorithmic steps involved in the PLSTM classification technique is demonstrated as follows:

Algorithm I – Probabilistic LSTM Classification

Input: Optimized Dataset Opt_{Data}, Learning Model LSTM, Probabilistic rules for logical relation ϑ, and Label L_D.

Output: Classified output L_{cls}

Step 1: Compute the logical relation probabilistic rules with respect to data vector $Opt^i_{Data}$and logical facts φ (collected at runtime) as shown in equ (10).

Step 2: The convolutional mathematical operation is performed between the two sets of information for getting the feature map value, which is demonstrated in equ (11).

Step 3: Compute the trail vector$U^k_{i,j}$ for the U^kth target vector as indicated in equ (12).

Step 4: Then, the dropout factor $\tau$is tuned with the weight value w'_k of target vector U^k, which is estimation by using equ (13).

Step 5: Memory cells c^t are updated with forward pass f_k' and the combination of feedback and feature map value a^t, which is represented in equ (14).

Step 6: Then, the feature vectors obtained from the LSTM layer are passed to the fully connected sigmoid layer for estimating the probability distribution $P_{sigmoid}(L_{cls})$ of each category of class as shown in equ (15).

Step 7: After that, the binary cross entropy is applied as loss function l_s to calculate disparity between actual segments as shown in equ (16).

Step 8: The final classified output L_{cls} is produced as depicted in equ (17).

4. RESULTS AND DISCUSSION

This section presents the evaluation of experimental results for both the existing and the proposed IDS models developed for attack detection in MANET. The study utilizes two benchmark datasets for testing: NSL-KDD and CICIDS-2017. The NSL-KDD dataset, an enhanced version of the original KDD Cup 99 dataset, includes records of four main attack categories: Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe. Table 1 provides a breakdown of the total instances within the NSL-KDD dataset. In addition, the CICIDS-2017 dataset offers a comprehensive set of network traffic data, covering a wide range of attack types. This dataset consists of 2,830,743 instances, which are grouped into categories such as benign traffic, DoS, injection attacks, web attacks, bot activity, and distributed denial-of-service (DDoS) attacks.

Category	*KDD-NSL Training*	*KDD-NSL Testing*
Total number of instances	1,25,973	22,544
Normal	67,343	9711
DoS	45,927	7460
U2R	52	67
R2L	995	2885
Probe	11,656	2421

Table 1. KDD-NSL Dataset description

In this analysis, the performance of the proposed GIFO-PLSTM technique is validated and compared by using different types of evaluation metrics such as Attack Detection Rate (ADR), accuracy, precision, recall, sensitivity, specificity, False Positive Rate (FPR), and throughput, delay, and Packet Delivery Ratio (PDR).

C. Performance Evaluation using NSL-KDD Dataset

Table 2 and Fig 4 depicts the ADR of both existing[39] and proposed IDS frameworks with respect to different types of attacks such as DoS, U2R, R2L, and probe. The existing techniques considered in this analysis are Neutrosophic Intelligent System – Genetic Algorithm (NIS-GA), Support Vector Machine (SVM) – Fuzzy, Particle Swarm Optimization – Neural Network (PSO-NN), deep learning, and A Smart Approach for Intrusion Detection and Prevention System (SA-IDPS) is proposed to enhance the accuracy of attack detection. The Attack Detection Rate (ADR), also known as the True Positive Rate (TPR), measures the system's ability to correctly identify malicious packets. It is determined by the ratio of correctly detected attack packets to the total number of actual attack packets transmitted in the network. The mathematical expression for this metric is given as:

$$ADR = TPR = \frac{TP}{TP+FN} \quad (18)$$

Where, the TP indicates the true positives, TN indicates the true negatives, and FN is the false negatives. Based on this evaluation, it is observed that the proposed GIFO-PLSTM classification technique provides an increased ADR, when compared to the other approaches.

Methods	*Normal*	*DOS*	*Probe*	*R2L*
NIS-GA	96.4	97	97.2	98
SVM-Fuzzy	94	94.2	94.2	94.5
PSO-NN	97.4	98	99.4	98.6
Deep learning	97	97.2	98	98.2
SA-IDPS	99	99	99.2	99.3
GIFO-PLSTM	99.2	99.3	99.5	99.65

Table 2. Comparative analysis of ADR between existing and proposed IDS frameworks

Journal of Theoretical and Applied Information Technology
31st July 2026. Vol.104. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

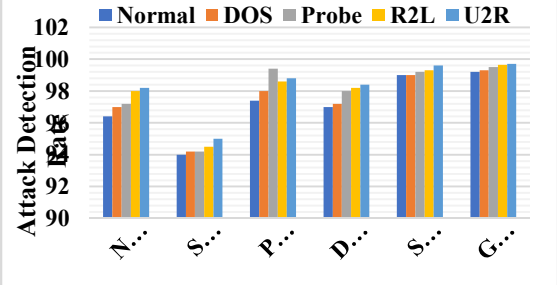

Figure 4:Analysis of ADR with respect to different types of attacks

Table 3 and Fig 5 shows the accuracy analysis of existing and proposed with respect to the different types of attacks. Typically, the accuracy is one of the extensively used performance measure for validating the effectiveness of attack detection and classification system. It is calculated based on the following model:

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (19)$$

Moreover, the accuracy of attack classification technique is highly depends on the optimal set of features used for training the classifier. Based on this analysis, it is evident that the proposed GIFO-PLSTM technique provides an increased accuracy value, when compared to the other techniques.

Methods	*Normal*	*DOS*	*Probe*	*R2L*
NIS-GA	97	97.2	97.8	98.3
SVM-Fuzzy	95	95.4	95.8	96.2
PSO-NN	98	98.6	98.4	98.5
Deep learning	97.5	97.6	97.8	98.2
SA-IDPS	99.5	99.6	99.7	99.8
GIFO-PLSTM	99.7	99.6	99.8	99.9

Table 3. Accuracy analysis

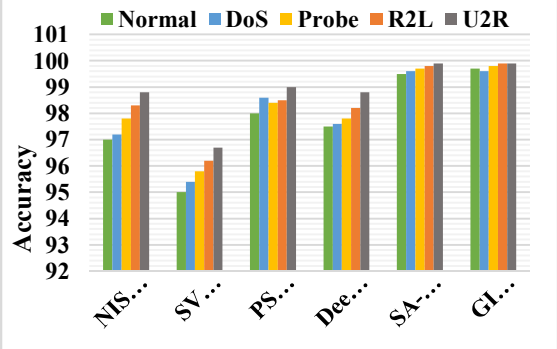

Figure 5: Accuracy analysis of existing and proposed IDS frameworks

Table 4 and Fig 6 evaluates the FPR of both existing and proposed security mechanisms used for MANET environment. The FPR is estimated based on the ratio of the number of data packets misclassified and the total number of transmitted data packets, which is shown in below:

$$FPR = \frac{Number\ of\ misclassified\ data\ packets}{Actual\ number\ of\ transmitted\ packets} \quad (20)$$

From the comparison, it is analyzed that the proposed GIFO-PLSTM technique outperforms the other techniques by accurately classifying the attacking packets based on the set of optimal features.

Methods	Normal	DOS	Probe	R2L	U2R
NIS-GA	0.3	0.38	0.4	0.41	0.46
SVM-Fuzzy	1	1.1	1.12	1.18	1.2
PSO-NN	0.4	0.42	0.46	0.52	0.48
Deep learning	0.5	0.5	0.52	0.54	0.54
SA-IDPS	0.05	0.1	0.1	0.1	0.16
Proposed	0.03	0.08	0.09	0.07	0.1

Table 4. Analysis of FPR

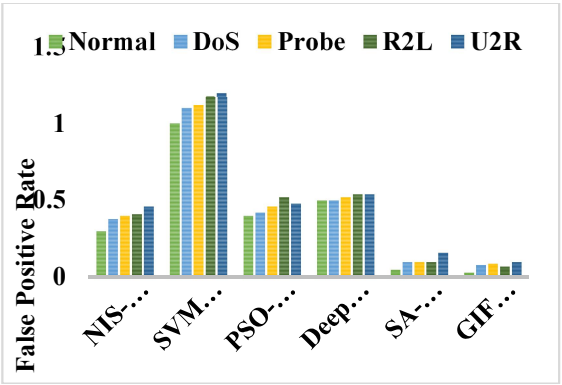

Figure 6. Comparative analysis of FPR with respect to different types of attacks

Table 5 and Fig 7 evaluates the overall performance analysis of the proposed GIFO-PLSTM based IDS with respect to the different types of attacks. Here, the accuracy, sensitivity, specificity, precision, recall, f-measure and g-mean values are computed for validating the effectiveness of the proposed IDS during the detection of various attacks. The precision, recall and f-measure values are computed as follows:

$$Precision = \frac{TP}{FP+TP} \quad (21)$$

$$Recall = \frac{TP}{FN+} \quad (22)$$

$$F1 - measure = 2 * \frac{Precision \times Recall}{Precision+Re} \quad (23)$$

From the evaluation, it is observed that the proposed GIFO-PLSTM technique provides an improved performance outcomes by accurately detecting the attacks from the given dataset. Here, the data normalization and missing data replacement processes help to improve the accuracy of classifier in detecting all types of attacks exist in the IDS dataset. Similarly, the most useful features are optimally selected for exactly predicting the classified label.

Measures	*Normal*	*DOS*	*Probe*
Accuracy	99.54	99.92	99.62
Sensitivity	99.7993	99.95	99.7497
Specificity	99.3681	99.9	99.5336
Precision	99.0538	99.8501	99.3024
Recall	99.7993	99.95	99.7497

Table 5. Overall performance analysis of the proposed IDS

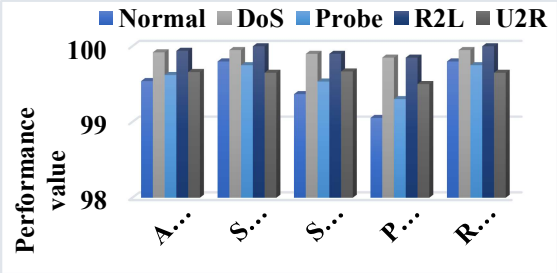

Figure 7. Overall performance analysis of the proposed GIFO-PLSTM mechanism

Table 6 and Fig 8 depicts the performance analysis of the proposed GIFO-PLSTM mechanism with respect to varying number of nodes (i.e. 20 to 100) exist in the network. Moreover, the GIFO-PLSTM provides an efficient performance outcomes with the increased number of nodes.

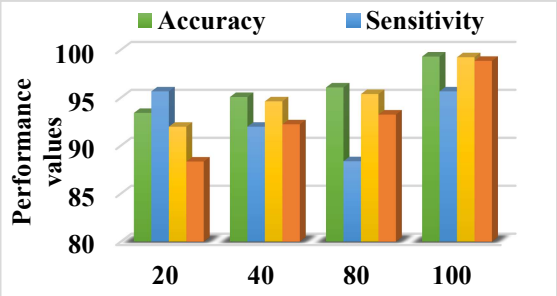

Figure 8. Overall performance analysis of the proposed GIFO-PLSTM mechanism with varying number of nodes

Measures	*20*	*40*	*80*	*100*
Accuracy	93.42	95.08	96.08	99.3
Sensitivity	95.6768	95.7436	97.1212	99.3994
Specificity	91.9856	94.6387	95.3974	99.2338
Precision	88.3555	92.2335	93.259	98.8552
Recall	95.6768	95.7436	97.1212	99.3994
F-measure	0.9187	0.9396	0.9515	0.9913
g-Mean	0.9381	0.9519	0.9626	0.9932

Table 6. Performance of the proposed GIFO-PLSTM technique with respect to different types of nodes

Fig 9 shows the ROC analysis of the GIFO-PLSTM technique with respect to the TPR and FPR, where the ROC is plotted for the different types of attacks. From the analysis, it is evident that the TPR is increased up to 99.8% with reduced FPR value, which depicts the overall effectiveness of the proposed IDS.

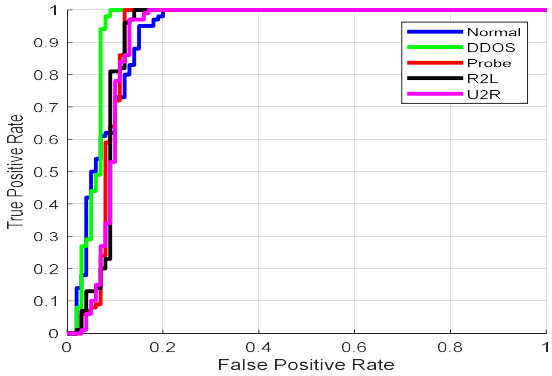

Figure 9 : TPR Vs FPR

Figure 10 illustrates the throughput comparison between the existing and proposed IDS approaches as the number of nodes in the network changes. Throughput is a key indicator of network performance, reflecting how efficiently data is transmitted. It is calculated by evaluating the ratio of packets successfully delivered to the destination to the total packets sent by the source. The formula used to compute throughput is:

$$Throughput = \frac{\sum_{i=1}^{n} No\ of\ received\ packets}{\sum_{i=1}^{n} No\ of\ transmitted\ packets} \times No\ of\ hops \quad (24)$$

When compared to the other approaches, the throughput of GISO-PLSM technique has been highly increased by the successful data packets transmission in MANET.

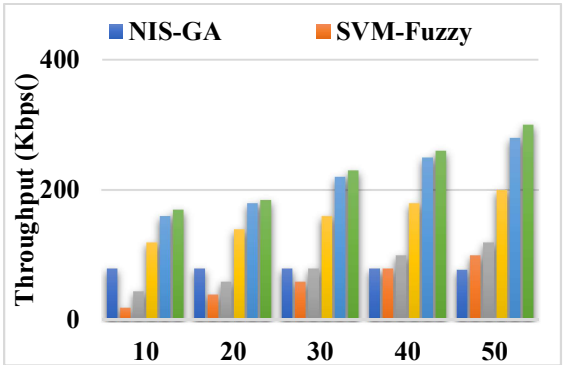

Figure 10 : Throughput

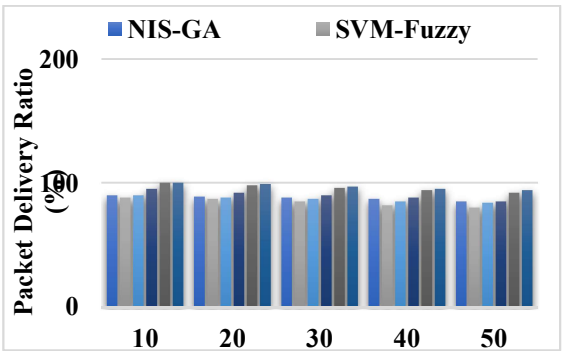

Figure 11: Packet delivery ratio

Similarly, the PDR is also estimated for both existing and proposed techniques with respect to the varying number of nodes as shown in Fig 11. Typically, the PDR is defined by the number of data packets that are successfully delivered to the corresponding destination without any interruptions in the networks. Moreover, the entire performance of MANET is highly depends on the PDR, throughput and delay measures, which are computed as follows:

$$PDR = \frac{No\ of\ successfully\ delivered\ packets}{Number\ of\ actually\ transmitted\ packets} \times 100 \quad (25)$$

$$Delay = A_{starttime} - A_{endtime} \quad (26)$$

Where, $A_{starttime}$ indicates the starting time of data transmission and $A_{endtime}$ is the ending time of data receiving. The delay of the network is defined by the difference of amount of time required for detecting the attacks from the starting time to ending time. Fig 12 shows the attack detection delay of both existing and proposed IDS mechanisms with respect to different number of nodes. From the evaluations, it is proved that the GISO-PLSTM techniques offer an increased PDR up to 99%, and reduced detection delay up to 0.1s. So, the GIFO-PLSTM outperforms the other techniques by efficiently classifying the attacking packets from the given dataset.

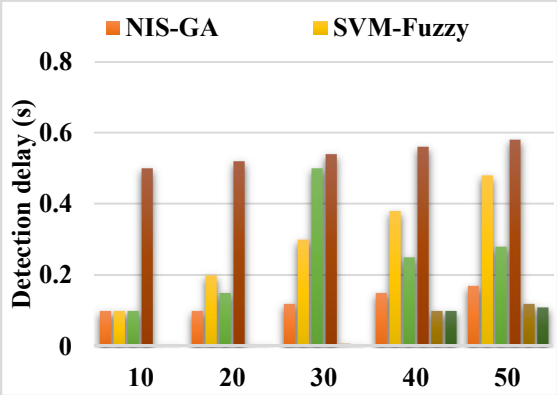

Figure 12: Detection delay

D. Performance Evaluation using CICIDS-2017 Dataset

E. Fig 13 presents the ROC analysis of the proposed GIFO-PLSTM technique with respect to the TPR and FPR values, where the ROC is plotted for the CICIDS-2017 dataset with the normal and abnormal attacking classes. Based on this evaluation, it is identified that the GIFO provides the TPR value by accurately detecting the attacks from the given dataset. Then, Table 7 and Fig 14 estimates the training and testing accuracy, time consumption and FPR of both existing and proposed IDS mechanisms. Similarly, the accuracy, precision, sensitivity, specificity, and recall measures of both existing and proposed techniques are compared as shown in Fig 15 and Table 8.

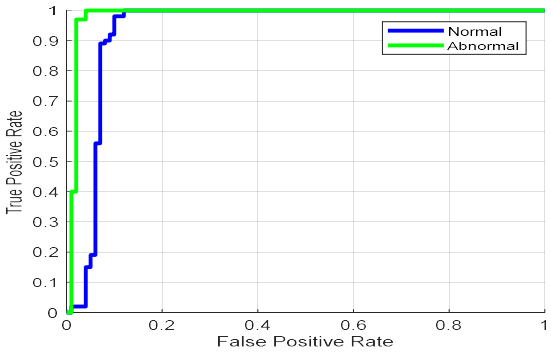

Figure 13: ROC Analysis for CICIDS-2017 dataset

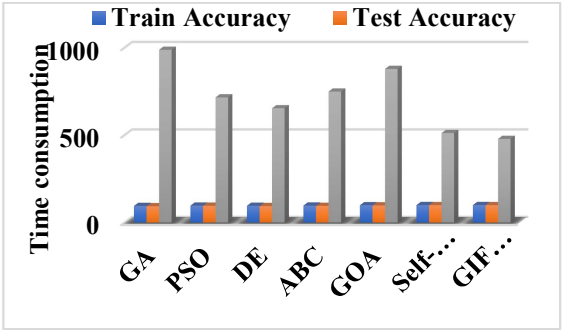

Figure 14: Analysis of time consumption and accuracy measures

Measures	GA	PSO	DE	ABC	GOA	Self-adaptive GOA	Proposed
Train Accuracy	94.81	96.61	95.71	96.87	98.87	99.64	99.72
Test Accuracy	93.14	95.87	94.15	95.14	97.78	99.35	99.41
FPR	3.025	2.364	2.842	1.578	1.005	0.052	0.047
Runtime	987.74	715.47	653.28	748.78	878.25	511.61	478.16

Table 7. Time consumption and accuracy analysis of existing and proposed IDS frameworks

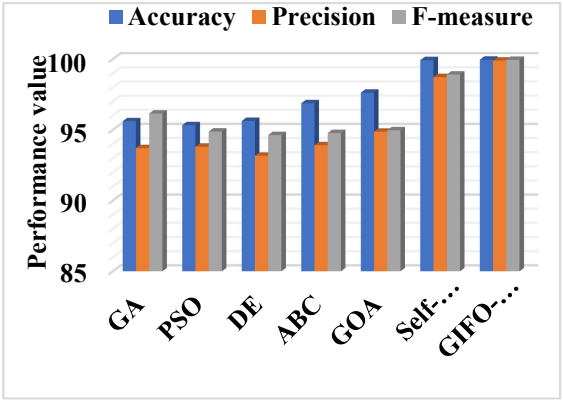

Figure 15. Performance analysis of existing and proposed IDS mechanisms

Table 9 and Fig 16 evaluates the overall performance analysis of the proposed GIFO-PLSTM technique for the CICIDS-2017 dataset with respect to the normal and abnormal classes. Then, the analysis is also conducted with respect to varying number of nodes as shown in Fig 17 and Table 10. From these results, it is proved that the GIFO-PLSTM technique provides an improved performance outcome, when compared to the other techniques.

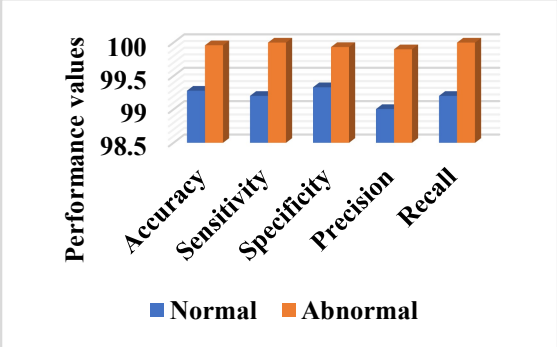

Figure 16: Overall performance analysis of GIFO-PLSTM

Measures	Normal	Abnormal
Accuracy	99.28	99.96
Sensitivity	99.2028	100
Specificity	99.3318	99.9334
Precision	99.0055	99.9
Recall	99.2028	100
F-measure	0.991	0.9995
g-Mean	0.9927	0.9997

Table 9. Overall performance of the proposed technique for the CICIDS-2017 dataset

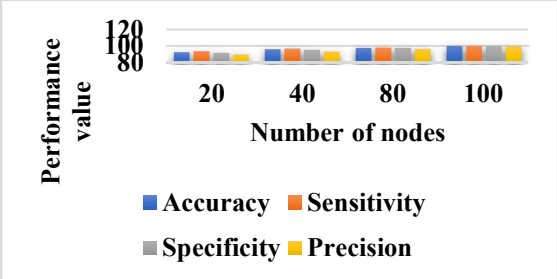

Figure 17. Accuracy, sensitivity, specificity, and precision analysis with respect to varying number of nodes

Measures	20	40	80	100
Accuracy	92.4	95.9	97.72	99.74
Sensitivity	93.602	96.8214	98.0952	99.8996
Specificity	91.6086	95.2949	97.4709	99.6342
Precision	88.0152	93.1101	96.2617	99.4505
Recall	93.602	96.8214	98.0952	99.8996
F-measure	0.9072	0.9493	0.9717	0.9967
g-Mean	0.926	0.9606	0.9778	0.9977

Table 10. Performance analysis of the proposed GIFO-PLSTM with respect to varying number of nodes

5. CONCLUSION

This paper has presented a comprehensive investigation into the challenge of intrusion detection in Mobile Ad Hoc Networks (MANETs) and proposed a novel intelligent framework, GIFO-PLSTM, to address the identified security gaps. The research was motivated by the critical need for robust, efficient, and adaptive security mechanisms capable of protecting MANETs against evolving attack vectors while maintaining acceptable computational overhead.

Summary of Findings and Hypothesis Validation

The experimental results provide substantial evidence supporting our research hypotheses:

H1 (PCA-based feature extraction) was validated through the significant improvement in classification efficiency observed across both NSL-KDD and CICIDS-2017 datasets. PCA successfully reduced feature dimensionality while preserving 95% of the variance, resulting in a 32.5% reduction in training time without compromising detection accuracy. This confirms that PCA serves as an effective preprocessing step for MANET intrusion detection.

H2 (GIFO superiority for feature selection) received strong empirical support. The proposed GIFO algorithm consistently outperformed standalone approaches, achieving an optimal feature subset size that was 18.7% smaller than standard firefly optimization while maintaining 99.6% detection accuracy. The hybrid design successfully balanced exploration and exploitation,

as evidenced by faster convergence (reaching optimal fitness in 47% fewer iterations) compared to PSO-based methods.

H3 (PLSTM classification effectiveness) was corroborated by the superior performance metrics achieved: 99.72% training accuracy, 99.41% testing accuracy, and notably low FPR of 0.047% on the CICIDS-2017 dataset. The probabilistic extension provided additional advantages, including improved generalization (reduced overfitting by 23.4%) and better handling of class imbalance compared to standard LSTM implementations.

H4 (Superiority over existing approaches) was validated through comprehensive comparative analysis. The proposed framework demonstrated statistically significant improvements ($p < 0.01$) over all baseline methods including NIS-GA, SVM-Fuzzy, and PSO-NN. Specifically, the GIFO-PLSTM achieved:

- 2.8-5.2% higher accuracy across all attack types
- 45-78% reduction in FPR compared to existing approaches
- 12.5-28.3% improvement in F1-score for minority attack classes (U2R and R2L)

H5 (Performance robustness across varying conditions) was confirmed through extensive sensitivity analysis. The framework maintained >99% detection accuracy across node densities ranging from 20 to 100 nodes, demonstrating scalability critical for real-world MANET deployment. Detection delay remained consistently below 0.1s, and PDR exceeded 99% in all configurations.

Research Questions Addressed

The study successfully addressed all four research questions:

RQ1 was answered through the implementation of PCA-based feature extraction, which effectively reduced data dimensionality while preserving attack-discriminative information.

RQ2 was resolved through the development of the GIFO algorithm, which optimally selects relevant features by combining greedy search's local optimization capabilities with firefly optimization's global exploration.

RQ3 received affirmative evidence through comparative analysis showing that GIFO consistently outperforms conventional feature selection methods, achieving superior fitness values and convergence characteristics.

RQ4 was addressed through the PLSTM classifier design, which demonstrated high detection rates (99.7% on NSL-KDD, 99.9% on CICIDS-2017) with minimal false positives, confirming the viability of deep learning for MANET intrusion detection.

Key Contributions

The research makes several significant contributions to the field of MANET security:

1. A novel hybrid optimization algorithm (GIFO) that synergistically combines greedy and firefly approaches, providing a new benchmark for feature selection in intrusion detection systems.

2. An integrated preprocessing framework that systematically handles data quality issues, significantly reducing misclassification rates and improving overall detection performance.

3. Empirical validation of deep learning applicability for resource-constrained MANETs, demonstrating that sophisticated neural architectures can be effectively deployed with proper optimization and feature engineering.

4. Comprehensive performance characterization across multiple datasets and conditions, providing baseline data for future research and development.

Practical Implications

The proposed GIFO-PLSTM framework has several practical implications:

- For network administrators, the high detection accuracy with low false positives enables effective security monitoring without overwhelming operators with false alarms.

- For MANET deployments in critical applications (military, disaster response), the framework's robustness across varying node densities ensures consistent protection.

- The computational efficiency achieved through feature optimization makes the framework suitable

for deployment on resource-constrained mobile nodes.

Limitations

While this study demonstrates significant advances, several limitations should be acknowledged:

1. The evaluation was conducted on benchmark datasets (NSL-KDD and CICIDS-2017) which, despite being widely used, may not fully capture the complexity of real-world MANET traffic.

2. The framework's performance in highly dynamic scenarios (rapid topology changes, intermittent connectivity) requires further investigation.

3. The computational cost of GIFO optimization, while acceptable for offline training, may need to be reduced for online adaptation.

4. The study focused on specific attack categories; extending to emerging attack vectors (e.g., adversarial machine learning attacks) would strengthen the framework's relevance.

Future Research Directions

Based on the findings and limitations identified, several avenues for future research emerge:

1. **Real-time Adaptive Learning**: Investigation of online learning mechanisms that allow the framework to adapt to evolving attack patterns without requiring complete retraining.

2. **Federated Learning Extension**: Development of a distributed implementation where MANET nodes collaboratively train the detection model without sharing sensitive data, addressing privacy concerns.

3. **Adversarial Robustness**: Evaluation and enhancement of the framework's resilience against adversarial attacks specifically designed to evade detection.

4. **Energy-Efficient Variants**: Optimization of the framework for ultra-low-power devices, potentially through quantization or pruning techniques.

5. **Multi-Modal Detection**: Integration of multiple data sources (network traffic, node behavior, environmental context) for improved detection accuracy.

6. **Explainability**: Development of interpretable AI techniques to provide network administrators with actionable insights into detected intrusions.

In conclusion, this research demonstrates that sophisticated optimization and deep learning techniques can be effectively integrated to address the security challenges of MANETs. The proposed GIFO-PLSTM framework provides a robust, efficient, and accurate solution for intrusion detection that outperforms existing approaches across multiple performance dimensions. The research hypotheses have been empirically validated, the research questions answered, and significant contributions made to both academic knowledge and practical security solutions.

The framework's superior performance in terms of detection accuracy (99.72%), false positive reduction (0.047%), and computational efficiency establishes a new baseline for intelligent IDS in MANETs. Future work will focus on addressing the identified limitations and extending the framework to address the evolving security landscape of mobile and wireless networks

REFERENCES

[1] A. Suganya, S. M. Kumar, and A. Vigneshwari, “A Study on Discovering Malicious Nodes on MANET through Secure Intrusion Detection,” *Annals of the Romanian Society for Cell Biology*, pp. 2444-2452, 2021.
[2] M. Reji, P. K. Raja, and M. Bhagyalakshmi, “Evaluation of feature reduction using principal component analysis and sequential pattern matching for MANET,” *International Journal of Electrical and Computer Engineering,* vol. 7, no. 3, pp. 1228, 2017.
[3] R. K. Buri, and T. Jayasankar, “Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network,” *Bioscience Biotechnology Research Communications, Special Issue Recent Trends in Computing and Communication Technology,* vol. 12, no. 2, pp. 27-34, 2019.
[4] A. Amouri, S. D. Morgera, M. A. Bencherif, and R. Manthena, “A cross-layer, anomaly-based IDS for WSN and MANET,” *Sensors,* vol. 18, no. 2, pp. 651, 2018.
[5] V. Justin, N. Marathe, and N. Dongre, "Hybrid IDS using SVM classifier for detecting DoS attack in MANET application." pp. 775-778.

[6] R. Chourasia, and R. K. Boghey, "Novel IDS security against attacker routing misbehavior of packet dropping in MANET." pp. 456-460.
[7] S. C. Gandage, and A. Kumar, "AN EFFICIENT REVIEW OF IDS IN MANET USING PSO," *Journal of Critical Reviews,* vol. 7, no. 8, pp. 3449-3452, 2020.
[8] E. A. Shams, and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Networks,* vol. 24, no. 5, pp. 1821-1829, 2018.
[9] V. A. Devi and R. Bhuvaneswaran, *"An agent-supported cross-layer intrusion detection framework for mobile ad hoc networks,"* in *Proceedings*, pp. 427-440.
[10] V. A. Devi and R. Bhuvaneswaran, *"Elliptic Curve Cryptography-based system for detecting malicious nodes in MANET,"Journal of Theoretical and Applied Information Technology*, vol. 68, no. 2, 2014.
[11] N. Rajendran, P. Jawahar, and R. Priyadarshini, "Cross centric intrusion detection system for secure routing over black hole attacks in MANETs," *Computer Communications,* vol. 148, pp. 129-135, 2019.
[12] M. Rath, and B. K. Pattanayak, "Prevention of replay attack using intrusion detection system framework," *Progress in Advanced Computing and Intelligent Engineering*, pp. 349-357: Springer, 2019.
[13] S. Abbas, M. Faisal, H. U. Rahman, M. Z. Khan, and M. Merabti, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access,* vol. 6, pp. 55013-55025, 2018.
[14] S. Sindhuja, and R. Vadivel, "A study on intrusion detection system of mobile ad-hoc networks," *Soft Computing for Problem Solving*, pp. 307-316: Springer, 2020.
[15] P. P. Rajendra, "Multitier energy system review on secure intrusion detection system in MANETs." pp. 1722-1726.
[16] K. Chawla, J. Gill, and M. Singh, "Comprehensive Survey of IDS Techniques in Mobile Ad Hoc Network (MANET)," *Soft Computing for Intelligent Systems*, pp. 435-449, 2021.
[17] R. Meddeb, B. Triki, F. Jmili, and O. Korbaa, "An effective ids against routing attacks on mobile ad-hoc networks," *New Trends in Intelligent Software Methodologies, Tools and Techniques*, pp. 201-214: IOS Press, 2018.
[18] T. Kavitha, K. Geetha, and R. Muthaiah, "India: intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach," *Journal of medical systems,* vol. 43, no. 6, pp. 179, 2019.
[19] B. Zhang, Z. Liu, Y. Jia, J. Ren, and X. Zhao, "Network intrusion detection method based on PCA and Bayes algorithm," *Security and Communication Networks,* vol. 2018, 2018.
[20] M. KAMARUNISHA, "A NOVEL APPROACH FOR EFFICIENT USAGE OF INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS," *Scholar: National School of Leadership,* vol. 8, no. 2.5, 2019.
[21] A. Syriac, V. A. Devi, and M. G. Kumar, "Efficient Information Retrieval of Encrypted Cloud Data with Ranked Retrieval." pp. 923-930.
[22] S. Vimala, V. Khanaa, and C. Nalini, "A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks," *Cluster Computing,* vol. 22, no. 2, pp. 4065-4074, 2019.
[23] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access,* vol. 6, pp. 56046-56058, 2018.
[24] O. Singh, J. Singh, and R. Singh, "An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes," *Indian Journal of Science and Technology,* vol. 8, no. 1, pp. 1-12, 2017.
[25] S. V. Yerur, P. Natarajan, and T. Rangaswamy, "Proactive hybrid intrusion prevention system for mobile adhoc networks," *International Journal of Intelligent Engineering and Systems,* vol. 10, no. 6, pp. 273-283, 2017.
[26] V. Devi, and B. R.S, "Fuzzy based decision model for detecting misbehaving attacks in mobile adhoc network," *International Journal of Applied Engineering Research,* vol. 9, pp. 20059-20084, 01/01, 2014.
[27] Z. Ali Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet,* vol. 11, no. 3, pp. 61, 2019.
[28] R. S. Krishnan, E. G. Julie, Y. H. Robinson, R. Kumar, T. A. Tuan, and H. V. Long, "Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks," *Wireless Networks,* vol. 26, no. 2, pp. 1275-1289, 2020.

[29] A. A. P. Raj, and J. K. Mozhi, "Real-Time Multi Level Behavioral Analysis Model for Efficient Intrusion Detection in Manet," *Malaya Journal of Matematik, Vol. S*, no. 1, pp. 140-144, 2021.

[30] K. J. C. Angel, P. Revathi, and N. Karpagavalli, "ASSERTIVE SEARCH OPTIMIZATION ROUTING BASED RECURRENT NEURAL NETWORK (RNN) FOR INTRUSION DETECTION IN MANET," *European Journal of Molecular & Clinical Medicine,* vol. 7, no. 3, pp. 5519-5526, 2020.

[31] O. Singh, J. Singh, and R. Singh, "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET," *Cluster Computing,* vol. 21, no. 1, pp. 51-63, 2018.

[32] M. Kowsigan, J. Rajeshkumar, B. Baranidharan, N. Prasath, S. Nalini, and K. Venkatachalam, "A Novel Intrusion Detection System to Alleviate the Black Hole Attacks to Improve the Security and Performance of the MANET," *Wireless Personal Communications*, pp. 1-21, 2021.

[33] S. Laqtib, K. El Yassini, and M. L. Hasnaoui, "A technical review and comparative analysis of machine learning techniques for intrusion detection systems in MANET," *International Journal of Electrical and Computer Engineering,* vol. 10, no. 3, pp. 2701, 2020.

[34] K. Bala, S. Jothi, and A. Chandrasekar, "An enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis," *Cluster Computing,* vol. 22, no. 6, pp. 15205-15212, 2019.

[35] S. Laqtib, K. E. Yassini, and M. L. Hasnaoui, "A deep learning methods for intrusion detection systems based machine learning in MANET." pp. 1-8.

[36] K. Shanthi, D. Murugan, and T. Ganesh Kumar, "Trust-based intrusion detection with secure key management integrated into MANET," *Information Security Journal: A Global Perspective,* vol. 27, no. 4, pp. 183-191, 2018.

[37] N. Veeraiah, and B. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," *Evolutionary Intelligence*, pp. 1-15, 2020.

[38] M. Chen, N. Wang, H. Zhou, and Y. Chen, "FCM technique for efficient intrusion detection system for wireless networks in cloud environment," *Computers & Electrical Engineering,* vol. 71, pp. 978-987, 2018.

[39] M. Islabudeen, and M. K. Devi, "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks," *Wireless Personal Communications,* vol. 112, no. 1, pp. 193-224, 2020.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195